EXAMEN FINAL
PRUEBA FINAL DE HABILIDADES CCNA

LUIS GERARDO BURBANO MUÑOZ
CODIGO: 1.004.108.308

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
FACULTAD DE INGENIERIA DE SISTEMAS
SAN JUAN DE PASTO
2018

EXAMEN FINAL
PRUEBA FINAL DE HABILIDADES CCNA

LUIS GERARDO BURBANO MUÑOZ
CODIGO: 1.004.108.308

TRABAJO PRESENTADO AL TUTOR
Ing. JUAN CARLOS VESGA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
FACULTAD DE INGENIERIA DE SISTEMAS
SAN JUAN DE PASTO
2018

CONTENIDO

RESUMEN 4
INTRODUCCION 5
1. OBJETIVOS 6
1.1.1OBJETIVO GENERAL 6
1.1.1 OBJETIVOS ESPECIFICOS 6
1.2 PLANTEAMIENTO DEL PROBLEMA 7
1.2.1 PLANTEAMIENTO DEL PROBLEMA 7
1.2.2 JUSTIFICACIÓN 7
1.3 MARCO TEORICO 9
1.4 MATERIALES Y MÉTODOS 12
1.4.1 MATERIALES 12
1.4.2 METODOLOGÍA 12
1.5 DESARROLLO DEL PROYECTO 13
PREPARACIÓN 13
DIRECCIONAMIENTO IP 18
CONEXIÓN A LA NUBE 21
APLICACIÓN DEL PROTOCOLO OSPFV2 23
Verificación de configuración de OSPFv2 en los routers 26
CONFIGURACIÓN DE SWITCHES 31
INCORPORACIÓN DE DHCP Y TRADUCCIÓN DE REDES NAT EN LA TOPOLOGÍA 40
INCORPORACIÓN DE NAT EN R2 42
CREACIÓN DE LISTAS ACL 44
PRUEBAS DE CONECTIVIDAD 47
CONCLUSIONES 52
BIBLIOGRAFIA 53

RESUMEN

Como una de las pruebas para el trabajo final, se va a realizar un ejercicio que consiste en solucionar un problema que se presenta en una red. Utilizando diferentes herramientas, como un simulador de redes llamado Packet Tracer, se desarrolló una topología la cual debía cumplir una serie de condiciones para que el problema fuera resuelto. Se incorporaron diferentes conocimientos y procedimientos vistos en todo el curso de Cisco como DHCP, OSPFv2, tipos de enrutamiento y redes VLAN, así como hacer ping para que se pudieran probar las diferentes conexiones.

Palabras clave: Enrutamiento, DHCP, OSPFv2, VLAN, Switch, Router

INTRODUCCION

Luego de varios meses estudiando el curso de diplomado de profundización en redes CISCO y al haber estudiado cada uno de los procedimientos de la creación de las redes, ha llegado la hora de poner en práctica el conocimiento que se ha adquirido en todo el semestre. En el mundo moderno hay una enorme serie de retos a tomar en cuenta para la creación y administración de redes y siempre se busca una manera de aportar soluciones a diferentes problemas que se puedan presentar ya sean problemas físicos o lógicos.

Como trabajo final, se harán una serie de ejercicios y pruebas para demostrar los conocimientos que se han adquirido en todo el semestre, solucionando diferentes problemas de los más sencillos a los más complejos, demostrando que se cuenta con la capacidad para aplicar lo aprendido en el manejo de las redes

1. OBJETIVOS

1.1.1OBJETIVO GENERAL

- Demostrar los conocimientos adquiridos en el curso de Cisco mediante la resolución de un problema planteado

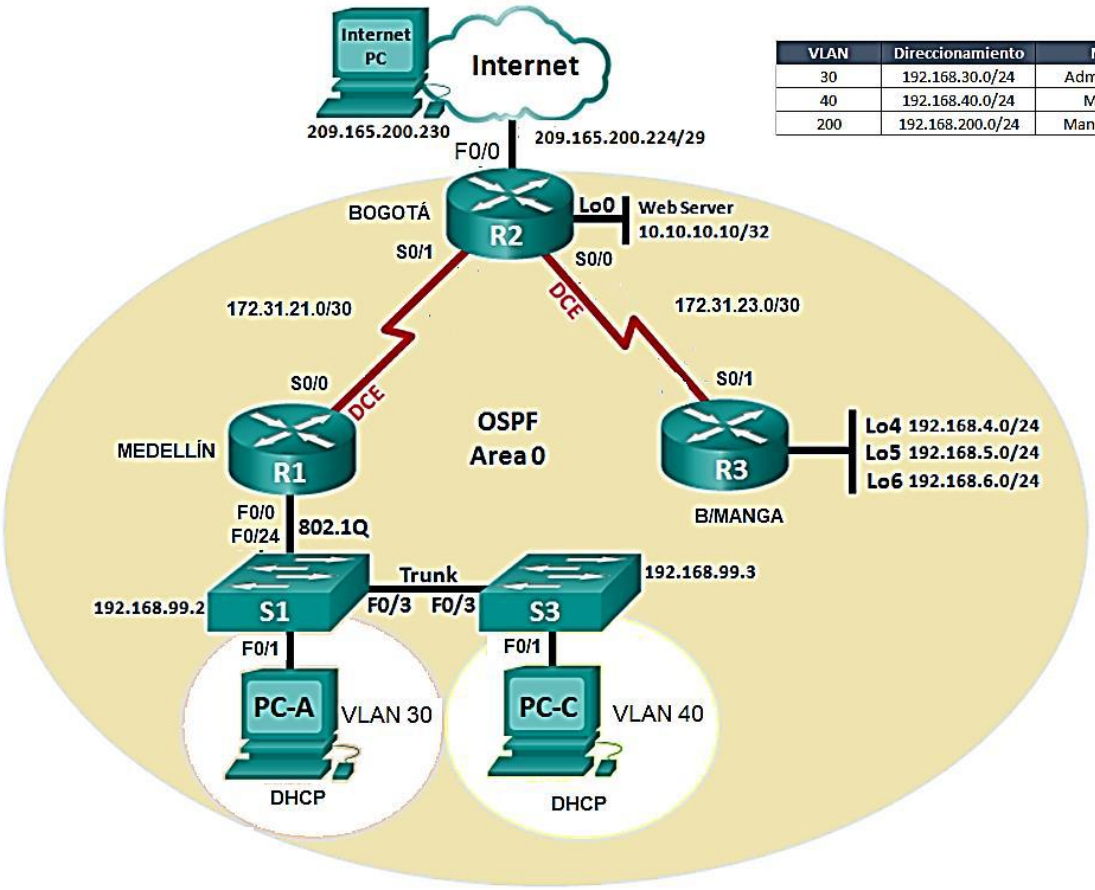
1.1.1 OBJETIVOS ESPECIFICOS

- Crear una red acorde a las condiciones preestablecidas
- Dar respuesta a las preguntas planteadas en la situación problemática

1.2 PLANTEAMIENTO DEL PROBLEMA

1.2.1 PLANTEAMIENTO DEL PROBLEMA

Una empresa de Tecnología posee tres sucursales distribuidas en las ciudades de Bogotá, Medellín y Bucaramanga, 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.



