Universidad Nacional Abierta y a Distancia

Solución de estudios de caso bajo el uso de tecnología CISCO

CAMILO EDUARDO MOEALES ARIZA

CODIGO: 80.098.024

TUTOR: EFRAÍN ALEJANDRO PEREZ

DIRECTOR: JUAN CARLOS VESGA

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

Universidad Nacional Abierta A Distancia – UNAD

Escuela De Ciencias Básicas Tecnología e Ingeniería – ECBTI

Bogotá noviembre de 2018

Universidad Nacional Abierta y a Distancia

RESUMEN

El objetivo del trabajo es demostrar las habilidades que se adquirieron durante el desarrollo del diplomado de profundización CCNA, el esenario numero uno se busca demostrará y reforzará la capacidad del estudiante para implementar NAT, servidor de DHCP, RIPV2 y el routing entre VLAN,.

En el escenario dos, se entrega una topología distribuida en las ciudades de Bogotá, Buenos Aires y Miami, donde se debe configurar e interconectar entre sí cada uno de los dispositivos de red.

Para esto se lleva a cabo la configuración de protocolos de enrutamiento dinámico OSPF V2 para interconectar los routers del escenario propuesto.

ABSTRACT

The objective of the work is to demonstrate the skills that were acquired during the development of the CCNA deepening diploma, the number one search engine will demonstrate and reinforce the student's ability to implement NAT, DHCP server, RIPV2 and VLAN routing.

In scenario two, a distributed topology is delivered in the cities of Bogotá, Buenos Aires and Miami, where each of the network devices must be configured and interconnected.

For this, the configuration of dynamic routing protocols OSPF V2 is carried out to interconnect the routers of the proposed scenario.

Universidad Nacional Abierta y a Distancia

TABLA DE CONTENIDO

Universidad Nacional Abierta y a Distancia

TABLA DE ILUSTRACIONES

INTRODUCCION

Durante el desarrollo del diplomado de profundización CCNA, se pudieron adquirir conocimientos y habilidades relacionadas con aspectos de Networking, estos se pondrán en práctica en el desarrollo de la actividad, donde es necesario configurar cada uno de los dispositivos de red los dos escenarios propuestos para interconectarlos entre sí, de acuerdo con las especificaciones establecidas para el direccionamiento IP, protocolos de enrutamiento y demás características que forman parte de la topología de red descrita en cada uno de los ejercicios.

El desarrollo de cada escenario propuesto se desarrolla sobre el programa Packet Tracer, en el cual se llevó a cabo cada una de las tareas propuestas, con el objetivo de demostrar las habilidades adquiridas durante el diplomado.

OBJETIVOS

General

Poner en práctica las habilidades prácticas, teóricas y experiencia, para identificar y aplicar una solución a un caso o situaciones expuestas en la guia

Específicos

- Realizar configuración básica de los dispositivos de comunicación Routers, Switch, Servidores.
- Implementar la configuración necesaria para la implementación de OPSFv2, protocolo dinámico de Routing.
- Implementar de DHCP y NAT en dispositivos de comunicación.
- Configurar y verificar listas de control de acceso ACL
- Verificar conectividad entre los dispositivos de una topología.
- Identificar que dispositivos se utilizan para la construcción de una topología de red.
- Implementar niveles de seguridad en Switch, elaboración de Vlans e inter Vlan Routing.

ESCENARIO 1

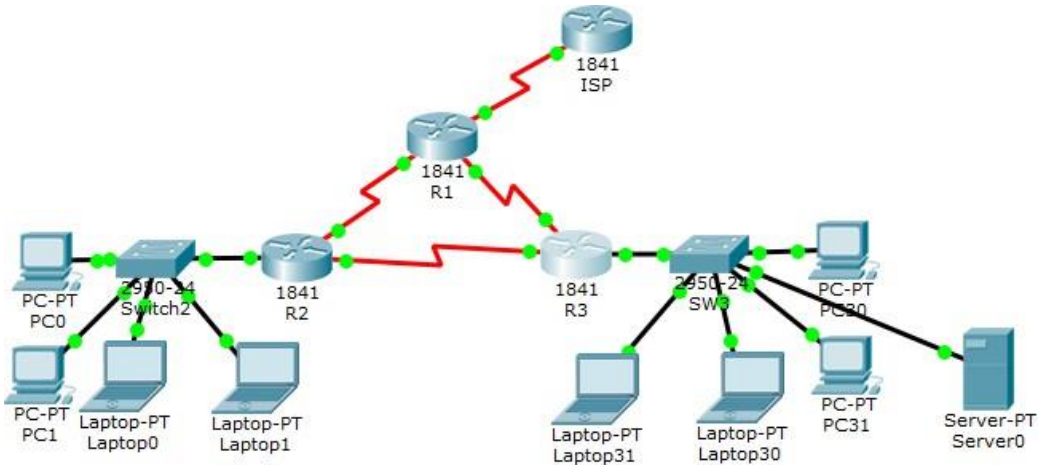


Ilustración 1 Topología

administrador	Interfaces	Dirección IP	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

Ilustración 2Tabla de direccionamiento

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

Ilustración 3Tabla de asignación de VLAN y de puertos

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

Ilustración 4Tabla de enlaces troncales

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 únicamente.

