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

JOHN ALEXANDER MUÑOZ

CÓDIGO. 10696958.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA (UNAD)

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA (ECBTI)

INGENIERÍA DE SISTEMAS

PIEDRA SENTADA

2018

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

JOHN ALEXANDER MUÑOZ

CÓDIGO. 10696958.

DIPLOMADO DE PROFUNDIZACIÓN CISCO (DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN / WAN)

ASESOR.

DIEGO EDINSON RAMIREZ.

INGENIERO ELECTRÓNICO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA (UNAD)

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA (ECBTI)

INGENIERÍA DE SISTEMAS

PIEDRA SENTADA

2018

NOTA DE ACEPTACION

_____
_____
_____
_____
_____
_____
_____

_____

Presidente del jurado

_____

Jurado

_____

Jurado (En caso de ser solo uno, borrar este o agregar de ser necesario).

Piedra Sentada 21 de Diciembre de 2018

DEDICATORIA.

El presente trabajo va dedicado principalmente a Dios por ayudarme siempre para que este sueño hoy en día sea una realidad.

A mi familia por estar siempre presente tanto en mis tristezas como en mis alegrías porque estoy seguro que sin su apoyo, comprensión y motivación no habría podido lograrlo.

A mi comunidad en general por que les he demostrado que nada es difícil con voluntad, que los sueños por imposibles que parezcan se pueden hacer realidad y que una persona humilde puede llegar a superarse y ser un buen referente para los demás.

AGRADECIMIENTOS.

Primero que todo darle gracias a Dios todo poderoso por permitirme haber escalado un paso más en este largo caminar y llevarme hasta el lugar donde me encuentro hoy en día seguro de que sin su ayuda no habría podido lograrlo y confiando plenamente en EL en cada paso que doy.

En segundo lugar darle gracias a todas las personas que sin egoísmo aportaron a mi formación como profesional con sus conocimientos especialmente al señor Diego Edinson Ramírez, el cual fue el asesor del DIPLOMADO DE PROFUNDIZACIÓN CISCO, que estuvo siempre motivando y dando lo mejor de él para alcanzar ese gran objetivo.

Agradecerles también a mi esposa y a mis hijos que siempre estuvieron presentes a pesar de las dificultades en el desarrollo de cada uno de los ejercicios presentes en el DIPLOMADO DE PROFUNDIZACIÓN CISCO, porque ellos también sufrieron conmigo en esos momentos. Gracias por comprenderme y estar presentes en ese largo pero muy fructífero logro de ser un ingeniero de Sistemas con un gran conocimiento en redes de internet y presto a seguir aprendiendo cada día más.

Agradecerle a mis compañeros del grupo ya que siempre estuvieron ahí para ayudarnos conjuntamente apoyándonos unos a otros y así alcanzar este gran logro que es obtener nuestro título como profesionales.

TABLA DE CONTENIDO.

LISTAS DE TABLAS.

LISTA DE FIGURAS.

GLOSARIO.

DHCP. (Dynamic Host Configuration Protocol, protocolo de configuración de host dinámico) es un protocolo que permite que un equipo conectado a una red pueda obtener su configuración (principalmente, su configuración de red) en forma dinámica (es decir, sin una intervención especial). Solo tienes que especificarle al equipo, mediante DHCP, que encuentre una dirección IP de manera independiente. El objetivo principal es simplificar la administración de la red

Dirección IP. Número que identifica, de manera lógica y jerárquica, a una Interfaz en red (elemento de comunicación/conexión) de un dispositivo (computadora, tableta, portátil, smartphone) que utilice el protocolo IP o (Internet Protocol), que corresponde al nivel de red del modelo TCP/IP. La dirección IP no debe confundirse con la dirección MAC, que es un identificador de 48 bits para identificar de forma única la tarjeta de red y no depende del protocolo de conexión utilizando la red.

DNS Loockup. La búsqueda DNS inversa o la resolución DNS inversa (rDNS) es la determinación de un nombre de dominio que está asociado a una determinada dirección IP utilizando el Sistema de nombres de dominio (DNS) de Internet. Las redes de ordenadores utilizan el Sistema de Nombres de Dominio para determinar la dirección IP asociada a un nombre de dominio. Este proceso también se conoce como la resolución de DNS hacia adelante. La búsqueda de DNS inversa es el proceso inverso, la resolución de una dirección IP a su nombre de dominio designado.

DSL. Conexión Internet DSL utiliza tu línea telefónica para recibir información del proveedor de Internet. Debido a que la conexión es digital, esto permite que utilices el teléfono y el Internet simultáneamente. Los módems DSL por lo general incluyen divisores que te permiten conectar la computadora y el teléfono al mismo contacto telefónico.

DCE. (Data Terminal Equipment): equipos que son la fuente y destino de los datos. Comprenden equipos de computación (Host, Microcomputadores y Terminales). DCE (Data Communications Equipment): equipos de conversión entre el DTE y el canal de transmisión, es decir, los equipos a través de los cuales conectamos los DTE a las líneas de comunicación 20 Equipo de comunicación de datos (DCE): Un dispositivo que suministra los servicios de temporización a otro dispositivo. Habitualmente, este dispositivo se encuentra en el extremo del enlace que proporciona el acceso WAN. Lista de acceso estándar Lista de acceso extendida

OSPF. Open Shortest Path First (OSPF), Primer Camino Más Corto, es un protocolo de red para encaminamiento jerárquico de pasarela interior o Interior

Gateway Protocol (IGP), que usa el algoritmo SmoothWall Dijkstra enlace-estado (Link State Advertisement, LSA) para calcular la ruta idónea entre dos nodos cualesquiera de un sistema autónomo.

NAT. La traducción de direcciones de red o NAT (del inglés Network Address Translation) es un mecanismo utilizado por routers IP para intercambiar paquetes entre dos redes que asignan mutuamente direcciones incompatibles. Consiste en convertir, en tiempo real, las direcciones utilizadas en los paquetes transportados. También es necesario editar los paquetes para permitir la operación de protocolos que incluyen información de direcciones dentro de la conversación del protocolo.

ROUTER. Dispositivo de hardware que permite la interconexión de ordenadores en red.

SWITCH. Dispositivo que permite que la conexión de computadoras y periféricos a la red para que puedan comunicarse entre sí y con otras redes.

RESUMEN.

El presente trabajo se realiza teniendo en cuenta el conocimiento obtenido en el largo periodo del Diplomado de Profundización CISCO, donde aplicamos ese conocimiento a dos escenarios que presentan una topología de red diferentes pero utilizan entre si dispositivos tanto intermediarios como finales de las mismas características. Se diseña la topología de la red en la herramienta interactiva Packet Tracer, la cual es de muy fácil uso que permite diseñar, configurar y simular las topologías de red que en ella se elaboran, logrando realizar configuraciones de dispositivos que ayudan en el desarrollo de la presente práctica.

El uso de comandos que se emplean en la configuración de los dispositivos hacen que cada escenario realice su tarea para la cual fue diseñada, para eso se tiene en cuenta el comando Ping para verificar su conectividad entre dispositivos.

La configuración de la red en cada escenario involucra dispositivos de capa 2 y capa 3 para alcanzar lograr interconectividad entre las redes Virtuales LAN, a la misma vez los dispositivos terminales conectados a la LAN puedan salir a internet por el uso del protocolo NAT.

INTRODUCCIÓN.

A lo largo de nuestra carrera como ingenieros de sistemas y ya próximos a graduarnos, hemos sido emprendedores y conocedores de lo que la tecnología y las redes hacen que el mundo no están inmenso como no lo hacen creer, ya que la tecnología lo ha convertido en algo muy pequeño gracias a las redes que nos tienen en contacto directo con los demás hermanos de diferentes Países.

Packet Tracer es la herramienta de aprendizaje y simulación de redes interactiva para los instructores y alumnos de Cisco CCNA. Esta herramienta les permite a los usuarios crear topologías de red, configurar dispositivos, insertar paquetes y simular una red con múltiples representaciones visuales. Packet Tracer se enfoca en apoyar mejor los protocolos de redes que se enseñan en el currículum de CCNA. Packet Tracer tiene el propósito de ser usado como un producto educativo que brinda exposición a la interfaz de línea de comandos de los dispositivos de Cisco para practicar y aprender por descubrimiento.