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

1.2.2 JUSTIFICACIÓN

Con los avances de la tecnología y la constante actualización, es importante mejorar los sistemas existentes para que los sistemas rindan de forma eficiente y no utilicen más recursos de los necesarios para resolver los problemas. Pero antes de

implementar las soluciones sería prudente realizar un diseño previo para evitar cualquier inconveniente que se presente si el diseño está mal configurado.

Para crear un buen diseño de la red, se utilizará un programa que simula la creación de redes y como estas son configuradas, llamado Packet Tracer. Packet Tracer permite diseñar redes e instalar todas las configuraciones posibles ya sean las direcciones IP o instalar los enrutamientos o los protocolos de seguridad. Se diseñará la red en el programa y se probarán los componentes antes de aplicar la solución en la vida real.

1.3 MARCO TEORICO

La red de la empresa con las diferentes sedes requiere la implementación de varios conocimientos que se han aprendido del curso de Cisco. Cada uno de los conceptos permitirá crear redes que permitan llevar a cabo sus labores de forma más eficiente y con tal motivo se explicarán los conceptos que se van a ejecutar para solucionar el problema planteado, entre los conceptos que van a aplicarse se encuentran los siguientes:

Para empezar, la red necesita la incorporación de VLAN. Una VLAN se trata de un grupo de puertos divididos en una LAN, aunque estos puertos están basados en la división lógica en lugar de la división física. Al dividir una red en diferentes segmentos de VLAN, se permite reducir los costos al reducir la necesidad de hacer actualizaciones costosas en cada sección. Permiten al personal de TI trabajar de forma más eficiente al brindar la posibilidad de identificar de manera más precisa los problemas que se pueden presentar al asignar un número y nombre a cada VLAN. Sin mencionar que los niveles de seguridad se incrementan al filtrar los datos que se permiten en cada sección.

Una vez se han creado las VLAN, debe realizarse un enrutamiento para permitir que los equipos puedan interactuar en la Red. Para permitir el enrutamiento entre VLAN se debe hacer un proceso de capa 3 para controlar el tráfico. Existen tres métodos de enrutamiento para las VLAN:

- El enrutamiento de VLAN antiguo que anteriormente se utilizaba mediante el uso de interfaces físicas a diferentes puertos del Switch. A cada interfaz se le asignaba una VLAN diferente.
- El enrutamiento con Router-on-a-stick permite al router dividir la interfaz en varias subinterfaces. Se utiliza como enlace troncal y se conecta a un switch en el enlace troncal.
- El enrutamiento en Switch multicapa el cual puede realizar funciones de capa 2 y capa 3 a reemplazar a los routers para la realización de esta función.

Por su puesto, para que la red funcione esta debe enrutarse. Los caminos que hay entre los routers debe tenerse muy claro para que no se pierdan los paquetes enviados y se aplicarán diferentes clases de rutas para que el paquete no se pierda si la distancia entre los routers es muy larga. Hay dos clases de formas de descubrir redes remotas:

- De forma manual al introducir rutas estáticas.
- De forma dinámica al establecer un protocolo

Las rutas estáticas se utilizan para las redes pequeñas si tienen una ruta a una red externa aunque pueden funcionar para las redes grandes para manejar un determinado tipo de tráfico. Por lo general es necesario utilizar tanto un tipo de enrutamiento como otro puesto que cada clase de enrutamiento tiene sus propias ventajas y desventajas.

OSPF es un protocolo de enrutamiento para reemplazar el protocolo de vector distancia RIP para realizar los procesos de escalabilidad. OSPF es un protocolo que se caracteriza por ser un protocolo sin clase, puede propagar los cambios de forma rápida y permite procesos de autenticación de síntesis de mensaje 5. OSPF establece una distancia administrativa acorde al origen de la ruta.

La conexión a internet requiere de una dirección IP. Por lo general, la asignación de direcciones no es una tarea sencilla debido a la cantidad de problemas que pueden presentarse si no se configuran de forma correcta, sin mencionar que podría llevar tiempo configurar cada IP de forma manual.

DHCP permite asignar direcciones al cliente al programar una serie de parámetros para que cada cliente pueda contar con su dirección. DHCP puede asignar direcciones de forma manual al establecer una IP predeterminada, de forma automática al establecer una serie de direcciones IP disponibles de forma permanente o por asignación dinámica que arrienda una dirección de forma terminal, hasta que el cliente no necesite la dirección o hasta que se cumpla un plazo predeterminado.

Las ACL o listas de control de acceso son una serie de comandos que se programan en los routers con el objetivo de controlar una serie de paquetes de acuerdo con la información que se establece en el paquete. Las justificaciones para incorporar las listas de control de acceso se hacen por las siguientes razones:

- Limitar el tráfico de red para mejorar el rendimiento
- Proporcionar el flujo de tráfico al restringir la entrega de actualizaciones
- Proporcionar un nivel de seguridad al restringir el acceso a usuarios no autorizados
- Filtrar el tráfico de acuerdo al tipo de tráfico, como por ejemplo permitir o denegar el tráfico de Telnet
- Permitir a los hosts acceso a determinados servicios de la Red

Con las listas de acceso, la red funcionará de forma eficiente al utilizar los servicios necesarios y se reducirán los chances de que se presenten problemas por conexiones no autorizadas. Y son las listas de control de acceso las que se van a utilizar para un proceso importante en la red. El proceso de convertir las direcciones privadas a públicas mediante el uso de NAT.

NAT es un servicio que tiene como objetivo conservar las direcciones IPV4 públicas al permitir que las redes utilicen IP4 privadas a nivel interno y solo sean traducidas cuando sea estrictamente necesario. Además de proporcionar privacidad también propone un nivel de seguridad al ocultar las direcciones IPV4 de las redes externas.

Los routers se pueden configurar con una o más direcciones IPV4 válidas. El grupo de direcciones se conoce como “Conjunto NAT”. Cuando un dispositivo interno envía tráfico fuera de la red, el router con NAT traduce la dirección IPV4 interna a una dirección pública del conjunto NAT.

1.4 MATERIALES Y MÉTODOS

1.4.1 MATERIALES

Para el desarrollo del proyecto se ha utilizado la versión más reciente del programa simulador de redes Packet Tracer. Más exactamente la versión 7.1la cual cuenta con las versiones más recientes de los routers que existen en la actualidad.

Para cerciorarse de que la topología sea lo más fiel posible al problema planteado se eligieron los siguientes dispositivos de forma cuidadosa para que se cumplan todos los objetivos planteados en el trabajo final. Los dispositivos fueron los siguientes:

- 2 Switches 2960
- 3 Routers 2811 con un sistema operativo Cisco con la adición de módulos HWIC-2T para la habilitación de interfaces seriales.
- 3 computadoras genéricas
- Una nube WAN para simular la conexión de un equipo externo a la red
- Dos cables DCE para la conexión entre dos de los routers
- 5 cables para las conexiones entre los dispositivos que conforman la red

Para la parte teórica se utiliza el curso de Cisco CCNA2 el cual abarca los temas de VLAN, enrutamiento, DHCP, OSPF y en los cuales mediante ejemplos se explica cómo se realizan las diferentes conexiones y configuraciones.

1.4.2 METODOLOGÍA

Para solucionar el problema he optado por crear la topología en Packet Tracer dado que es un programa muy efectivo para simular redes Cisco. Se crearon primero los componentes físicos para especificar los equipos utilizados para la simulación.

Si bien la configuración de los distintos componentes de cada dispositivo se puede programar mediante CLI, se utiliza el modo de “Config” para algunos procedimientos y la creación de configuraciones de emergencia en caso de errores.