Descripción de las actividades

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

   ➢ Se ingresa a SW2 para configurar la vlan 100 y la vlan 200:

```
SW2>en
SW2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW2(config)#vlan 100
SW2(config-vlan)#name LAPTOPS
```

SW2(config-vlan)#exit
SW2(config)#vlan 200
SW2(config-vlan)#name DESTOPS

- Se ingresa a SW2 para configurar el rango de puertos

  SW2(config)#int range f0/2-3
  SW2(config-if-range)#switchport mode acces
  SW2(config-if-range)#switchport access vlan 100
  SW2(config)#int range f0/4-5
  SW2(config-if-range)#switchport mode acces
  SW2(config-if-range)#switchport access vlan 100
  SW2(config-if-range)#int f0/1

- Se ingresa a SW3 para configurar la vlan 1:

  SW3>en
  SW3#conf t
  Enter configuration commands, one per line. End with CNTL/Z.
  SW3(config)#vlan 1
  SW3(config-vlan)#exit
  SW3(config)#int range f0/1-24
  SW3(config-if-range)#switchport mode access
  SW3(config-if-range)#switchport access vlan 1

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

- Se ingresa a SW2 para deshabilitar los puertos del 6-24

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

- Se ingresa a SW3 para deshabilitar los puertos del 6-23

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

- Se ingresa a SW2 para dejar los puertos en modo trunk

  SW2(config)#int f0/1
  SW2(config-if)#switchport mode trunk

- Se ingresa a SW3 para dejar los puertos en modo trunk

  SW3(config)#int f0/1
  SW3(config-if)#switchport mode trunk

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

- Se ingresa a R2 para realizar la configuración del direccionamiento

```
R2#
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#int s0/0/0
R2(config-if)#ip address 10.0.0.2 255.255.255.252
R2(config-if)#exit
R2(config)#int s0/0/0
R2(config-if)#ip address 10.0.0.2 255.255.255.252
R2(config-if)#exit
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-if)#exit
R2(config)#int s0/0/1
R2(config-if)#ip address 10.0.0.9 255.255.255.252
```

- Se ingresa a R1 para realizar la configuración del direccionamiento

```
R1#
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
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
```

- Se ingresa a R3 para realizar la configuración del direccionamiento

```
R3>en
R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
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)#int s0/0/0
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
```

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

   - Ingresar al Laptop20 a la pestaña Desktop ye en la opción IP Configuración seleccionar DHCP.
   - Ingresar al Laptop21 a la pestaña Desktop ye en la opción IP Configuración seleccionar DHCP
   - Ingresar al PC20 a la pestaña Desktop ye en la opción IP Configuración seleccionar DHCP
   - Ingresar al PC21 a la pestaña Desktop ye en la opción IP Configuración seleccionar DHCP
   - Ingresar al Laptop30 a la pestaña Desktop ye en la opción IP Configuración seleccionar DHCP
   - Ingresar al Laptop31 a la pestaña Desktop ye en la opción IP Configuración seleccionar DHCP
   - Ingresar al PC30 a la pestaña Desktop ye en la opción IP Configuración seleccionar DHCP
   - Ingresar al PC31 a la pestaña Desktop ye en la opción IP Configuración seleccionar DHCP
   - Ingresar al Server0 a la pestaña Desktop ye en la opción IP Configuración seleccionar DHCP

4. 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.