En el presente trabajo se dará a conocer la realización de dos escenarios de red, correspondientes a los diferentes temas del curso Cisco CCNA1 y CCNA2 mediante el cual aplicaremos nuestro conocimiento adquirido durante el desarrollo del mismo, en el cual se demostrará la capacidad para implementar la seguridad en cada uno de los dispositivos tanto finales como intermediarios y realizar configuraciones como: NAT, servidor de DHCP, RIPV2 y el routing entre VLAN, configuración de direcciones IP, las VLAN, los enlaces troncales y las subinterfaces; dichas configuraciones se aplicaron a los distintos equipos de las diferentes redes propuestas, con el fin de adquirir y medir nuestro conocimiento en el desarrollo de cada una de las practicas.

OBJETIVOS.

Objetivo General.

- Aplicar la temática de conectividad IPv4, seguridad de switch enrutamiento inter VLAN, OSPFv2, DHCP, NAT dinámica / estática y listas de control de acceso (ACL) mediante un caso práctico propuesto por el tutor del diplomado.

Objetivos Especificos.

- Analizar los conceptos de conectividad IPv4, seguridad de switch, enrutamiento inter VLAN, OSPFv2, DHCP, NAT dinámica / estática y listas de control de acceso (ACL) previo a la configuración de dispositivos.

- Desarrollar un informe con evidencias donde se aplique y configure una solución práctica descrita en el escenario propuesto en la prueba de habilidades.

- Generar un escenario virtual en Packet Tracer (archivo de extensión pka) con la configuración sugerida en la prueba de habilidades.

- Verificar la conectividad de los dispositivos virtuales mediante el uso de comandos: ping, traceroute, show ip route, entre otros. Y así cumplir con los requisitos del escenario virtual.

ESCENARIO 1.

ACTIVIDAD A DESARROLLAR.

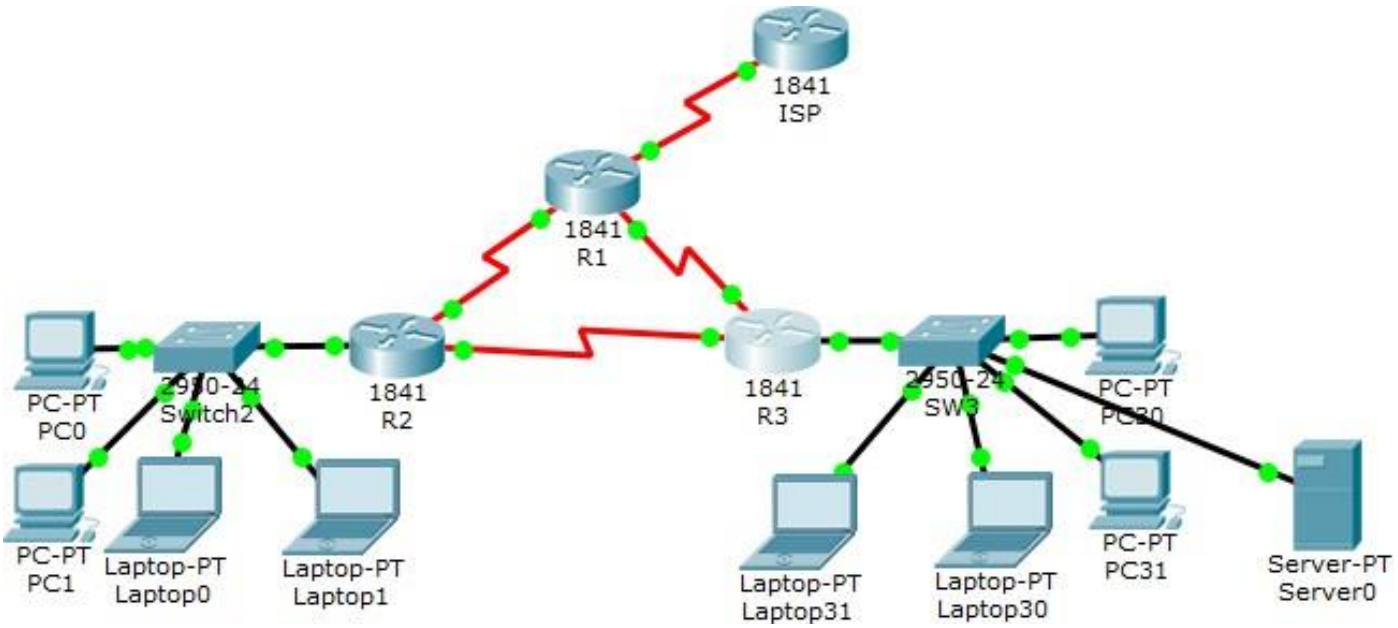


Figura 1. Escenario 1.

Tabla 1. Direccionamiento.

El administrador	Interfaces	Dirección IP	áscara 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 2. Asignación de VLAN y de puertos.

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

Tabla 3. Enlaces troncales.

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

Situación.

En esta actividad, demostrará y reforzará su capacidad para implementar NAT, servidor de DHCP, RIPV2 y el routing entre VLAN, incluida la configuración de direcciones IP, las VLAN, los enlaces troncales y las subinterfaces. Todas las pruebas de alcance deben realizarse a través de ping unicamente.

DESCRIPCIÓN DE LAS ACTIVIDADES.

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

Primero antes de signar puertos a las VLANs le ponemos nombres a las VLANs así:

S2(vlan)#vlan 100 name laptops

VLAN 100 modified:

Name: laptops

S2(vlan)#vlan 200 name destops

VLAN 200 added:

Name: destops

S2(vlan)#exit

Después asignamos los puertos a las VLAN así:

S2(config)#interface f0/2

S2(config-if)#switchport mode access

S2(config-if)#switchport access vlan 100

S2(config-if)#end

S2(config)#interface f0/3

S2(config-if)#switchport mode access

S2(config-if)#switchport access vlan 100

S2(config-if)#end

S2(config)#interface f0/4

S2(config-if)#switchport mode access

S2(config-if)#switchport access vlan 200

S2(config-if)#end

S2(config)#interface f0/5

S2(config-if)#switchport mode access

S2(config-if)#switchport access vlan 200

S2(config-if)#end

Con el empleo del comando show vlan observamos lo que se ha configurado hasta el momento.

S2>enable

S2#show vlan

VLAN Name Status Ports

---- -------------------------------- --------- -------------------------------

1 default active Fa0/1, Fa0/6, Fa0/7, Fa0/8

Fa0/9, Fa0/10, Fa0/11, Fa0/12

Fa0/13, Fa0/14, Fa0/15, Fa0/16

Fa0/17, Fa0/18, Fa0/19, Fa0/20

Fa0/21, Fa0/22, Fa0/23, Fa0/24

100 laptops active Fa0/2, Fa0/3

200 destops active Fa0/4, Fa0/5

1002 fddi-default act/unsup

1003 token-ring-default act/unsup

1004 fddinet-default act/unsup

1005 trnet-default act/unsup

VLAN Type SAID MTU Parent RingNo BridgeNo Stp BrdgMode Trans1 Trans2

---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------

1 enet 100001 1500 - - - - - 0 0

100 enet 100100 1500 - - - - - 0 0

200 enet 100200 1500 - - - - - 0 0

1002 fddi 101002 1500 - - - - - 0 0

1003 tr 101003 1500 - - - - - 0 0

1004 fdnet 101004 1500 - - - ieee - 0 0

1005 trnet 101005 1500 - - - ibm - 0 0

Remote SPAN VLANs

Primary Secondary Type Ports

------- --------- ----------------- --

S2#

Configuración de puertos en el S3.

S3(config)#interface range f0/1-24

S3(config-if-range)#switchport mode access

S3(config-if-range)#switchport access vlan 1

S3(config-if-range)#end

Comprobamos configuración con el comando show vlan.