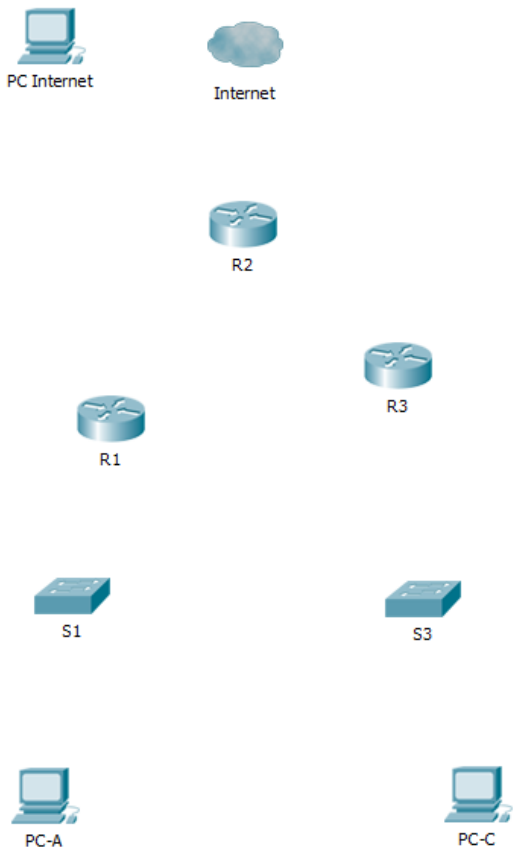
En cada segmento he optado por hacer la prueba del Ping entre las interfaces para verificar su conectividad. El único inconveniente que se ha presentado con Packet Tracer reside en que algunos de los comandos en la consola, no se encuentran presentes por lo cual algunos de los resultados no se pueden mostrar al cien por ciento.

1.5 DESARROLLO DEL PROYECTO

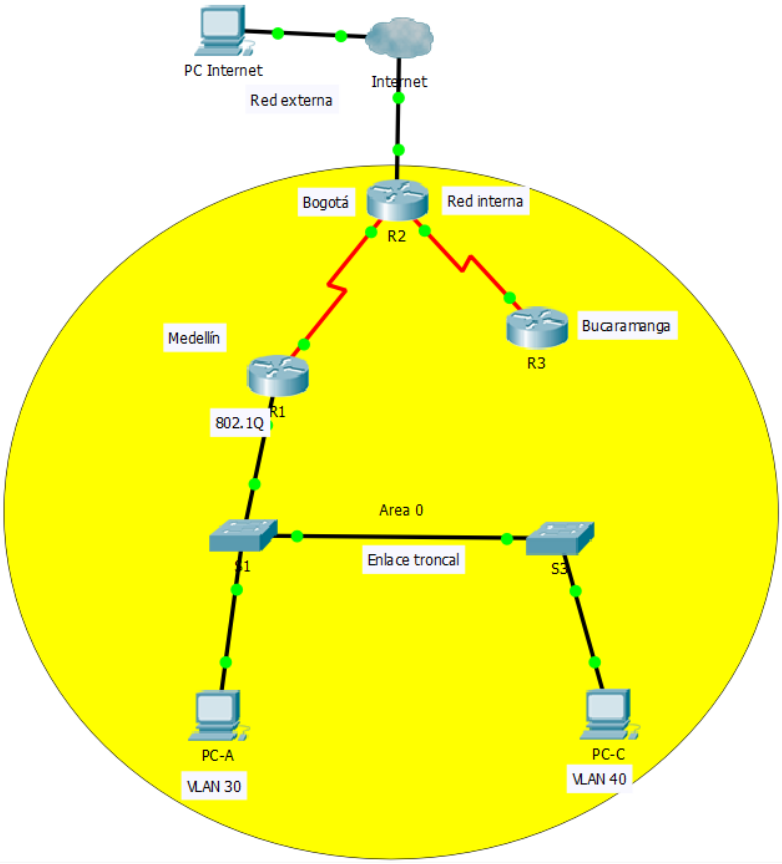
PREPARACIÓN

El proyecto consiste en la creación de una topología de una empresa en Colombia que cuenta con tres diferentes sucursales. El plan consiste en recrearla en Packet Tracer siguiendo una serie de objetivos los cuales planean poner a prueba los conocimientos adquiridos para Cisco. Se siguieron diferentes pasos para la creación de la topología.

Primero se crea la topología que corresponde a la situación problemática. Se crean los diferentes equipos tales como los switches, routers y las PC.



Una vez se han creado los dispositivos, el siguiente paso consiste en realizar las conexiones para conectar uno a uno los dispositivos. El resultado final se presentará en la siguiente ilustración:

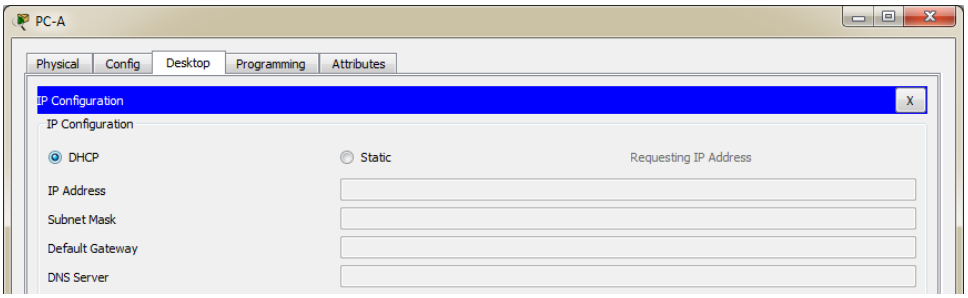


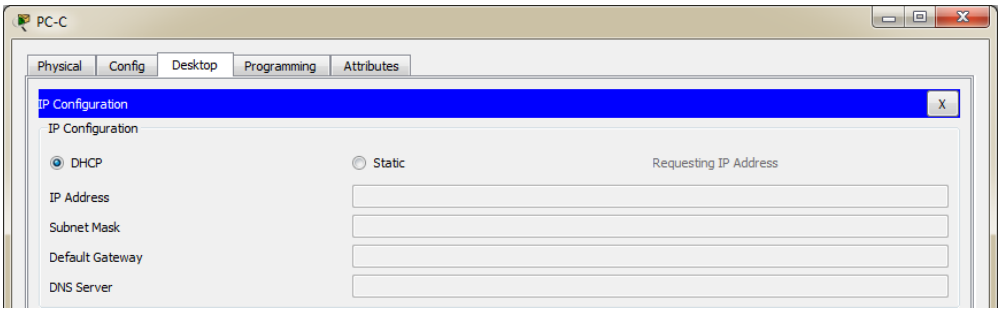
Una vez se ha creado la topología, el siguiente paso fue crear una tabla de direccionamiento basado en las direcciones que se agregarán en las interfaces correspondientes. Las PC por su puesto solo cuando se incorpore el protocolo de DHCP. Por el momento las interfaces son las siguientes:

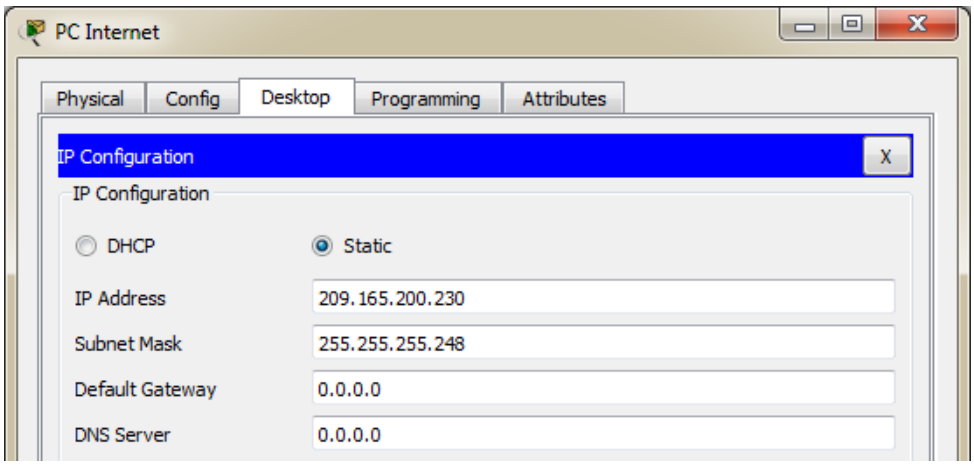
DISPOSITIVO	INTERFAZ	DIRECCIÓN IP	MÁSCARA DE SUBRED
R1	S0/0/0	172.31.21.1	255.255.255.252
	F 0/0	192.168.99.1	255.255.255.0
R2	S0/0/0	172.31.23.1	255.255.255.252
	S0/0/1	172.31.21.2	255.255.255.252
	F 0/0	209.165.200.224	255.255.255.248
	Lo0	10.10.10.10	255.255.255.255
R3	S0/0/1	171.31.23.2	255.255.255.252
	Lo4	192.168.4.0	255.255.255.0
	Lo5	192.168.5.0	255.255.255.0
	Lo6	192.168.6.0	255.255.255.0
S1	F 0/1	(Enlace de VLan 30)	255.255.255.0
	F 0/3		(Enlace troncal)

	F 0/24		255.255.255.0
S3	F 0/1	(Enlace de Vlan 40)	255.255.255.0
	F 0/3		(Enlace troncal)

Las PC con la excepción de la PC de Internet, no deben insertarse direcciones IP, en lugar de ello simplemente, o se las deja en la configuración predeterminada o se las deja en modo de DHCP para que más tarde se pueda agregar esa configuración, lo que se mostrará en la siguiente ilustración:

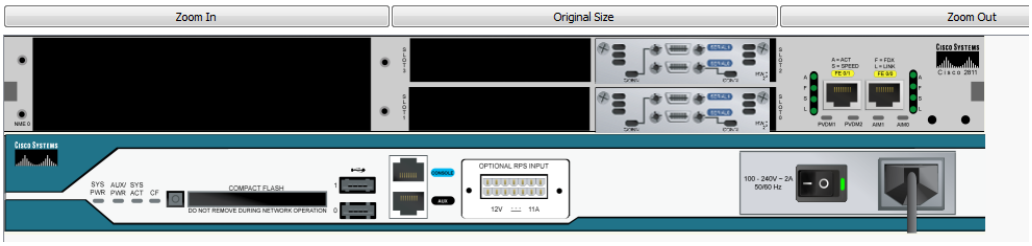




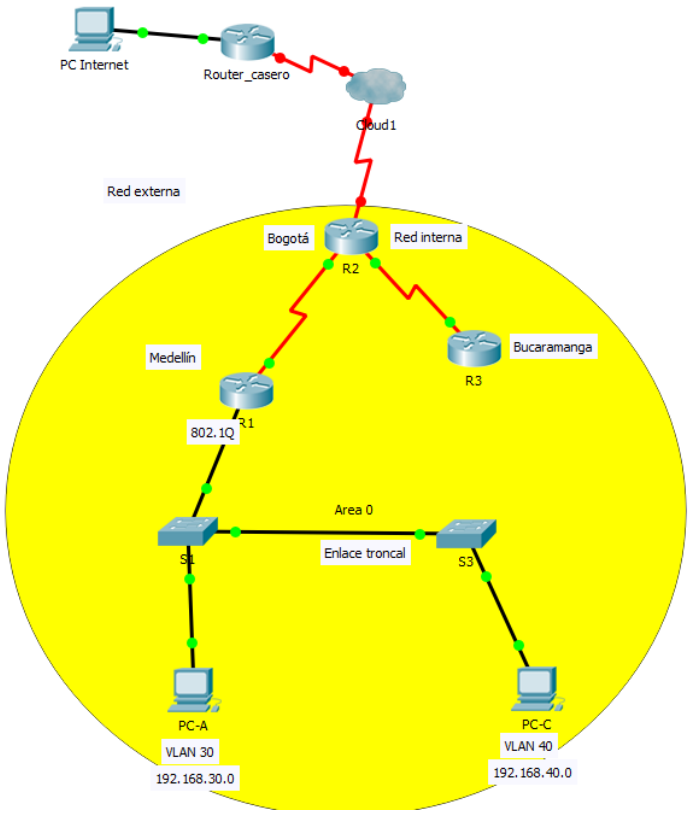


La topología que se muestra en el planteamiento del problema incluye una nube la cual representa una conexión a internet. Si bien se puede omitir el detalle, con el propósito de demostrar la posibilidad de interconectar varios aparatos se decidieron hacer las siguientes modificaciones, las cuales se presentarán a medida que se realiza el trabajo:

Modificación del Router R2 para incorporar una interfaz serial



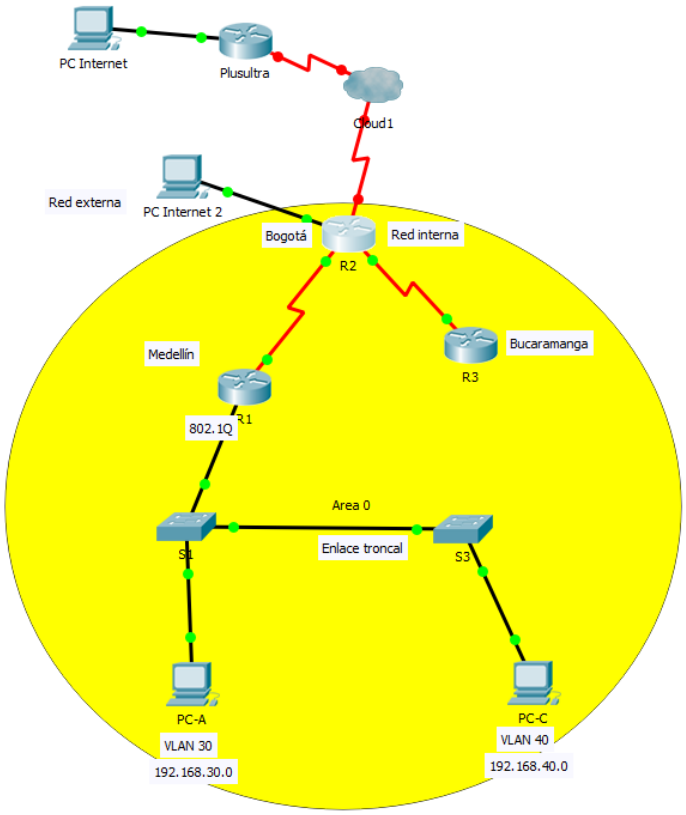
Al router R2 se le agrega un nuevo módulo HWIC-2T para crear una nueva interfaz serial, la cual se agregará un cableado DCE para conectar a la nube, y de la misma se conectará a otro router que se conectará a otra PC que se utilizará para las pruebas de Ping, dando el siguiente resultado:



Se actualizará la tabla de enrutamiento agregando los siguientes datos antes de proseguir al paso del direccionamiento IP:

DISPOSITIVO	INTERFAZ	DIRECCIÓN IP	MÁSCARA DE SUBRED
R2	S0/0/2	172.31.25.1	255.255.255.252
PLUSULTRA	S0/0/0	172.31.25.2	255.255.255.252
	F0/0	209.165.205.225	255.255.255.248
PC_INTERNET	F0/0	209.165.205.230	255.255.255.248

Y para comprobar que se puede conectar una PC al Router R2 y también hacer las respectivas pruebas del Ping se hizo una modificación especial, además de renombrar el router casero a Plusultra:



Al router R2 se le agrega una nueva computadora llamada Pc Internet 2, la cual tendrá los siguientes datos:

DISPOSITIVO	INTERFAZ	DIRECCIÓN IP	MÁSCARA DE SUBRED

PC INTERNET 2	F0/0	209.165.200.230	255.255.255.248

DIRECCIONAMIENTO IP

El próximo paso para la creación de la topología consiste en el direccionamiento IP. Desde el modo CLI se configurarán todas las opciones en los routers y switches. Para hacer una demostración de lo que se va a hacer, se mostrarán los pasos para la configuración del Router R1

Configuración de interfaces en el router 1

```
Router(config-if)#ip address 172.31.21.1 255.255.255.252
Router(config-if)#no shutdown
Router(config)#hostname R1
R1(config)#
%SYS-5-CONFIG_I: Configured from console by console
R1(config)#
R1(config)#interface FastEthernet0/0
R1(config-if)#ip address 192.168.99.1 255.255.255.0
R1(config-if)#
```

Las únicas interfaces que cuentan para el router R1 son: Interfaz serial 0/0/0 y FastEthernet 0/0. Las demás no están activadas por defecto lo que permitirá ahorrar algo de tiempo.

Configuración de las interfaces en el router 2

Para el router 2 se configurarán las interfaces seriales S0/0/0 y S0/0/1 además de una interfaz para LAN y Loopback 0.

Cambio de nombre del Router

```
Router(config)#hostname R2
```

Dirección IP en la interfaz serial S0/0/0

```
R2(config)#interface lo0
R2(config-if)#ip address 172.31.23.1 255.255.255.252
R2(config-if)#no shutdown
```

Dirección IP en la interfaz serial S0/0/1

```
R2(config)#interface serial0/0/1
R2(config-if)#ip address 172.31.21.2 255.255.255.252
R2(config-if)#no shutdown

R2(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up

R2(config-if)#
```

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

R2(config-if)#

Dirección IP en la interfaz Loopback 0

R2(config)#interface lo0
R2(config-if)#ip address 10.10.10.10 255.255.255.255
R2(config-if)#no shutdown

Dirección IP en la interfaz Fastethernet 0/0

R2(config)#interface FastEthernet0/0
R2(config-if)#ip address 209.165.200.225 255.255.255.248
R2(config-if)#no shutdown

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
```

Como una nota importante, la interfaz de Loopback 0 actuará como el servidor conectado al Router 2 en lugar de conectar un equipo físico allí.

A continuación se agregan las nuevas interfaces que han sido mencionadas en la sección de preparación:

```
Dirección IP en la interfaz serial S0/2/0

R2(config)#interface Serial0/2/0
R2(config-if)#ip address 172.31.25.1 255.255.255.252
```

Configuración de las interfaces en el router 3

El Router 3 cuenta con tres interfaces Loopback y una interfaz serial, por lo que la configuración se hará de la siguiente forma:

```
Dirección IP en la interfaz serial S0/0/1
R3(config)#interface Serial0/0/1
R3(config-if)# ip address 172.31.23.2 255.255.255.252
R3(config-if)#no shutdown
R3(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up

R3(config-if)#
Cambio de nombre de Router
Router(config)#hostname R3
R3(config)#
Dirección IP en la interfaz Lo4

R3(config)#interface lo4

R3(config-if)#
%LINK-5-CHANGED: Interface Loopback4, changed state to up
```

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

R3(config-if)#ip address 192.168.4.1 255.255.255.0
R3(config-if)#no shut
R3(config-if)#
%LINK-5-CHANGED: Interface Loopback4, changed state to up

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

R3(config-if)#
```

Dirección IP en la interfaz Lo5

```
R3(config-if)#interface lo5
R3(config-if)#ip address 192.168.5.1 255.255.255.0
R3(config-if)#no shut
R3(config-if)#shut

R3(config-if)#
%LINK-5-CHANGED: Interface Loopback5, changed state to administratively down

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

R3(config-if)#no shut

R3(config-if)#
%LINK-5-CHANGED: Interface Loopback5, changed state to up

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

R3(config-if)#
```

Dirección IP en la interfaz Lo6

```
R3(config)#interface lo6

R3(config-if)#
%LINK-5-CHANGED: Interface Loopback6, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback6, changed state to up
R3(config-if)#ip address 192.168.6.1 255.255.255.0
R3(config-if)#shut

R3(config-if)#
%LINK-5-CHANGED: Interface Loopback6, changed state to administratively down

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

R3(config-if)#no shut
R3(config-if)#
%LINK-5-CHANGED: Interface Loopback6, changed state to up

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

R3(config-if)#
```

Configuración del router casero

El router casero servirá para hacer las pruebas de ping y para probar la nube que actuará como el internet en la topología. La configuración del router casero es la siguiente:

```
Router>enable
Router#
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface FastEthernet0/0
Router(config)#interface Serial0/0/0
Router(config-if)#ip address 172.31.25.2 255.255.255.252
Router(config-if)#
Router(config-if)#exit
Router(config)#interface FastEthernet0/0
Router(config-if)#ip address 209.165.205.225 255.255.255.248
Router(config-if)#
Router(config)#hostname Plusultra
Plusultra(config)#
Plusultra(config)#
%SYS-5-CONFIG_I: Configured from console by console

Plusultra(config)#
```