   - Se ingresa a R1 para realizar la configuración del NAT

```
R1>en
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
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
```

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

   - Se ingresa a R1 para realizar la configuración del Dominio

```
R1(config)#router rip
R1(config-router)#version 2
R1(config-router)#network 10.0.0.0
```

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

   - Se ingresa a R2 para realizar la configuración de DHCP

```
R2>en
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
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%DHCPD-4-PING_CONFLICT: DHCP address
conflnetwork 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)#
```

7. R2 debe, además de enrutamiento a otras partes de la red, ruta entre las VLAN 100 y 200
   - Se ingresa a R2 para realizar la configuración de DHCP

```
R2#en
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#int vlan 100
R2(config-if)#ip address 192.168.20.1 255.255.255.0
% 192.168.20.0 overlaps with FastEthernet0/0.100
R2(config-if)#exit
R2(config)#int vlan 200
R2(config-if)#ip address 192.168.21.1 255.255.255.0
% 192.168.21.0 overlaps with FastEthernet0/0.200
R2(config-if)#
```

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

   - Ingresar al Server0 a la pestaña Desktop ye en la opción IPv6 Configuración seleccionar Autoconfig

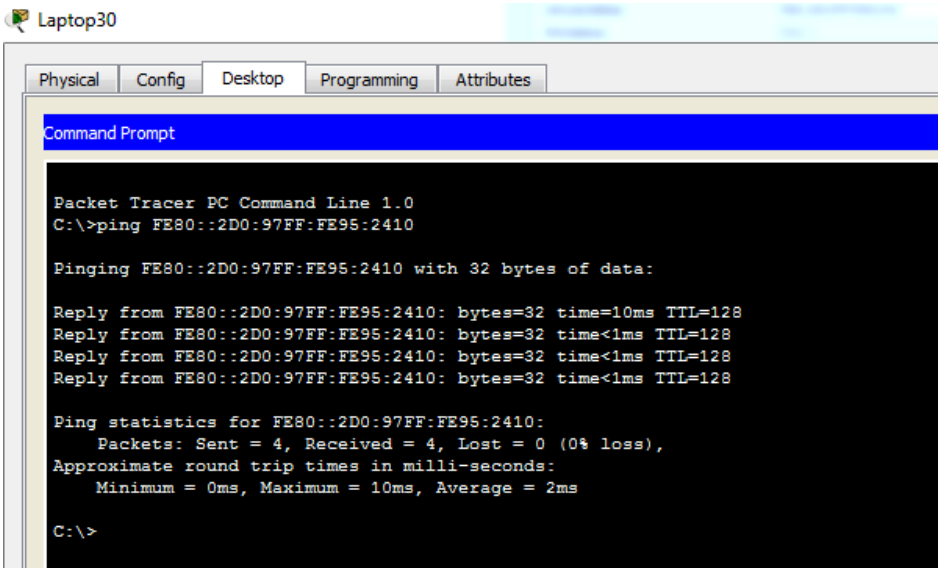


Ilustración 5 prueba de ping

9. 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.

   - Ingresar al Laptop30 a la pestaña Desktop ye en la opción IPv6 Configuración seleccionar Autoconfig
   - Ingresar al Laptop31 a la pestaña Desktop ye en la opción IPv6 Configuración seleccionar Autoconfig
   - Ingresar al PC30 a la pestaña Desktop ye en la opción IPv6 Configuración seleccionar Autoconfig
   - Ingresar al PC31 a la pestaña Desktop ye en la opción IPv6 Configuración seleccionar Autoconfig
   - Ingresar al Server0 a la pestaña Desktop ye en la opción IPv6 Configuración seleccionar Autoconfig

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

    - Se ingresa a R3 para realizar la configuración de DHCP

      ```
      R3>en
      R3#conf t
      Enter configuration commands, one per line. End with CNTL/Z.
      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:db8:130::9C0:80F:301/64
      R3(config-if)#shutdown
      R3(config-if)#
      %LINK-5-CHANGED: Interface FastEthernet0/0, changed state
      to administratively down
      %LINEPROTO-5-UPDOWN: Line protocol on Interface
      FastEthernet0/0, changed state to down
      R3(config-if)#
      ```

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

- Se ingresa a R1 para realizar la configuración del Roting RIP

```
R1>en
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#route rip
R1(config-router)#version 2
R1(config-router)#network 10.0.0.0
R1(config-router)#network 10.0.0.4
R1(config-router)#end
R1#
```

- Se ingresa a R2 para realizar la configuración del Roting RIP

```
R2>en
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
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)#end
R2#
```

- Se ingresa a R3 para realizar la configuración del Roting RIP

```
R3>en
R3#conf t
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#
```

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

- Se ingresa a R2 a la pestaña config -> RIP en la opción network adicionar la dirección 200.123.211.0
- Se ingresa a R3 a la pestaña config -> RIP en la opción network adicionar la dirección 200.123.211.0
- Se ingresa a R1 a la pestaña config -> RIP en la opción network adicionar la dirección 200.123.211.0