S3#show vlan

VLAN Name Status Ports

---- -------------------------------- --------- -------------------------------

1 default active Fa0/1, Fa0/2, Fa0/3, Fa0/4

Fa0/5, Fa0/6, Fa0/7, Fa0/8

Fa0/9, Fa0/10, Fa0/11, Fa0/12

Fa0/13, Fa0/14, Fa0/15, Fa0/16

Fa0/17, Fa0/18, Fa0/19, Fa0/20

Fa0/21, Fa0/22, Fa0/23, Fa0/24

1002 fddi-default act/unsup

1003 token-ring-default act/unsup

1004 fddinet-default act/unsup

1005 trnet-default act/unsup

VLAN Type SAID MTU Parent RingNo BridgeNo Stp BrdgMode Trans1 Trans2

---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------

1 enet 100001 1500 - - - - - 0 0

1002 fddi 101002 1500 - - - - - 0 0

1003 tr 101003 1500 - - - - - 0 0

1004 fdnet 101004 1500 - - - ieee - 0 0

1005 trnet 101005 1500 - - - ibm - 0 0

Remote SPAN VLANs

Primary Secondary Type Ports

------- --------- ---------- ----------

S3#

Los puertos de red que no se utilizan se deben deshabilitar.

Deshabilitar en S2.

S2>enable

S2#config ter

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

S2(config)#interface range f0/6-24

S2(config-if-range)#shutdown

%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/7, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/8, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/9, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/10, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/11, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/12, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/13, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/14, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/15, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/16, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/17, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/18, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/19, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/20, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/21, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/22, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/23, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/24, changed state to administratively down

S2(config-if-range)#

Deshabilitar en S3.

S3>enable

S3#confi ter

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

S3(config)#interface range f0/7-24

S3(config-if-range)#shutd

S3(config-if-range)#shutdown

%LINK-5-CHANGED: Interface FastEthernet0/7, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/8, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/9, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/10, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/11, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/12, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/13, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/14, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/15, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/16, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/17, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/18, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/19, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/20, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/21, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/22, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/23, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/24, changed state to administratively down

S3(config-if-range)#exit

Configuración de troncales en el S2.

S2#

S2#configure terminal

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

S2(config)#interface range f0/2-3

S2(config-if-range)#switchport mode trunk

S2(config-if-range)#

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up

S2(config-if-range)#end

S2#

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

Configuración de IP al ISP.

Router>enable

Router#config terminal

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

Router(config)#hostname ISP

ISP(config)#interface s0/0/0

ISP(config-if)#ip address 200.123.211.1 255.255.255.0

ISP(config-if)#no shut

ISP(config-if)#no shutdown

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

ISP(config-if)#

Configuración de IP al R1.

Router>enable

Router#configure ter

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

Router(config)#hostname R1

R1(config)# service password-encryption

R1(config)#interface s0/0/0

R1(config-if)#ip address 200.123.211.2 255.255.255.0

R1(config-if)# clock rate 128000

R1(config-if)#no shutd

R1(config-if)#no shutdown

R1(config-if)#

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

R1(config-if)#no shutd

R1(config-if)#no shutdown

R1(config-if)#

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

R1(config)#interface s0/1/0

R1(config-if)#ip address 10.0.0.1 255.255.255.252

R1(config-if)#clock rate 128000

This command applies only to DCE interfaces

R1(config-if)#no shutd

R1(config-if)#no shutdown

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

R1(config)#interface s0/1/1

R1(config-if)#ip address 10.0.0.5 255.255.255.252

R1(config-if)#clock rate 128000

This command applies only to DCE interfaces

R1(config-if)#no shutdown

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

R1(config-if)#exit

R1(config)#exit

R1#

%SYS-5-CONFIG_I: Configured from console by console

R1#wr

Building configuration...

[OK]

Configuración de IP al R2.

Router>enable

Router#conf ter

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

Router(config)#hostname R2

R2(config)#interface s0/0/0

R2(config-if)#ip address 10.0.0.2 255.255.255.252

R2(config-if)#clock rate 128000

R2(config-if)#no shutd

R2(config-if)#no shutdown

R2(config-if)#

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

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

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

R2(config-if)#ip address 10.0.0.9 255.255.255.252

R2(config-if)#clock rate 128000

R2(config-if)#no shutdown

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

R2(config-if)#exit

R2(config)#

Configuración de IP al R3.

Router>enable

Router#conf ter

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

Router(config)#hostname R3

R3(config)#interface f0/0

R3(config-if)#ip address 192.168.30.1 255.255.255.0

R3(config-if)#no shutd

R3(config-if)#no shutdown

R3(config-if)#

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

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

R3(config-if)#ip address 10.0.0.6 255.255.255.252

R3(config-if)#clock rate 128000

R3(config-if)#no shutd

R3(config-if)#no shutdown

R3(config-if)#

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

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

R3(config-if)#interface s0/0/1

R3(config-if)#ip address 10.0.0.9 255.255.255.252

R3(config-if)#clock rate 128000

This command applies only to DCE interfaces

R3(config-if)#no shutdown

R3(config-if)#

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

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up

R3(config-if)#

R3#wr

Building configuration...

[OK]

R3#

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

Información IPv4 del servidor DHCP de Laptop20.

Damos clic al círculo DHCP para activarlo

IP Address: **169.254.222.86**
Mascara de subred: **255.255.0.0**
Gateway predeterminado: **0.0.0.0**

Información IPv4 del servidor DHCP de Laptop21.

IP Address: **169.254.9.12**
Mascara de subred: **255.255.0.0**
Gateway predeterminado: **0.0.0.0**

Información IPv4 del servidor DHCP de PC20.

IP Address: **169.254.152.153**
Mascara de subred: **255.255.0.0**
Gateway predeterminado: **0.0.0.0**

Información IPv4 del servidor DHCP de PC21.

IP Address: **169.254.235.125**
Mascara de subred: **255.255.0.0**
Gateway predeterminado: **0.0.0.0**

Información IPv4 del servidor DHCP de Laptop30.

IP Address: **169.254.28.231**
Mascara de subred: **255.255.0.0**
Gateway predeterminado: **0.0.0.0**

Información IPv4 del servidor DHCP de Laptop31.

IP Address: **169.254.145.34**
Mascara de subred: **255.255.0.0**
Gateway predeterminado: **0.0.0.0**

Información IPv4 del servidor DHCP de PC30.

IP Address: **169.254.4.106**
Mascara de subred: **255.255.0.0**
Gateway predeterminado: **0.0.0.0**

Información IPv4 del servidor DHCP de PC31.

IP Address: **169.254.200.20**
Mascara de subred: **255.255.0.0**
Gateway predeterminado: **0.0.0.0**

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.

R1>enable

```
R1#configure ter
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#interface s0/1/1
R1(config-if)#ip nat inside
R1(config-if)#exit
R1(config)#interface s0/1/0
R1(config-if)#ip nat inside
R1(config-if)#exit
R1(config)#interface 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)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#wr
Building configuration...
[OK]
R1#
```

Con el uso del comando **show ip nat translations** verificamos TCP.

R1#show ip nat translations

Pro Inside global Inside local Outside local Outside global

tcp 200.123.211.1:80 192.168.30.6:80 --- ---

Con el comando **show ip nat statistics** verificamos la ruta estática y las interfaces de salida

R1#show ip nat statistics

Total translations: 1 (1 static, 0 dynamic, 1 extended)

Outside Interfaces: Serial0/0/0

Inside Interfaces: Serial0/1/0 , Serial0/1/1

Hits: 0 Misses: 0

Expired translations: 0

Dynamic mappings:

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

R1#conf ter

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

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)#exit

R1#

%SYS-5-CONFIG_I: Configured from console by console

R1#wr

Building configuration...

[OK]

R1#

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

R2>enable

R2#conf ter

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

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

% Incomplete command.

R2(dhcp-config)#dns-server 0.0.0.0

R2(dhcp-config)#exit

R2(config)#exit

R2#

%SYS-5-CONFIG_I: Configured from console by console

R2#wr

Building configuration...

[OK]

R2#

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

R2#conf ter

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

R2(config)#interface vlan 100

R2(config-if)#ip address 192.168.20.1 255.255.255.0

R2(config-if)#ip address 192.168.20.1 255.255.255.0

R2(config-if)#exit

R2(config)#interface vlan 200

R2(config-if)#ip address 192.168.21.1 255.255.255.0

R2(config-if)#exit

R2(config)#exit

R2#

%SYS-5-CONFIG_I: Configured from console by console

R2#wr

Building configuration...