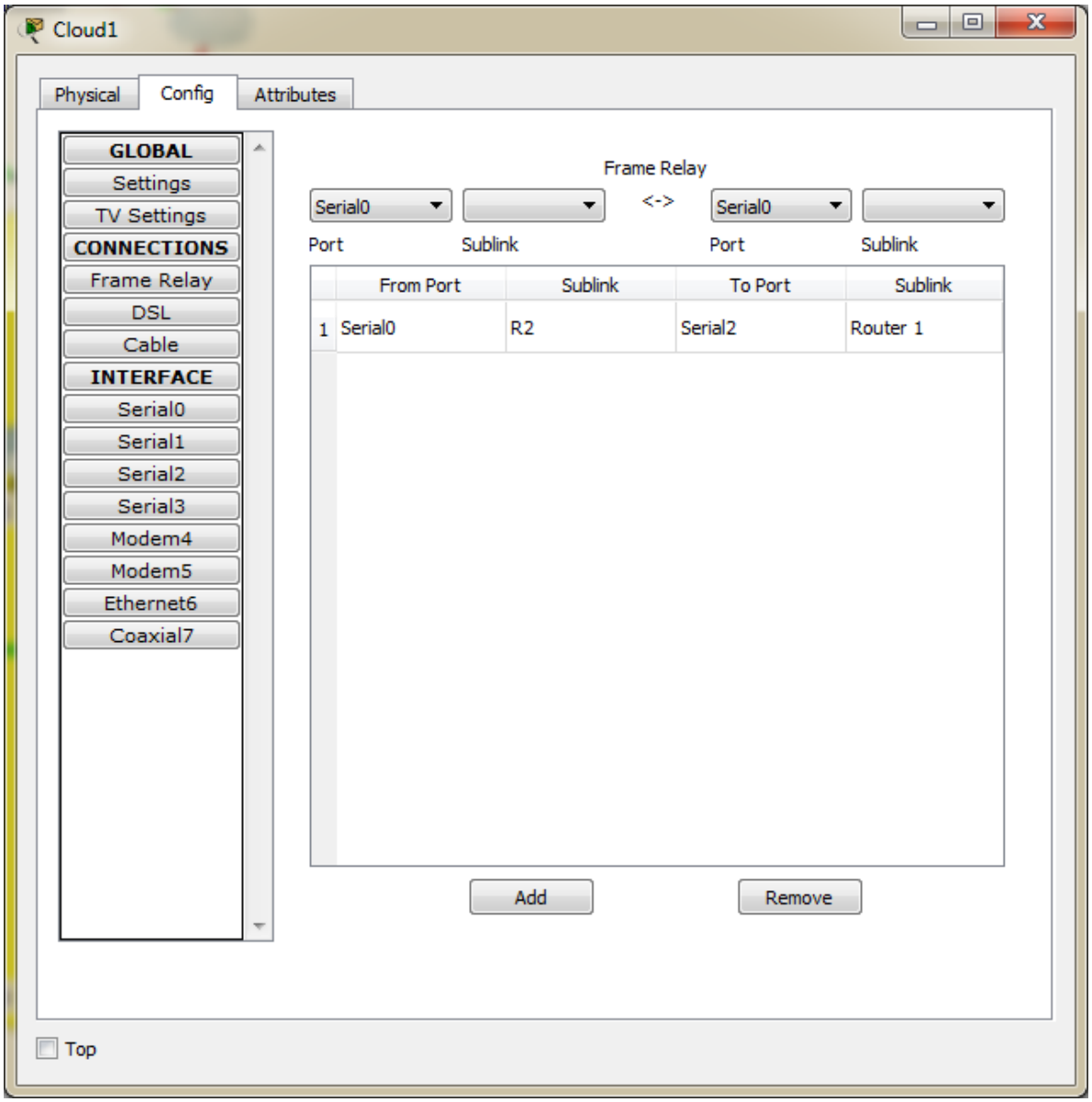
CONEXIÓN A LA NUBE

Antes de aplicar el protocolo de OSPFv2, se optó por crear una nube en la cual se conectarán los routers Plusultra y R2. Para que dos routers se puedan comunicar en la nube, se aplicará un protocolo de encapsulamiento llamado frame-relay en cada uno de los routers:

```
Plusultra(config)#interface Serial0/0/0
Plusultra(config-if)#encapsulation frame-relay
Plusultra(config-if)#
```

```
R2(config)#interface Serial0/2/0
R2(config-if)#encapsulation frame-relay
```

El siguiente paso consiste en modificar la nube para que los dos routers se encuentren conectados.



En la siguiente ilustración, una vez los routers con sus interfaces seriales se activa el protocolo de Frame-Relay, se enciende la nube, se verifica que los cables estén conectados a la interfaz correcta y se agregan en cada serial las siguientes configuraciones:

- Serial 0 es la de R2
- Serial 2 es la del Router R1(Plusultra)

Con la nube encendida y los cables conectados, se puede simular que la Pc Internet es un acceso remoto a la red y servirá para hacer las pruebas de conexiones.

El último paso para que haya una conexión entre Plusultra y R2 consiste en agregar una dirección estática de siguiente paso, de la siguiente forma:

R2

R2(config)#ip route 0.0.0.0 0.0.0.0 172.31.25.2

Plus ultra

Plusultra(config)#ip route 0.0.0.0 0.0.0.0 172.31.25.1

APLICACIÓN DEL PROTOCOLO OSPFV2

Una vez están listos los routers, el siguiente paso consiste en incorporar OSPFv2 en ellos. Hay que seguir una serie de condiciones en los routers para aplicar el protocolo. Las condiciones se mostrarán en la siguiente tabla:

Configuración, ítem o task	Especificación
ID del Router 1	1.1.1.1
ID del Router 2	2.2.2.2
ID del Router 3	3.3.3.3
Las interfaces LAN deben ser pasivas	
Ancho de banda en interfaces seriales	128KB/s
Costo de métrica en S0/0	7500

Configuración de OSPFv2 en el Router 1

```
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#router ospf 1
R1(config-router)#router-id 1.1.1.1
R1(config-router)#end

Habilitación de OSPF
R1(config)#router ospf 1
R1(config-router)#network 172.31.21.0 0.0.0.3 area 0
R1(config-router)#

Interfaces LAN pasivas
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#router ospf 1
```

```
R1(config-router)#passive-interface f0/0
R1(config-router)#^Z

Ancho de banda en interfaces seriales
R1(config)#interface s0/0/0
R1(config-if)#bandwidth 128
R1(config-if)# #interface s0/0/1
R1(config-if)#interface s0/0/1
R1(config-if)#bandwidth 128

Costo de métrica en S0/0/0
R1(config)#interface serial 0/0/0
R1(config-if)#ip ospf cost 7500
R1(config-if)#^Z
R1#
```

Configuración de OSPFv2 en el Router 2

```
R2#config t
R2(config)#router ospf 1
R2(config-router)#router-id 2.2.2.2
R2(config-router)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console

R2#copy r s
Destination filename [startup-config]?
Building configuration...
[OK]
R2#

Activación de OSPFv2 en las interfaces
R2(config)#router ospf 1
R2(config-router)#network 172.31.21.0 0.0.0.3 area 0
R2(config-router)#network 172.31.23.0 0.0.0.3 area 0
R2(config-router)#network 209.165.200.224 0.0.0.7 area 0
R2(config-router)#network 10.10.10.10 0.0.0.255 area 0
R2(config-router)#network 172.31.25.0 0.0.0.3 area 0

R2(config-router)#^Z

Interfaces LAN pasivas

R2(config)#router ospf 1
R2(config-router)#passive-interface f0/0

Ancho de banda

R2(config)#interface serial 0/0/0
R2(config-if)#bandwidth 128
R2(config-if)#^Z
R2#
%SYS-5-CONFIG_I: Configured from console by console
```

```
R2#enable
R2#config t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#interface serial 0/0/1
R2(config-if)#bandwidth 128
R2(config)#interface Serial0/2/0
R2(config-if)#ip address 172.31.25.1 255.255.255.252
R2(config-if)#bandwidth 128
R2(config-if)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console

R2#
```
Costo de métrica en S0/0/0
```
R2(config)#interface s0/0/0
R2(config-if)#ip ospf cost 7500
R2(config-if)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console
R2#
```

Configuración de OSPFv2 en el Router 3

```
R3#config t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#router ospf 1
R3(config-router)#router-id 3.3.3.3
R3(config-router)#end
R3#
%SYS-5-CONFIG_I: Configured from console by console

R3#copy r s
Destination filename [startup-config]?
Building configuration...
[OK]
R3#

R3(config)#router ospf 1
R3(config-router)#network 172.31.23.0 0.0.0.3 area 0
R3(config-router)#
```