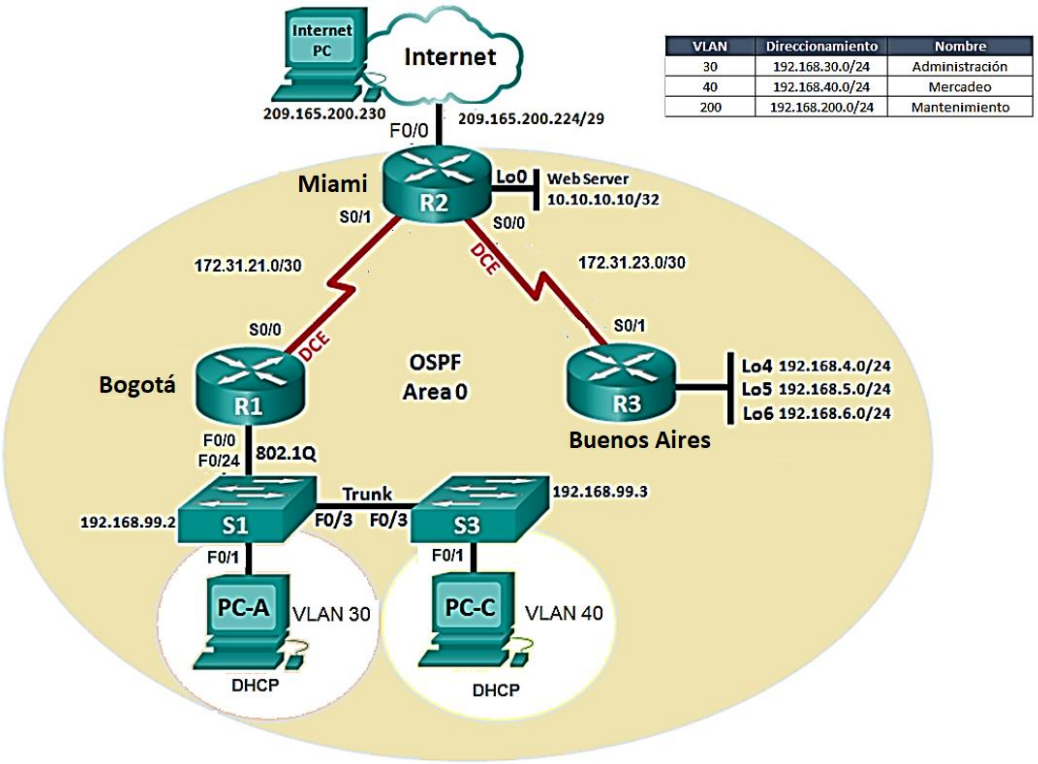
13. Verifique la conectividad. Todos los terminales deben poder hacer ping entre sí y a la dirección IP del ISP. Los terminales bajo el R3 deberían poder hacer IPv6-ping entre ellos y el servidor.

PDU List Window

Fire	Last Status	Source	Destination	Type
	Successful	Server0	PC31	ICMP
	Successful	Server0	Laptop30	ICMP
	Successful	Server0	Laptop31	ICMP
	Successful	Server0	PC30	ICMP
	Successful	Server0	R3	ICMP
	Successful	Server0	R1	ICMP
	Successful	Server0	ISP	ICMP
	Successful	R3	R2	ICMP
	Successful	R3	R1	ICMP
	Successful	R1	R2	ICMP
	Successful	PC21	R2	ICMP
	Successful	PC20	R2	ICMP
	Successful	Laptop21	R2	ICMP
	Failed	Laptop21	Server0	ICMP
	Failed	Laptop20	Server0	ICMP
	Failed	Laptop21	Server0	ICMP
	Failed	PC20	Server0	ICMP

Ilustración 6 Ping entre los equipos

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

Ilustración 5 Topología

Situación

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

Descripción de las actividades

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

   - Se ingresa a Internet-PC en la pestaña Dektop configurar en IP configuración:

Static

IP Address: 209.165.200.230

Subnet Mask 255.255.248

Default Gateway 209.165.200.225

- Se ingresa a PC-A y PC-C en la pestaña Dektop configurar en IP configuración:

  Habilitar la opción DHCP

- Se ingresa a R1 y se realiza la configuración de Nombre, seguridad y direccionamiento

```
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#Hostname Bogota
Bogota(config)#no ip domain-lookup
Bogota(config)#enable secret class
Bogota(config)#line con 0
Bogota(config-line)#password cisco
Bogota(config-line)#login
Bogota(config-line)#line vty 0 4
Bogota(config-line)#password cisco
Bogota(config-line)#login
Bogota(config-line)#exit
Bogota(config)#service password-encryption
Bogota(config)#banner motd $Prohibido Ingreso no Autorizado$
Bogota(config)#
Bogota(config)#int s0/0/0
Bogota(config-if)#ip address 172.31.21.1 255.255.255.0
Bogota(config-if)#clock rate 128000
Bogota(config-if)#no shutdown

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

- Se ingresa a R3 y se realiza la configuración de Nombre, seguridad y direccionamiento