[OK]

R2#

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

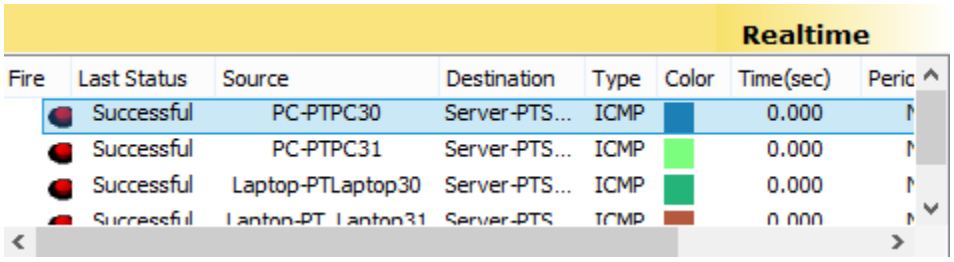


Figura 2. Ping para dispositivos en R3

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.

Figura 3. DHCP y DHCPv6 Laptop30.

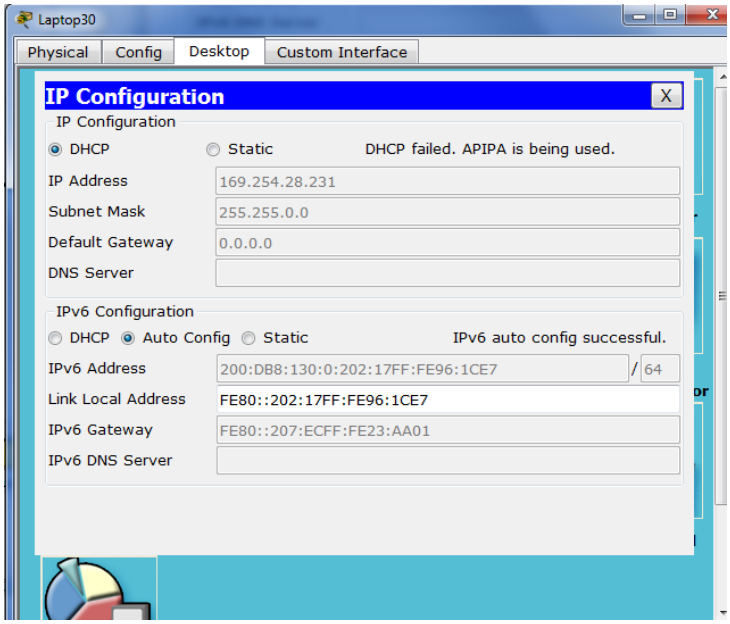


Figura 4. DHCP y DHCPv6 PC30.

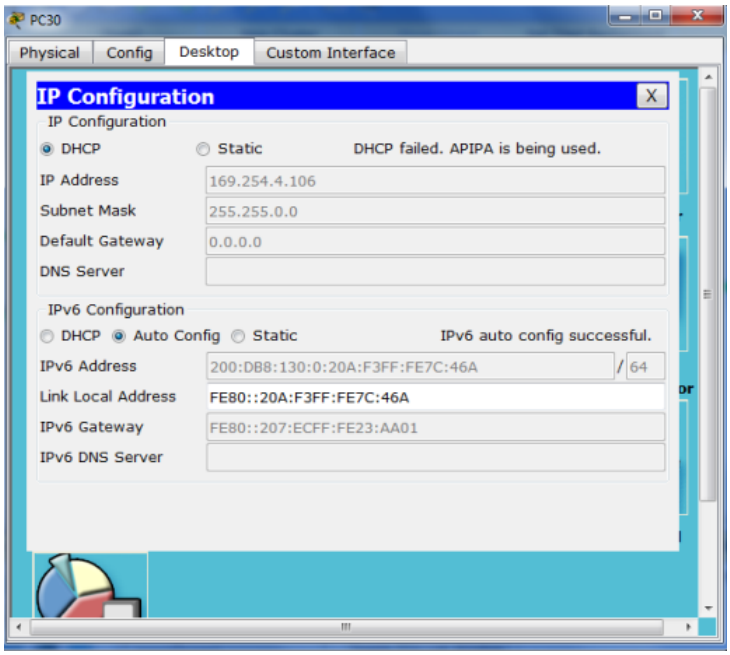


Figura 5. DHCP y DHCPv6 Laptop31.

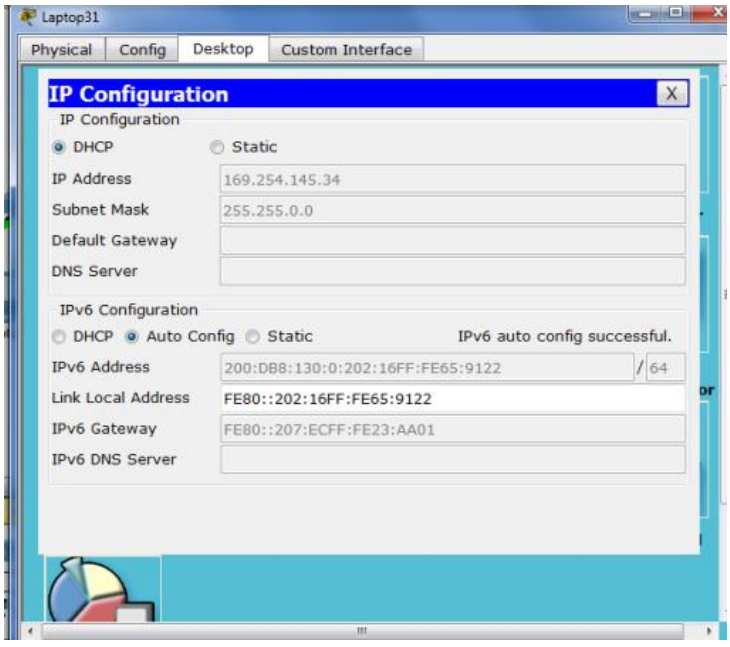
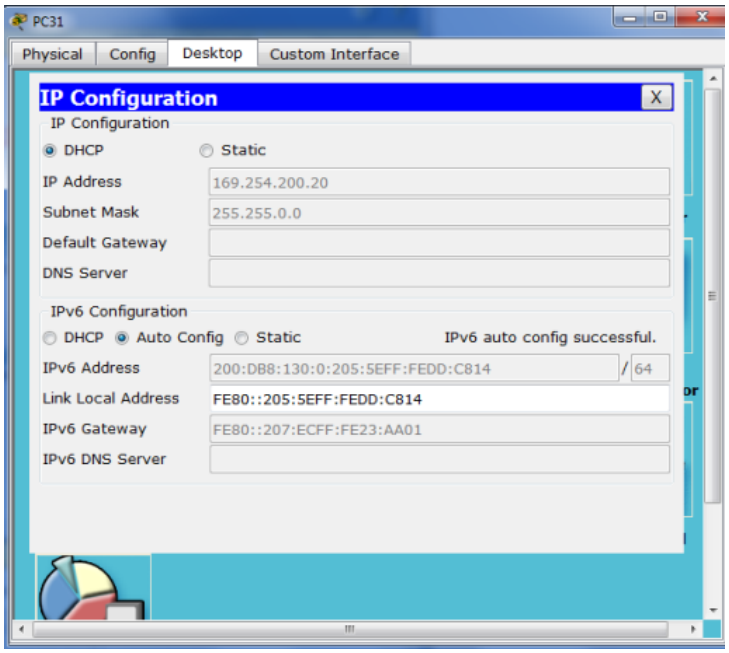


Figura 6. DHCP y DHCPv6 PC31.



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

R3>enable

R3#confi ter

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

R3(config)#ipv6 unicast-routing

R3(config)#interface f0/0

R3(config-if)#ip address 192.168.30.1 255.255.255.0

R3(config-if)#ip address 2001:db8::9C0:80F:301/64

R3(config-if)#ipv6 address 2001:db8::9C0:80F:301/64

R3(config-if)#no shutd

R3(config-if)#no shutdown

R3(config-if)#exit

R3(config)#exit

R3#

%SYS-5-CONFIG_I: Configured from console by console

R3#wr

Building configuration...

[OK]

R3#

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

R1.

R1>enable

R1#conf ter

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

R1(config)#router rip

R1(config-router)#version 2

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

C 10.0.0.0/30 is directly connected, Serial0/1/0

C 10.0.0.4/30 is directly connected, Serial0/1/1

C 200.123.211.0/24 is directly connected, Serial0/0/0

R1(config-router)#network 10.0.0.0

R1(config-router)#network 10.0.0.4

R1(config-router)#end

R1#

%SYS-5-CONFIG_I: Configured from console by console

R1#wr

Building configuration...