Ancho de banda

```
R3#config t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#interface s0/0/0
R3(config-if)#bandwidth 128
R3(config-if)#^Z
R3#
%SYS-5-CONFIG_I: Configured from console by console
```

```
R3#config t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#interface s0/0/1
R3(config-if)#bandwidth 128
R3(config-if)#^Z
R3#
%SYS-5-CONFIG_I: Configured from console by console

R3#

Costo de métrica en S0/0/0
R3(config)#interface s0/0/0
R3(config-if)#ip ospf cost 7500
R3(config-if)#end
R3#
%SYS-5-CONFIG_I: Configured from console by console

R3#
```

Verificación de configuración de OSPFv2 en los routers

Router 1

```
R1#show ip ospf
Routing Process "ospf 1" with ID 1.1.1.1
Supports only single TOS(TOS0) routes
Supports opaque LSA
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
Number of external LSA 0. Checksum Sum 0x000000
Number of opaque AS LSA 0. Checksum Sum 0x000000
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
External flood list length 0
Area BACKBONE(0)
Number of interfaces in this area is 2
Area has no authentication
SPF algorithm executed 3 times
Area ranges are
Number of LSA 3. Checksum Sum 0x01a684
Number of opaque link LSA 0. Checksum Sum 0x000000
Number of DCbitless LSA 0
Number of indication LSA 0
Number of DoNotAge LSA 0
Flood list length 0

R1#show ip protocols

Routing Protocol is "ospf 1"
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Router ID 1.1.1.1
```

```
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Maximum path: 4
Routing for Networks:
172.31.21.0 0.0.0.3 area 0
192.168.99.0 0.0.0.255 area 0
Passive Interface(s):
FastEthernet0/0
Routing Information Sources:
Gateway Distance Last Update
1.1.1.1 110 00:02:24
2.2.2.2 110 00:02:24
3.3.3.3 110 00:02:24
Distance: (default is 110)
R1#show ip ospf interface

FastEthernet0/0 is up, line protocol is up
Internet address is 192.168.99.1/24, Area 0
Process ID 1, Router ID 1.1.1.1, Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State DR, Priority 1
Designated Router (ID) 1.1.1.1, Interface address 192.168.99.1
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
No Hellos (Passive interface)
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
Neighbor Count is 0, Adjacent neighbor count is 0
Suppress hello for 0 neighbor(s)
Serial0/0/0 is up, line protocol is up
Internet address is 172.31.21.1/30, Area 0
Process ID 1, Router ID 1.1.1.1, 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 00:00:01
Index 2/2, 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
Neighbor Count is 1 , Adjacent neighbor count is 1
Adjacent with neighbor 2.2.2.2
Suppress hello for 0 neighbor(s)
```

Router 2

```
R2#show ip ospf
Routing Process "ospf 1" with ID 2.2.2.2
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
```

```
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
 Number of external LSA 0. Checksum Sum 0x000000
 Number of opaque AS LSA 0. Checksum Sum 0x000000
 Number of DCbitless external and opaque AS LSA 0
 Number of DoNotAge external and opaque AS LSA 0
 Number of areas in this router is 1. 1 normal 0 stub 0 nssa
 External flood list length 0
    Area BACKBONE(0)
        Number of interfaces in this area is 5
        Area has no authentication
        SPF algorithm executed 14 times
        Area ranges are
        Number of LSA 3. Checksum Sum 0x0129d4
        Number of opaque link LSA 0. Checksum Sum 0x000000
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0

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 2.2.2.2
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.31.21.0 0.0.0.3 area 0
    172.31.23.0 0.0.0.3 area 0
    209.165.200.224 0.0.0.7 area 0
    10.10.10.10 0.0.0.0 area 0
    172.31.25.0 0.0.0.3 area 0
  Passive Interface(s):
    FastEthernet0/0
  Routing Information Sources:
    Gateway         Distance      Last Update
    1.1.1.1              110      00:14:00
    2.2.2.2              110      00:05:10
    3.3.3.3              110      00:13:58
  Distance: (default is 110)

R2#show ip ospf interface

Loopback0 is up, line protocol is up
  Internet address is 10.10.10.10/32, Area 0
  Process ID 1, Router ID 2.2.2.2, Network Type LOOPBACK, Cost: 1
  Loopback interface is treated as a stub Host
Serial0/0/0 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 00:00:02
  Index 2/2, 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
  Neighbor Count is 1 , Adjacent neighbor count is 1
    Adjacent with neighbor 3.3.3.3
  Suppress hello for 0 neighbor(s)
Serial0/0/1 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: 781
  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 00:00:02
  Index 3/3, 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
  Neighbor Count is 1 , Adjacent neighbor count is 1
    Adjacent with neighbor 1.1.1.1
  Suppress hello for 0 neighbor(s)
FastEthernet0/0 is up, line protocol is up
  Internet address is 209.165.200.225/29, Area 0
  Process ID 1, Router ID 2.2.2.2, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 2.2.2.2, Interface address 209.165.200.225
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    No Hellos (Passive interface)
  Index 4/4, 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
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
Serial0/2/0 is up, line protocol is up
  Internet address is 172.31.25.1/30, Area 0
  Process ID 1, Router ID 2.2.2.2, Network Type NON-BROADCAST, Cost: 781
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 2.2.2.2, Interface address 172.31.25.1
  No backup designated router on this network
  Timer intervals configured, Hello 30, Dead 120, Wait 120, Retransmit 5
    Hello due in 00:00:13
  Index 5/5, 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
  Neighbor Count is 0, Adjacent neighbor count is 0
```

```
  Suppress hello for 0 neighbor(s)
R2#
```

Router 3

```
R3#show ip ospf
Routing Process "ospf 1" with ID 3.3.3.3
Supports only single TOS(TOS0) routes
Supports opaque LSA
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
Number of external LSA 0. Checksum Sum 0x000000
Number of opaque AS LSA 0. Checksum Sum 0x000000
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
External flood list length 0
Area BACKBONE(0)
Number of interfaces in this area is 1
Area has no authentication
SPF algorithm executed 3 times
Area ranges are
Number of LSA 3. Checksum Sum 0x01a684
Number of opaque link LSA 0. Checksum Sum 0x000000
Number of DCbitless LSA 0
Number of indication LSA 0
Number of DoNotAge LSA 0
Flood list length 0

R3#
R3#show ip protocols

Routing Protocol is "ospf 1"
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Router ID 3.3.3.3
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Maximum path: 4
Routing for Networks:
172.31.23.0 0.0.0.3 area 0
Routing Information Sources:
Gateway Distance Last Update
1.1.1.1 110 00:05:55
2.2.2.2 110 00:05:55
3.3.3.3 110 00:05:55
Distance: (default is 110)

R3#show ip ospf interface

Serial0/0/1 is up, line protocol is up
Internet address is 172.31.23.2/30, Area 0
Process ID 1, Router ID 3.3.3.3, Network Type POINT-TO-POINT, Cost: 781
```

```
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 00:00:04
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
Neighbor Count is 1 , Adjacent neighbor count is 1
Adjacent with neighbor 2.2.2.2
Suppress hello for 0 neighbor(s)
R3#
```

CONFIGURACIÓN DE SWITCHES

Los switches se van a configurar para que acepten redes VLAN y también puedan aceptar enlaces troncales. A cada Interfaz se le asignará una VLAN correspondiente para que desde el Router R1 se les pueda asignar las correspondientes direcciones mediante DHCP. Pero antes de calibrar las VLAN, primero hay que crear en el router R1 subinterfaces.