```
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#Hostname Buenos-Aires
Buenos-Aires(config)#no ip domain-lookup
```

```
Buenos-Aires(config)#enable secret class
Buenos-Aires(config)#line con 0
Buenos-Aires(config-line)#password cisco
Buenos-Aires(config-line)#login
Buenos-Aires(config-line)#line vty 0 4
Buenos-Aires(config-line)#password cisco
Buenos-Aires(config-line)#login
Buenos-Aires(config-line)#exit
Buenos-Aires(config)#service password-encryption
Buenos-Aires(config)#banner motd $Prohibido Ingreso no
Autorizado$
Buenos-Aires(config)#
Buenos-Aires#

Buenos-Aires(config)#int s0/0/1

Buenos-Aires(config-if)#ip address 172.31.23.2
255.255.255.252
Buenos-Aires(config-if)#no shutdown

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

Buenos-Aires(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed state to up

Buenos-Aires(config-if)#
```

- Se ingresa a R3 y se realiza la configuración de **Loopback 4, Loopback 5, Loopback 6,**

```
Buenos-Aires(config-if)#int lo4

Buenos-Aires(config-if)#
%LINK-5-CHANGED: Interface Loopback4, changed state to
up

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

Buenos-Aires(config-if)#ip address 192.168.4.1
255.255.255.0
Buenos-Aires(config-if)#int lo5

Buenos-Aires(config-if)#
%LINK-5-CHANGED: Interface Loopback5, changed state to
up
```

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

Buenos-Aires(config-if)#ip address 192.168.5.1
255.255.255.0
Buenos-Aires(config-if)#int lo4
Buenos-Aires(config-if)#ip address 192.168.4.1
255.255.255.0
Buenos-Aires(config-if)#no shutdown
Buenos-Aires(config-if)#int lo5
Buenos-Aires(config-if)#ip address 192.168.5.1
255.255.255.0
Buenos-Aires(config-if)#no shutdown
Buenos-Aires(config-if)#int lo6

Buenos-Aires(config-if)#
%LINK-5-CHANGED: Interface Loopback6, changed state to
up

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

Buenos-Aires(config-if)#ip address 192.168.6.1
255.255.255.0
Buenos-Aires(config-if)#no shutdown
```

- Se ingresa a R2 y se realiza la configuración de Nombre, seguridad y direccionamiento

```
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#Hostname Miami
Miami(config)#no ip domain-lookup
Miami(config)#enable secret class
Miami(config)#line con 0
Miami(config-line)#password cisco
Miami(config-line)#login
Miami(config-line)#line vty 0 4
Miami(config-line)#password cisco
Miami(config-line)#login
Miami(config-line)#exit
Miami(config)#service password-encryption
Miami(config)#banner motd $Prohibido Ingreso no Autorizado$
Miami(config)#
```

```
Miami(config)#int s0/0/1
Miami(config-if)#ip address 172.31.23.1 255.255.255.252
Miami(config-if)#no shutdown
Miami(config-if)#exit
Miami(config)#int s0/0/0
Miami(config-if)#ip address 172.31.21.2 255.255.255.252
Miami(config-if)#no shutdown
Miami(config)#int f0/1
Miami(config-if)#int f0/0
Miami(config-if)#ip address 209.165.200.225 255.255.255.248
Miami(config-if)#no shutdown

Miami(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state
to up

Miami(config-if)#int f0/1
Miami(config-if)#ip address 10.10.10.10 255.255.255.0
Miami(config-if)#no shutdown

Miami(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(config-if)#

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

- Se ingresa a S1 y se realiza la configuración Seguridad:

```
S1>en
S1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#no ip domain-lookup
S1(config)#enable secret class
S1(config)#line con 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#exit
S1(config)#service password-encryption
```

S1(config)#banner motd $Prohibido Ingreso no Autorizado$
S1(config)#

2. Configurar el protocolo de enrutamiento OSPFv2 bajo los siguientes criterios:

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

Ilustración 6 OSPFv2 area 0

- Se ingresa a R1 para configurar el ospf