[OK]

R1#

R2.

R2>enable

R2#conf ter

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

R2(config)#router rip

R2(config-router)#verson 2

^

% Invalid input detected at '^' marker.

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

C 10.0.0.0/30 is directly connected, Serial0/0/0

C 10.0.0.8/30 is directly connected, Serial0/0/1

R2(config-router)#end

R2#

%SYS-5-CONFIG_I: Configured from console by console

R2#wr

Building configuration...

[OK]

R2#

R3.

R3>enable

R3#conf ter

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

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)#end

R3#

%SYS-5-CONFIG_I: Configured from console by console

R3#show ip route connected

C 10.0.0.4/30 is directly connected, Serial0/0/0

C 10.0.0.8/30 is directly connected, Serial0/0/1

C 192.168.30.0/24 is directly connected, FastEthernet0/0

R3#wr

Building configuration...

[OK]

R3#

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

R1#show protocol

Global values:

Internet Protocol routing is enabled

FastEthernet0/0 is administratively down, line protocol is down

FastEthernet0/1 is administratively down, line protocol is down

Serial0/0/0 is up, line protocol is up

Internet address is 200.123.211.2/24

Serial0/0/1 is administratively down, line protocol is down

Serial0/1/0 is up, line protocol is up

Internet address is 10.0.0.1/30

Serial0/1/1 is up, line protocol is up

Internet address is 10.0.0.5/30

Vlan1 is administratively down, line protocol is down

R1#

- 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.

Figura 7. Ping del Server0 al R3

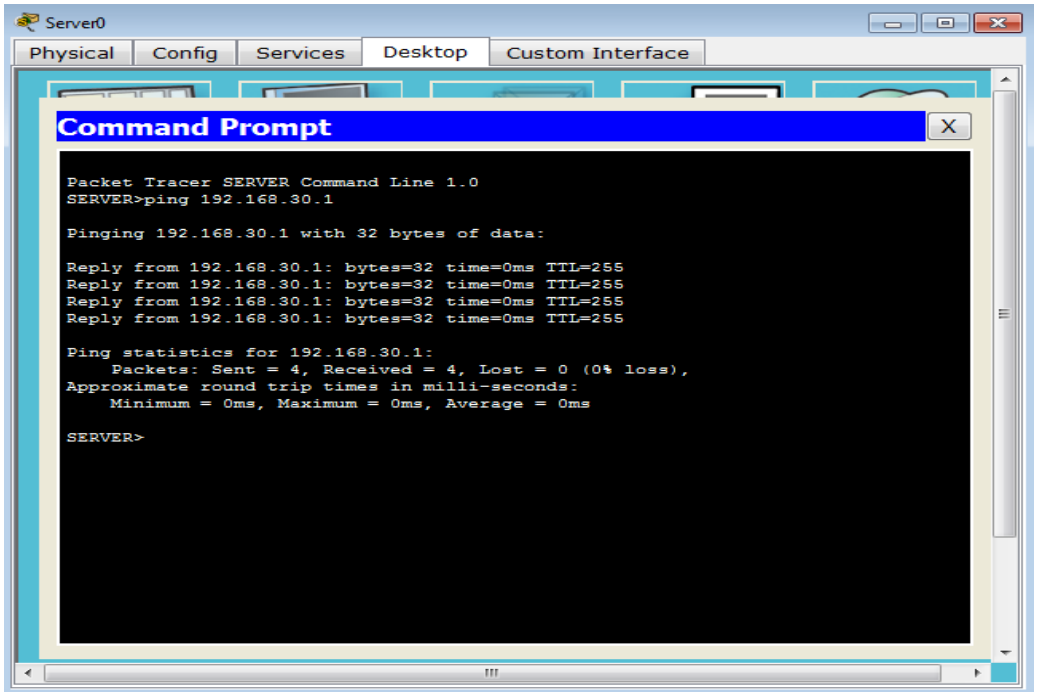
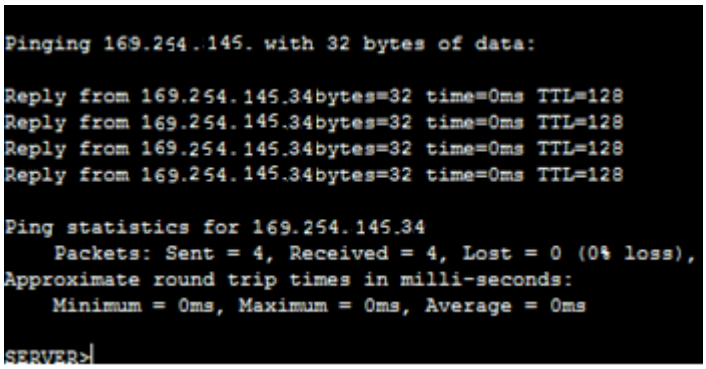


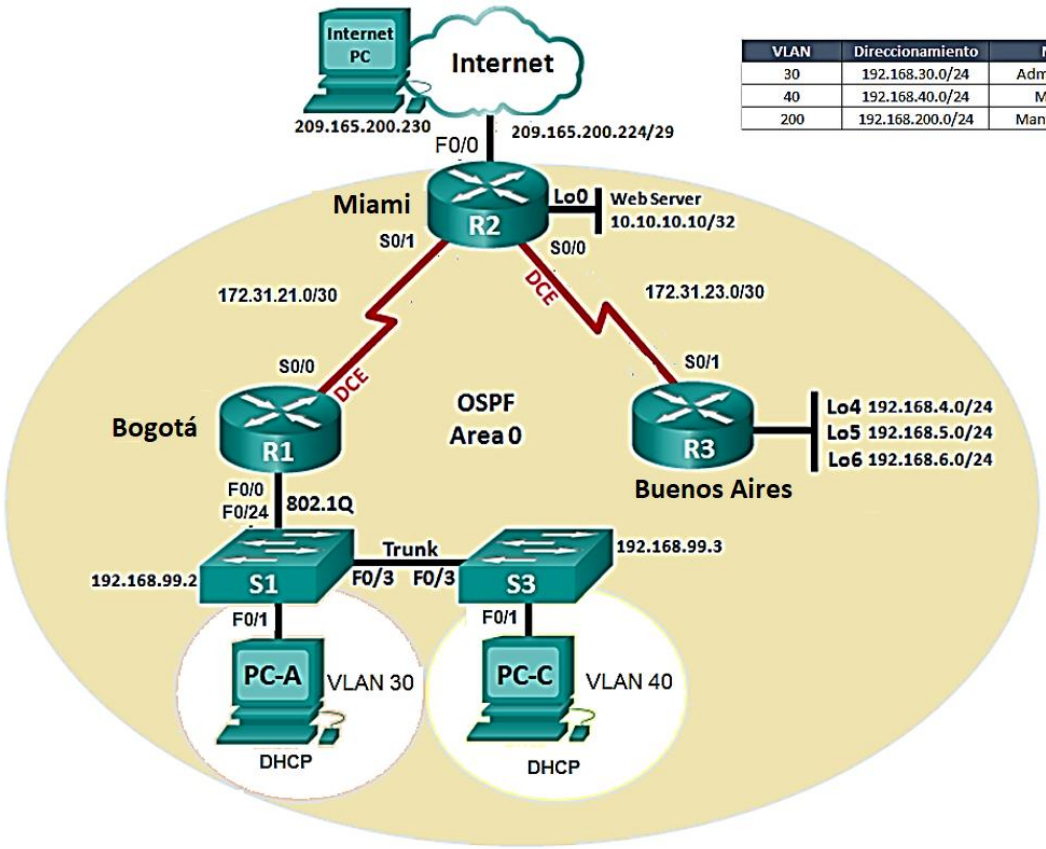
Figura 8. Ping del Server0 a la Laptop31


Pinging 169.254.145. with 32 bytes of data:
Reply from 169.254.145.34bytes=32 time=0ms TTL=128
Reply from 169.254.145.34bytes=32 time=0ms TTL=128
Reply from 169.254.145.34bytes=32 time=0ms TTL=128
Reply from 169.254.145.34bytes=32 time=0ms TTL=128
Ping statistics for 169.254.145.34
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
SERVER>

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.

Figura 9. 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

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

Primero que todo configuramos el direccionamiento de IP Internet y al server

IP address: 209.165.200.230

Mascara de subred: 255.255.255.248

Gateway predeterminado: 209.165.200.225

Web Server

Seleccionamos la configuración IP estática y configuramos lo siguiente:

IP address: 10.10.10.10

Mascara de subred: 255.255.255.0

Gateway predeterminado: 10.10.10.1

R1

Bogota-R1>enable

Bogota-R1#configure ter

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

Bogota-R1(config)#int s0/0/0

Bogota-R1(config-if)#description connection to Miami-R2

Bogota-R1(config-if)#ip address 172.31.21.2 255.255.255.252

Bogota-R1(config-if)#clock rate 128000

Bogota-R1(config-if)#no shu

Bogota-R1(config-if)#no shutdown

Bogota-R1(config-if)#

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

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

Bogota-R1(config-if)#

Bogota-R1(config-if)#exit

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

R1(config)#

R2

Miami-R2>enable

Miami-R2#configure ter

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

Miami-R2(config)#inter s0/0/1

Miami-R2(config-if)#descrip connection to Bogota-R1

Miami-R2(config-if)#ip address 172.31.23.1 255.255.255.252

Miami-R2(config-if)#no shutdown

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

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

Miami-R2(config-if)#descrip connection to BuenosAires-R3

Miami-R2(config-if)#ip add 172.31.23.1 255.255.255.252

Miami-R2(config-if)#clock rate 128000

Miami-R2(config-if)#no shutdown

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

Miami-R2(config-if)#int f0/0

Miami-R2(config-if)#descrip Internet PC

Miami-R2(config-if)#ip add 209.165.200.225 255.255.255.248

Miami-R2(config-if)#no shutdown

Miami-R2(config-if)#

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

Miami-R2(config-if)#int f0/1

Miami-R2(config-if)#ip address 10.10.10.1 255.255.255.0

Miami-R2(config-if)#no shutdown

Miami-R2(config-if)#

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

Miami-R2(config-if)#description connection to web server

Miami-R2(config-if)#exit

Miami-R2(config)#ip route 0.0.0.0 0.0.0.0 f0/0

Miami-R2(config)#

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

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

R3

BuenosAires-R3>enable

BuenosAires-R3#configure ter

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

BuenosAires-R3(config)#int s0/0/1

BuenosAires-R3(config-if)#description connection to Miami-R2

BuenosAires-R3(config-if)#ip address 172.31.23.2 255.255.255.252

BuenosAires-R3(config-if)#no shut

BuenosAires-R3(config-if)#no shutdown

BuenosAires-R3(config-if)#

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

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up

BuenosAires-R3(config-if)#int lo4

BuenosAires-R3(config-if)#

%LINK-5-CHANGED: Interface Loopback4, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback4, changed state to up

BuenosAires-R3(config-if)#ip address 192.168.4.1 255.255.255.0

BuenosAires-R3(config-if)#no shutdown

BuenosAires-R3(config-if)#int lo5

BuenosAires-R3(config-if)#

%LINK-5-CHANGED: Interface Loopback5, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback5, changed state to up

BuenosAires-R3(config-if)#ip add 192.168.5.1 255.255.255.0

BuenosAires-R3(config-if)#no shutdown

BuenosAires-R3(config-if)#int lo6

BuenosAires-R3(config-if)#

%LINK-5-CHANGED: Interface Loopback6, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback6, changed state to up

BuenosAires-R3(config-if)#ip add 192.168.6.1 255.255.255.0

BuenosAires-R3(config-if)#exit

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

BuenosAires-R3(config)#

S1

Switch>enable

Switch#configure terminal

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

Switch(config)#no ip domain-lookup

Switch(config)#hostname S1

S1(config)#exit

S1#

%SYS-5-CONFIG_I: Configured from console by console

S3

Switch>enable

Switch#configure terminal

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

Switch(config)#no ip domain-lookup

Switch(config)#hostname S3

S3(config)#exit

S3#

%SYS-5-CONFIG_I: Configured from console by console

Configuración de ip de PC-A

Seleccionamos la configuración IP por DHCP y nos queda de la siguiente manera:

IP address: 169.254.139.60

Mascara de subred: 255.255.0.0

Gateway predeterminado: 0.0.0.0

Configuración de ip de PC-C

Seleccionamos la configuración IPpor DHCP y nos queda de la siguiente manera:

IP address: 169.254.236.160

Mascara de subred: 255.255.0.0

Gateway predeterminado: 0.0.0.0

Configurar el protocolo de enrutamiento OSPFv2 bajo los siguientes criterios:

Tabla 4. 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

Configuración de OSPF en el R1

Bogota-R1>enable

Bogota-R1#configure terminal

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

Bogota-R1(config)#router ospf 1

Bogota-R1(config-router)#router-id 1.1.1.1

Bogota-R1(config-router)#Reload or use "clear ip ospf process" command, for this to take effect

Bogota-R1(config-router)#no router-id 1.1.1.1

Bogota-R1(config-router)#router-id 1.1.1.1

Bogota-R1(config-router)#Reload or use "clear ip ospf process" command, for this to take effect

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

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

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

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

Bogota-R1(config-router)#passive-interface f0/0

Bogota-R1(config-router)#exit

Bogota-R1(config)#int s0/0/0

Bogota-R1(config-if)#bandwidth 256

Bogota-R1(config-if)#ip ospf cost 9500

Bogota-R1(config-if)#

Configuración en R2

Miami-R2>enable

Miami-R2#configure terminal

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

Miami-R2(config)#router ospf 1

Miami-R2(config-router)#router-id 5.5.5.5

Miami-R2(config-router)#network 172.31.21.0 0.0.0.3 area 0

Miami-R2(config-router)#

02:12:01: %OSPF-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/0/1 from LOADING to FULL, Loading Done

Miami-R2(config-router)#network 172.31.23.0 0.0.0.3 area 0

Miami-R2(config-router)#network 172.31.23.0 0.0.0.3 area 0

Miami-R2(config-router)#network 172.31.21.0 0.0.0.3 area 0

Miami-R2(config-router)#network 10.10.10.0 0.0.0.255 area 0

Miami-R2(config-router)#passive-interface f0/0

Miami-R2(config-router)#interface s0/0/0

Miami-R2(config-if)#bandwidth 256

Miami-2(config-if)#interface s0/0/1

Miami-R2(config-if)#bandwidth 256

Miami-R2(config-if)#interface s0/0/0

Miami-R2(config-if)#ip ospf cost 7500

Miami-R2(config-if)#

Configuración en R3

BuenosAires-R3>enable

BuenosAires-R3#configure terminal

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

BuenosAires-R3(config)#router ospf 1

BuenosAires-R3(config-router)#router-id 8.8.8.8

BuenosAires-R3(config-router)#network 172.31.23.0 0.0.0.3 area 0

BuenosAires-R3(config-router)#

02:25:30: %OSPF-5-ADJCHG: Process 1, Nbr 5.5.5.5 on Serial0/0/1 from LOADING to FULL, Loading Done

BuenosAires-R3(config-router)#network 192.168.4.0 0.0.0.255 area 0

BuenosAires-R3(config-router)#passive-interface lo4

BuenosAires-R3(config-router)#passive-interface lo5

BuenosAires-R3(config-router)#passive-interface lo6

BuenosAires-R3(config-router)#exit

BuenosAires-R3(config)#int s0/0/1

BuenosAires-R3(config-if)#bandwidth 256

BuenosAires-R3(config-if)#ip ospf cost 9500

BuenosAires-R3(config-if)#exit

Verificar información de OSPF

- Visualizar tablas de enrutamiento y routers conectados por OSPFv2

Miami-R2>enable

Miami-R2#show ip ospf neighbor

Neighbor ID Pri State Dead Time Address Interface

1.1.1.1 0 FULL/ - 00:00:30 172.31.21.1 Serial0/0/1

8.8.8.8 0 FULL/ - 00:00:39 172.31.23.2 Serial0/0/0

- Visualizar lista resumida de interfaces por OSPF en donde se ilustre el costo de cada interface

Para este paso se utiliza el comando **show ip ospf interface brief** pero este comando no es soportado por Packet tracert

Miami-R2#show ip ospf interface brief

^

% Invalid input detected at '^' marker.

- Visualizar el OSPF Process ID, Router ID, Address summarizations, Routing Networks, and passive interfaces configuradas en cada router.