```
Bogota(config)#router ospf 1
Bogota(config-router)#router-id 1.1.1.1
Bogota(config-router)#network 172.31.21.0 0.0.0.3 area 0
Bogota(config-router)#network 192.168.30.0 0.0.0.3 area 0
Bogota(config-router)#network 192.168.40.0 0.0.0.3 area 0
Bogota(config-router)#network 192.168.30.0 0.0.0.255 area 0
Bogota(config-router)#network 192.168.40.0 0.0.0.255 area 0
Bogota(config-router)#network 192.168.200.0 0.0.0.255 area 0
Bogota(config-router)#passive-interface f0/0.30
Bogota(config-router)#passive-interface f0/0.40
Bogota(config-router)#passive-interface f0/0.200
Bogota(config-router)#
Bogota(config-router)#auto-cost reference-bandwidth 7500
% OSPF: Reference bandwidth is changed.
Please ensure reference bandwidth is consistent across all
routers.
Bogota(config-router)#exit
Bogota(config)#int s0/0/0
Bogota(config-if)#bandwidth 128
Bogota(config-if)#ip ospf cost 7500
Bogota(config-if)#
Bogota#
```

- Se ingresa a R2 para configurar el ospf

```
Miami>en
Miami#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Miami(config)#router ospf 1
Miami(config-router)#router-id 2.2.2.2
Miami(config-router)#network 172.31.21.0 0.0.0.3 area 0
Miami(config-router)#network 172.31.23.0 0.0.0.3 area 0
Miami(config-router)#network 10.10.10.0 0.0.0.255 area 0
Miami(config-router)#passive-interface f0/1
Miami(config-router)#auto-cost reference-bandwidth 7500
% OSPF: Reference bandwidth is changed.
Please ensure reference bandwidth is consistent across all
routers.
Miami(config-router)#exit
Miami(config)#int s0/0/0
Miami(config-if)#bandwidth 128
Miami(config-if)#int s0/0/1
Miami(config-if)#bandwidth 128
Miami(config-if)#ip ospf cost 7500
Miami(config-if)#exit
Miami(config)#
```

- Se ingresa a R3 para configurar el ospf

```
Buenos-Aires(config)#router ospf 1
Buenos-Aires(config-router)#router-id 3.3.3.3
Buenos-Aires(config-router)#network 172.31.23.0 0.0.0.3 area 0
Buenos-Aires(config-router)#network 192.168.4.0 0.0.3.255
area 0
Buenos-Aires(config-router)#passive-interface lo4
Buenos-Aires(config-router)#passive-interface lo5
Buenos-Aires(config-router)#passive-interface lo6
Buenos-Aires(config-router)#auto-cost reference-bandwidth
7500
% OSPF: Reference bandwidth is changed.
Please ensure reference bandwidth is consistent across all
routers.
Buenos-Aires(config-router)#exit
Buenos-Aires(config)#int s0/0/1
Buenos-Aires(config-if)#bandwidth 128
Buenos-Aires(config-if)#exit
Buenos-Aires(config)#
```

Verificar información de OSPF

- Visualizar tablas de enrutamiento y routers conectados por OSPFv2

```
Neighbor ID     Pri   State           Dead Time   Address         Interface
1.1.1.1           0   FULL/  -        00:00:39    172.31.21.1     Serial0/0/1
3.3.3.3           0   FULL/  -        00:00:34    172.31.23.2     Serial0/0/0
Bogota#
```

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

Miami#show ip ospf interface|

Serial0/0/0 is up, line protocol is up
Internet address is 172.31.21.2/30, Area 0
Process ID 1, Router ID 2.2.2.2, Network Type POINT-TO-POINT, Cost: 4857
Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
No designated router on this network
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:05
Index 1/1, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Suppress hello for 0 neighbor(s)
Serial0/0/1 is up, line protocol is up
Internet address is 172.31.23.1/30, Area 0
Process ID 1, Router ID 2.2.2.2, Network Type POINT-TO-POINT, Cost: 7500
Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
No designated router on this network
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:08
--More--

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

Miami#show running-config

```
router ospf 1
 router-id 2.2.2.2
 log-adjacency-changes
 passive-interface GigabitEthernet0/1
 auto-cost reference-bandwidth 7500
 network 172.31.21.0 0.0.0.3 area 0
 network 172.31.23.0 0.0.0.3 area 0
 network 10.10.10.0 0.0.0.255 area 0
```

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

- Se ingresa a S1 y se configuran los nombres de las VLAN según tabla

```
S1#en
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)#exit
S1(config)#vlan 40
S1(config-vlan)#name Mercadeo
S1(config-vlan)#exit
S1(config)#vlan 200
S1(config-vlan)#name mantenimiento
S1(config-vlan)#