Miami-R2#show ip protocols

Routing Protocol is "ospf 1"

Outgoing update filter list for all interfaces is not set

Incoming update filter list for all interfaces is not set

Router ID 5.5.5.5

Number of areas in this router is 1. 1 normal 0 stub 0 nssa

Maximum path: 4

Routing for Networks:

172.31.21.0 0.0.0.3 area 0

172.31.23.0 0.0.0.3 area 0

10.10.10.0 0.0.0.255 area 0

Passive Interface(s):

FastEthernet0/0

Routing Information Sources:

Gateway Distance Last Update

1.1.1.1 110 00:28:05

5.5.5.5 110 00:17:56

8.8.8.8 110 00:13:05

Distance: (default is 110)

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

Configuración de seguridad en Bogota-R1

Bogota-R1>enable

Bogota-R1#configure terminal

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

Bogota-R1(config)#enable secret class

Bogota-R1(config)#line con 0

Bogota-R1(config-line)#pass cisco

Bogota-R1(config-line)#login

Bogota-R1(config-line)#line vty 0 4

Bogota-R1(config-line)#pass cisco

Bogota-R1(config-line)#login

Bogota-R1(config-line)#exit

Bogota-R1(config)#service pass

Bogota-R1(config)#service password-encryption

Bogota-R1(config)#banner motd #Prohibido El Acceso No Autorizado#

Bogota-R1(config)# exit

Bogota-R1#copy running-config startup-config

Destination filename [startup-config]?

Building configuration...

[OK]

Configuración de Seguridad en el Miami-R2

Miami-R2>enable

Miami-R2#configure terminal

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

Miami-R2(config)#enable secret class

Miami-R2(config)#line con 0

Miami-R2(config-line)#pass cisco

Miami-R2(config-line)#login

Miami-R2(config-line)#line vty 0 4

Miami-R2(config-line)#pass cisco

Miami-R2(config-line)#login

Miami-R2(config-line)#exit

Miami-R2(config)#service password-encryption

Miami-R2(config)#banner motd #Prohibido El Acceso No Autorizado#

Miami-R2(config)#exit

Miami-R2#

%SYS-5-CONFIG_I: Configured from console by console

Miami-R2#copy running-config startup-config

Destination filename [startup-config]?

Building configuration...

[OK]

Configuración de seguridad en BuenosAires-R3

BuenosAires-R3>enable

BuenosAires-R3#configure terminal

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

BuenosAires-R3(config)#enable secret class

BuenosAires-R3(config)#line con 0

BuenosAires-R3(config-line)#pass cisco

BuenosAires-R3(config-line)#login

BuenosAires-R3(config-line)#exit

BuenosAires-R3(config)#service password-encryption

BuenosAires-R3(config)#banner motd #Prohibido El Acceso No Autorizado#

BuenosAires-R3(config)#exit

BuenosAires-R3#

%SYS-5-CONFIG_I: Configured from console by console

BuenosAires-R3#copy running-config startup-config

Destination filename [startup-config]?

Building configuration...

[OK]

Configuración de seguridad en S1

S1>enable

Password:

S1#configure terminal

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

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 password-encryption

S1(config)#banner motd #Prohibido El Acceso No Autorizado#

S1(config)#exit

S1#

%SYS-5-CONFIG_I: Configured from console by console

S1#copy running-config startup-config

Destination filename [startup-config]?

Building configuration...

[OK]

Configuración de seguridad en S3

S3>enable

S3#configure terminal

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

S3(config)#hostname S3

S3(config)#no ip domain-lookup

S3(config)#enable secret class

S3(config)#line con 0

S3(config-line)#pass cisco

S3(config-line)#login

S3(config-line)#line vty 0 4

S3(config-line)#pass cisco

S3(config-line)#login

S3(config-line)#exit

S3(config)#service password-encryption

S3(config)#banner motd #Prohibido El Acceso No Autorizado#

S3(config)#exit

S3#

%SYS-5-CONFIG_I: Configured from console by console

Configuración de vlan en S1

S1#configure terminal

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

S1(config)#no ip domain-lookup

S1(config)#vlan 30

S1(config-vlan)#name Administracion

S1(config-vlan)#vlan 40

S1(config-vlan)#name Mercadeo

S1(config-vlan)#vlan 200

S1(config-vlan)#name Mantenimiento

S1(config-vlan)#exit

S1(config)#int vlan 200

S1(config-if)#

%LINK-5-CHANGED: Interface Vlan200, changed state to up

S1(config-if)#ip address 192.168.200.2 255.255.255.0

S1(config-if)#no shut

S1(config-if)#exit

S1(config)#ip default-gateway 192.168.200.1

S1(config)#interface f0/3

S1(config-if)#switchport mode trunk

S1(config-if)#

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan200, changed state to up

S1(config-if)#switchport trunk native vlan 1

S1(config-if)#interface f0/24

S1(config-if)#switchport mode trunk

S1(config-if)#switchport trunk native vlan 1

S1(config-if)#interface range fa0/1-2, fa0/4-23, GigabitEthernet0/1-2

S1(config-if-range)#switchport mode access

S1(config-if-range)#interface fa0/1

S1(config-if)#switchport mode access

S1(config-if)#switchport access vlan 30

S1(config-if)#interface range fa0/2, fa0/4-23, GigabitEthernet0/1-2

S1(config-if-range)#no shutdown

Configuración vlan en S3

Prohibido El Acceso No Autorizado

User Access Verification

Password:

S3>enable

Password:

S3#configure terminal

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

S3(config)#hostname S3

S3(config)#no ip domain-lookup

S3(config)#vlan 30

S3(config-vlan)#name Administracion

S3(config-vlan)#vlan 40

S3(config-vlan)#name Mercadeo

S3(config-vlan)#vlan 200

S3(config-vlan)#name Mantenimiento

S3(config-vlan)#exit

S3(config)#int vlan 200

S3(config-if)#

%LINK-5-CHANGED: Interface Vlan200, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan200, changed state to up

S3(config-if)#ip address 192.168.200.3 255.255.255.0

S3(config-if)#no shutdown

S3(config-if)#exit

S3(config)#ip default-gateway 192.168.200.1

S3(config)#interface f0/3

S3(config-if)#switchport mode trunk

S3(config-if)#switchport trunk native vlan 1

S3(config-if)#interface range fa0/1-2, fa0/4-24, GigabitEthernet0/1-2

S3(config-if-range)#switchport mode access

S3(config-if-range)#interface fa0/1

S3(config-if)#switchport mode access

S3(config-if)#switchport access vlan 40

S3(config-if)#

S3(config-if)#interface range fa0/2, fa0/4-24, GigabitEthernet0/1-2

S3(config-if-range)#shutdown

En el Switch 3 deshabilitar DNS lookup

S3#configure terminal

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

S3(config)#no ip domain-lookup

S3(config)#exit

S3#

%SYS-5-CONFIG_I: Configured from console by console

Asignar direcciones IP a los Switches acorde a los lineamientos.

Configuración de direcciones IP en S1

S1#configure terminal

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

S1(config)#int vlan 200

S1(config-if)#ip address 192.168.200.2 255.255.255.0

S1(config-if)#no shutdown

S1(config-if)#exit

S1(config)#ip default-gateway 192.168.200.1

Configuración de direcciones IP en S3

Prohibido El Acceso No Autorizado

User Access Verification

Password:

S3>enable

Password:

S3#configure terminal

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

S3(config)#int vlan 200

S3(config-if)#ip address 192.168.200.3 255.255.255.0

S3(config-if)#no shutdown

S3(config-if)#exit

S3(config)#ip default-gateway 192.168.200.1

S3(config)#

Desactivar todas las interfaces que no sean utilizadas en el esquema de red.