S1(config)#int vlan 200
S1(config-if)#
%LINK-5-CHANGED: Interface Vlan200, changed state to up

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

S1(config-if)#ip address 192.168.99.2 255.255.255.0
S1(config-if)#exit
S1(config)#int vlan 200
S1(config-if)#ip default-gateway 192.168.99.1
```

- Se ingresa a S1 para configurar Mode Trunk y la Vlan nativa

```
S1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#int 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

S1(config-if)#switchport trunk native vlan 1
S1(config-if)#exit
S1(config)#int f0/24
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 1
S1(config-if)#no shutdown
```

- Se ingresa a S1 para configurar los Puertos en mod acces

```
S1(config)#int f0/24
S1(config-if)#switchport acces vlan 1
S1(config-if)#int range fa0/2, fa0/4-24, g0/1-2
S1(config-if-range)#exit
S1(config)#int f0/1
S1(config-if)#switchport acces vlan 30
S1(config-if)#int range fa0/2, fa0/4-24, g0/1-2
S1(config-if-range)#shutdown
```

- Se ingresa a S3 y se realiza la configuración Seguridad:

```
S3>en
S3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S3(config)#no ip domain-lookup
S3(config)#enable secret class
S3(config)#line con 0
S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#exit
Switch(config)#service password-encryption
S3(config)#banner motd $Prohibido Ingreso no Autorizado$
S3(config)#
S3(config)#int vlan 200
S3(config-if)#ip address 192.168.99.3 255.255.255.0
S3(config-if)#exit
S3(config)#ip default-gateway 192.168.99.1
S3(config)#
```

4. En el Switch 3 deshabilitar DNS lookup

```
S3>en
S3#conf t
Enter configuration commands, one per line. End with
CNTL/Z.
S3(config)#no ip domain-lookup
S3(config)#
```

5. Asignar direcciones IP a los Switches acorde a los lineamientos

```
S1(config-if)#ip address 192.168.99.2 255.255.255.0
S1(config-if)#exit
```

```
S3(config-if)#ip address 192.168.99.3 255.255.255.0
S3(config-if)#exit
```

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

```
S3(config-if)#int range fa0/2, fa0/4-24, g0/1-2
S3(config-if-range)#shutdown
```

```
S1(config-if)#int range fa0/2, fa0/4-24, g0/1-2
S1(config-if-range)#shutdown
```

7. Implement DHCP and NAT for IPv4
8. Configurar R1 como servidor DHCP para las VLANs 30 y 40
9. Reservar las primeras 30 direcciones IP de las VLAN 30 y 40 para configuraciones estáticas

- Ingresar al Router Bogota y realizar la configuracion de exclusión

```
Bogota>en
Bogota#conf t
Enter configuration commands, one per line. End with CNTL/Z.
```

Bogota(config)#ip dhcp excluded-address 192.168.30.1 192.168.30.30
Bogota(config)#ip dhcp excluded-address 192.168.40.1 192.168.40.30

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.

Ilustración 7 Tabla de Direcciones

- Ingresar al Router Bogota y realizar la configuración de VLAN 30

```
Bogota>en
Bogota#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Bogota(config)#ip dhcp pool ADMINISTRACION
Bogota(dhcp-config)#dns-server 10.10.10.11
Bogota(dhcp-config)#default-router 192.168.30.1
Bogota(dhcp-config)#network 192.168.30.0 255.255.255.0
Bogota(dhcp-config)#
Bogota#
```

- Ingresar al Router Bogota y realizar la configuración de VLAN 40

```
Bogota>en
Bogota#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Bogota(config)#ip dhcp pool MERCADEO
Bogota(dhcp-config)#dns-server 10.10.10.11
Bogota(dhcp-config)#default-router 192.168.40.1
Bogota(dhcp-config)#network 192.168.40.0 255.255.255.0
Bogota(dhcp-config)#
```

10. Configurar NAT en R2 para permitir que los host puedan salir a internet

- Ingresar al Router Bogota y realizar la configuración para la salida a internet

```
Bogota>en
Bogota#conf t
Enter configuration commands, one per line. End with
CNTL/Z.
Bogota(config)#user webuser privilege 15 secret Colombia10
Bogota(config)#ip http server
^
% Invalid input detected at '^' marker.
Bogota(config)#ip nat inside source static 10.10.10.10
209.165.200.229
Bogota(config)#int f0/0
Bogota(config-if)#ip nat outside
Bogota(config-if)#int f0/1
Bogota(config-if)#ip nat inside
Bogota(config-if)#exit
```

11. 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.

```
Bogota(config)#access-list 1 permit 192.168.30.0 0.0.0.255
Bogota(config)#access-list 1 permit 192.168.40.0 0.0.0.255
Bogota(config)#access-list 1 permit 192.168.4.0 0.0.3.255
Bogota(config)#ip nat pool INTERNET 209.165.200.225
209.165.200.229 NETMASK 255.255.255.248
Bogota(config)#
Bogota(config)#ip nat inside source list 1 pool INTERNET
Bogota(config)#ip access-list standard ADMIN_S
Bogota(config-std-nacl)#permit host 172.31.21.1
Bogota(config-std-nacl)#line vty 0 4
Bogota(config-line)#access-class ADMIN_S in
Bogota(config-line)#
Bogota#
```

12. 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.

```
Bogota(config)#access-list 101 permit tcp any host
209.165.200.229 eq www
Bogota(config)#access-list 101 permit icmp any any echo-
reply
```

```
Bogota(config)#int f0/0
Bogota(config-if)#ip access-group 101 in
Bogota(config-if)#int s0/0/0
Bogota(config-if)#ip access-group 101 out
Bogota(config-if)#int s0/0/1
Bogota(config-if)#ip access-group 101 out
Bogota(config-if)#int f0/1
Bogota(config-if)#ip access-group 101 out
Bogota(config-if)#
Bogota#
```

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

```
Bogota#show access-list
Standard IP access list 1
10 permit 192.168.30.0 0.0.0.255
20 permit 192.168.40.0 0.0.0.255
30 permit 192.168.4.0 0.0.3.255
Standard IP access list ADMIN_S
10 permit host 172.31.21.1
Extended IP access list 101
10 permit tcp any host 209.165.200.229 eq www
20 permit icmp any any echo-reply
Bogota#
```

Universidad Nacional Abierta y a Distancia

CONCLUCIONES

Este documento consolida las actividades prácticas finales en el desarrollo de cada módulo, de acuerdo a dos casos de estudio dados, uno para cada módulo, y se ha aplicado los conocimientos proporcionados en el material de apoyo emanado por la empresa CISCO en el desarrollo del aprendizaje autónomo promovido para este tipo de ambientes virtuales.

• Primero que todo, se desarrolló la planeación de cada red, de acuerdo a las pautas dadas, en el caso de estudio CCNA1, utilizando VLSM para división de las subredes y el protocolo RIPv2 como estándar para enrutamiento. Para el caso de estudio CCNA2 se requirió integrar los protocolos RIP, EIGRP y OSPF de acuerdo a las necesidades plasmadas por la empresa, haciendo la correspondiente subdivisión de redes correspondiente.

• Se logró una satisfactoria conexión, configuración y simulación de los dispositivos de las redes en los correspondientes casos de estudio.

• En general se expresa satisfacción por el aprendizaje adquirido durante el desarrollo del curso, y la aplicación de la teoría vista en la plataforma cisco para aplicar un correcto subneteo y enrutamiento en una red, que la profesión Ingeniería de sistemas requiere aplicar en todos los campos de la vida profesional real.

Universidad Nacional Abierta y a Distancia

REFERENCIA BIBLIOGRÁFICAS

- MANUAL DE DIVISION DE SUBREDES, Universidad Tecnológica de México, http://mbchavez.files.wordpress.com/2011/07/manual_de_subneteo .pdf
- SUBREDES Y EJERCICIOS http://hbeatriz.files.wordpress.com/2010/06/subredes-teoria-ejerciciosresueltos-sim_2008-09.pdf
- CONFIGURAR IP VERSIÓN 1 Y 2 http://www.garciagaston.com.ar/verpost.php?id_noticia=146 • CONFIGURACIÓN DE REDES CON EL PROTOCOLO EIGRP http://www.garciagaston.com.ar/index.php?tema=14
- USO DE PROCOLO OPSF EN ENRUTAMIENTO DINÁMICO http://www.garciagaston.com.ar/verpost.php?id_noticia=208
- VIDEO CREACION DE SUBREDES POR HOSTS http://www.youtube.com/watch?v=Acae2VrenVw&feature=related • VIDEO DE CURSO CCNA - SUBNETTING - CAPACITY - 1/4 (MODULO 3) http://www.youtube.com/watch?v=NiWRxcth6V4
- PLATAFORMA CISCO CCNA1 – CCNA2 https://auth.netacad.net/idp/Authn/NetacadLogin
- Ovas CCNA1 y CCNA2, plataforma UNAD. • Tutoriales de Packet Tracer http://www.cif.acuareladelsur.org/tutoriales/packet4.pdf