Desactivar interfaces en S1

S1#configure terminal

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

S1(config)#

S1(config)#interface range fa0/1-2, fa0/4-23, GigabitEthernet0/1-2

S1(config-if-range)#switchport mode access

S1(config-if-range)#interface fa0/1

S1(config-if)#switchport mode access

S1(config-if)#switchport access vlan 30

S1(config-if)#interface range fa0/2, fa0/4-23, GigabitEthernet0/1-2

S1(config-if-range)#shutdown

S1(config-if-range)#

Desactivar interfaces en S3

S3>enable

Password:

S3#configure terminal

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

S3(config)#int vlan 200

S3(config-if)#ip address 192.168.200.3 255.255.255.0

S3(config-if)#no shutdown

S3(config-if)#exit

S3(config)#ip default-gateway 192.168.200.1

S3(config)#

S3(config)#interface range fa0/1-2, fa0/4-24, GigabitEthernet0/1-2

S3(config-if-range)#switchport mode access

S3(config-if-range)#int fa0/1

S3(config-if)#switchport mode access

S3(config-if)#switchport access vlan 40

S3(config-if)#interface range fa0/2, fa0/4-24, GigabitEthernet0/1-2

S3(config-if-range)#shutdown

S3(config-if-range)#

Implement DHCP and NAT for IPv4

Configuración para Bogota-R1

Bogota-R1#configure terminal

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

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

Bogota-R1(config)#ip dhcp pool Administracion

Bogota-R1(dhcp-config)#network 192.168.30.0 255.255.255.0

Bogota-R1(dhcp-config)#default-router 192.168.30.1

Bogota-R1(dhcp-config)#dns-server 10.10.10.11

Bogota-R1(dhcp-config)#end

Bogota-R1#

%SYS-5-CONFIG_I: Configured from console by console

Bogota-R1#enable

Bogota-R1#configure terminal

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

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

Bogota-R1(config)#ip dhcp pool Mercadeo

Bogota-R1(dhcp-config)#network 192.168.40.0 255.255.255.0

Bogota-R1(dhcp-config)#default-router 192.168.40.1

Bogota-R1(dhcp-config)#dns-server 10.10.10.11

Bogota-R1(dhcp-config)#end

Bogota-R1#

%SYS-5-CONFIG_I: Configured from console by console

Configurar R1 como servidor DHCP para las VLANs 30 y 40.

Bogota-R1#configure terminal

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

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

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

Bogota-R1(config)#ip dhcp pool ADMINISTRACION

Bogota-R1(dhcp-config)#dns-server 10.10.10.11

Bogota-R1(dhcp-config)#default-router 192.168.30.1

Bogota-R1(dhcp-config)#network 192.168.30.0 255.255.255.0

Bogota-R1(dhcp-config)#exit

Bogota-R1(config)#exit

Reservar las primeras 30 direcciones IP de las VLAN 30 y 40 para configuraciones estáticas.

Tabla 5. Configuración DHCP

Configurar DHCP pool para VLAN 30	Name: ADMINISTRACION DNS-Server: 10.10.10.11 Domain-Name: ccna-unad.com Establecer default gateway.
Configurar DHCP pool para VLAN 40	Name: MERCADEO DNS-Server: 10.10.10.11 Domain-Name: ccna-unad.com Establecer default gateway.

Bogota-R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Bogota-R1(config)#ip dhcp excluded-address 192.168.31.1 192.168.31.30
Bogota-R1(config)#ip dhcp excluded-address 192.168.31.1 192.168.31.30
Bogota-R1(config)#no ip dhcp excluded-address 192.168.31.1 192.168.31.30
Bogota-R1(config)#ip dhcp excluded-address 192.168.30.1 192.168.30.30
Bogota-R1(config)#ip dhcp excluded-address 192.168.40.1 192.168.40.30
Bogota-R1(config)#ip dhcp pool Administracion
Bogota-R1(dhcp-config)#dns-server 10.10.10.11
Bogota-R1(dhcp-config)#default-router 192.168.30.1
Bogota-R1(dhcp-config)#network 192.168.30.0 255.255.255.0
Bogota-R1(dhcp-config)#ip dhcp pool Mercadeo
Bogota-R1(dhcp-config)#dns-server 10.10.10.11
Bogota-R1(dhcp-config)#default-router 192.168.40.1
Bogota-R1(dhcp-config)#network 192.168.40.0 255.255.255.0
R1(dhcp-config)#

Configurar NAT en R2 para permitir que los hosts puedan salir a internet

Miami-R2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Miami-R2(config)#access-list 1 permit 192.168.30.1 0.0.0.255
Miami-R2(config)#access-list 1 permit 192.168.40.1 0.0.0.255
Miami-R2(config)#no access-list 1 permit 192.168.30.1 0.0.0.255
Miami-R2(config)#no access-list 1 permit 192.168.40.1 0.0.0.255
Miami-R2(config)#access-list 1 permit 192.168.30.0 0.0.0.255
Miami-R2(config)#access-list 1 permit 192.168.40.0 0.0.0.255
Miami-R2(config)#access-list 1 permit 192.168.4.0 0.0.3.255

Miami-R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.248

Miami-R2(config)#ip nat inside source list 1 pool INTERNET

Miami-R2(config)#ip nat inside source static 10.10.10.10 209.165.200.229

Miami-R2(config)#

Configurar al menos dos listas de acceso de tipo estándar a su criterio en para restringir o permitir tráfico desde R1 o R3 hacia R2.

Miami-R2#configure terminal

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

Miami-R2(config)#access-list 101 permit tcp any host 209.165.200.229 eq www

Miami-R2(config)#access-list 101 permit icmp any any echo-reply

Miami-R2(config)#int f0/0

Miami-R2(config-if)#ip access-group 101 in

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

Miami-R2(config-if)#ip access-group 101 out

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

Miami-R2(config-if)#ip access-group 101 out

Miami-R2(config-if)#int f0/1

Miami-R2(config-if)#ip access-group 101 out

Miami-R2(config-if)#

Configurar al menos dos listas de acceso de tipo extendido o nombradas a su criterio en para restringir o permitir tráfico desde R1 o R3 hacia R2.

Miami-R2#configure terminal

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

Miami-R2(config)#ip nat inside source static 10.10.10.10 209.165.200.229

Miami-R2(config)#int f0/0

Miami-R2(config-if)#ip nat outside

Miami-R2(config-if)#int f0/1

Miami-R2(config-if)#ip nat inside

Miami-R2(config-if)#end

Miami-R2#

%SYS-5-CONFIG_I: Configured from console by console

Miami-R2#configure terminal

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

Miami-R2(config)#access-list 1 permit 192.168.30.0 0.0.0.255

Miami-R2(config)#access-list 1 permit 192.168.40.0 0.0.0.255

Miami-R2(config)#access-list 1 permit 192.168.4.0 0.0.3.255

Miami-R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.248

Miami-R2(config)#ip nat inside source list 1 pool INTERNET

Miami-R2(config)#

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

Figura 10. Ping de R1 a R2

```
R1#ping 172.31.21.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.31.21.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/5/22 ms
```

Figura 11. Ping de R2 A R3

```
R2#ping 172.31.23.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.31.23.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/11 ms
```

Figura 12. Web Server

```
SERVER>ping 209.165.200.225

Pinging 209.165.200.225 with 32 bytes of data:

Reply from 209.165.200.225: bytes=32 time=1ms TTL=255
Reply from 209.165.200.225: bytes=32 time=0ms TTL=255
Reply from 209.165.200.225: bytes=32 time=0ms TTL=255
Reply from 209.165.200.225: bytes=32 time=0ms TTL=255

Ping statistics for 209.165.200.225:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

SERVER>
```

CONCLUSIONES.

A pesar de los grandes inconvenientes que se nos presentan en la configuración de cada uno de los dispositivos finales e intermediarios de la práctica, se da lo mejor para cumplir con la actividad práctica, presentado errores que son difícil desarrollo, ya que un trabajo final no cuenta con un apoyo de tutores al frente, pero igual se hace lo mejor.

De acuerdo con los contenidos analizados en el diplomado, podemos conceptualizar con claridad el termino de red, que no es más que un conjunto de equipos (computadoras y/o dispositivos) conectados por medio de cables, señales, ondas o cualquier otro método de transporte de datos, que comparten información

Después de configurar varias veces y varios días cada uno de los dispositivos tanto intermediarios como finales de cada uno de los escenarios, se logra realizar la actividad completa, pero con uno que otro error en la configuración, logrando obtener un nivel bueno en la práctica del curso el cual es muy esencial en la vida futura del profesional del Ingeniero de Sistemas, se envía el Word con los dos escenarios y los PKA de los mismo, el escenario uno lleva 2 PKA, ya que configure dos veces pero solucione unos puntos que hacían falta en el otro.

La creación de diferentes VLAN en una red hace que el nivel de seguridad y productividad en una compañía crezcan.

BIBLIOGRAFIA.

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). 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). VLANs. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module3/index.html#3.0.1.1

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

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