En la interfaz F0/0 del router R1 es donde se conectará el switch S1. Allí se van a crear tres subinterfaces, cada una correspondiente a una VLAN:

Para crear una inter-vlan debe crearse una serie de subinterfaces en el router R1.

Creación de la interfaz F0/0.30

```
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#int f0/0.30
R1(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/0.30, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.30, changed state to up

R1(config-subif)#encapsulation dot1q 30
R1(config-subif)#ip address 192.168.30.1 255.255.255.0
R1(config-subif)#^Z
R1#
%SYS-5-CONFIG_I: Configured from console by console

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

Creación de la interfaz F0/0.40

```
R1(config)#interface f0/0.40
R1(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/0.40, changed state to up
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.40, changed state to up

R1(config-subif)#encapsulation dot1q 40
R1(config-subif)#ip address 192.168.40.1 255.255.255.0
R1(config-subif)#^Z
R1#
%SYS-5-CONFIG_I: Configured from console by console
```

Creación de la interfaz F0/0.200

```
R1(config)#interface f0/0.200
R1(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/0.200, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.200, changed state to up

R1(config-subif)#encapsulation dot1q 200
R1(config-subif)#ip address 192.168.200.1 255.255.255.0
R1(config-subif)#shutdown

R1(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/0.200, changed state to administratively down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.200, changed state to down

R1(config-subif)#no shutdown

R1(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/0.200, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.200, changed state to up

R1(config-subif)#
```

Ya creada las subinterfaces en R1, el siguiente paso consiste en crear las VLAN y preparar los distintos tipos de enlaces en cada uno de los switches.

Configuración del Switch S1

Creación de VLAN

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

S1(config)#vlan 30
S1(config-vlan)#name Administracion
S1(config-vlan)#end
S1(config)#vlan 40
S1(config-vlan)#name mercadeo
S1(config-vlan)#vlan 200
S1(config-vlan)#name mantenimiento
```

```
S1(config-vlan)#end
```

Creación de puertos de acceso y puertos troncales

Puertos de acceso

```
S1(config)#interface f0/1
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 30
```

Puertos troncales

```
S1(config)#interface f0/3
S1(config-if)#switchport mode trunk
S1(config-if)#^Z
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1(config)#interface f0/24
S1(config-if)#switchport mode trunk
```

Enrutamiento

```
S1(config)#interface vlan 30
S1(config-if)#
%LINK-5-CHANGED: Interface Vlan30, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan30, changed state to up

S1(config-if)#ip address 192.168.30.2 255.255.255.0
S1(config-if)#^Z
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#config t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#interface vlan 40
S1(config-if)#
%LINK-5-CHANGED: Interface Vlan40, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan40, changed state to up

S1(config-if)#ip address 192.168.40.2 255.255.255.0
S1(config-if)#
S1(config-if)#^Z
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1(config)#interface vlan 2000
S1(config-if)# ip address 192.168.200.2 255.255.255.0
S1(config-if)#^Z
```

Configuración del Switch S3

Creación de VLAN

```
S3(config)#vlan 30
S3(config-vlan)#name Administracion
S3(config-vlan)#end
S3#
%SYS-5-CONFIG_I: Configured from console by console

S3#config t
Enter configuration commands, one per line. End with CNTL/Z.
S3(config)#vlan 40
S3(config-vlan)#name mercadeo
S3(config-vlan)#vlan 200
S3(config-vlan)#name mantenimiento
S3(config-vlan)#end
S3#
%SYS-5-CONFIG_I: Configured from console by console

S3#
```

Creación de puertos de acceso y puertos troncales

Puertos de acceso

```
S3(config)#interface f0/1
S3(config-if)#switchport mode access
S3(config-if)#switchport access vlan 40
S3(config-if)#^Z
S3#
```

Puertos troncales

```
S3(config)#interface f0/3
S3(config-if)#switchport mode trunk
S3(config-if)#^Z
S3#
%SYS-5-CONFIG_I: Configured from console by console

S3#show interfaces trunk
Port Mode Encapsulation Status Native vlan
Fa0/3 on 802.1q trunking 1

Port Vlans allowed on trunk
Fa0/3 1-1005

Port Vlans allowed and active in management domain
Fa0/3 1,30,40,200
```

```
Port Vlans in spanning tree forwarding state and not pruned
Fa0/3 1,30,40,200

S3#
```

Enrutamiento

```
S3(config)#interface 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)#^Z


S3(config)#interface vlan 30
S3(config-if)#
%LINK-5-CHANGED: Interface Vlan30, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan30, changed state to up

S3(config-if)#ip address 192.168.30.3 255.255.255.0
S3(config-if)#^Z
S3#
%SYS-5-CONFIG_I: Configured from console by console

S3#config t
Enter configuration commands, one per line. End with CNTL/Z.
S3(config)#interface vlan 40
S3(config-if)#
%LINK-5-CHANGED: Interface Vlan40, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan40, changed state to up

S3(config-if)#ip address 192.168.40.3 255.255.255.0
S3(config-if)#^Z
S3#
%SYS-5-CONFIG_I: Configured from console by console

S3#
```

Como último paso, se deshabilitará la búsqueda de DNS del Switch S3 escribiendo el siguiente comando:

S3(config)#no ip domain-lookup

Desactivación de interfaces no utilizadas

Para evitar problemas, cada interfaz que no se planea utilizar se desactivará de forma inmediata.

Router R1

```
R1(config)#interface FastEthernet0/1
R1(config-if)#shutdown
R1(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively down

R1(config-if)#exit
R1(config)#interface Serial0/0/1
R1(config-if)#shutdown
R1(config-if)#
```

Router R3

```
R3(config)#interface Serial0/0/0
R3(config-if)#shutdown
R3(config)#interface FastEthernet0/0
R3(config-if)#shutdown
R3(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to administratively down

R3(config-if)#exit
R3(config)#interface FastEthernet0/1
R3(config-if)#shutdown
R3(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively down

R3(config-if)#
```

Router R2

```
R2(config)#interface Serial0/2/1
R2(config-if)#shutdown
```

Switch S1

```
S1(config)#interface FastEthernet0/2
S1(config-if)#shutdown
S1(config-if)#
S1(config-if)#exit
S1(config)#interface FastEthernet0/4
S1(config-if)#shutdown
S1(config-if)#
S1(config-if)#exit
S1(config)#interface FastEthernet0/5
S1(config-if)#shutdown
S1(config-if)#
```

```
S1(config-if)#exit
S1(config)#interface FastEthernet0/6
S1(config-if)#shutdown
S1(config-if)#
S1(config-if)#exit
S1(config)#interface FastEthernet0/7
S1(config-if)#shutdown
S1(config-if)#
S1(config-if)#exit
S1(config)#interface FastEthernet0/8
S1(config-if)#shutdown
S1(config-if)#
S1(config-if)#exit
S1(config)#interface FastEthernet0/9
S1(config-if)#shutdown
S1(config-if)#
S1(config-if)#exit
S1(config)#interface FastEthernet0/10
S1(config-if)#shutdown
S1(config-if)#
S1(config-if)#exit
S1(config)#interface FastEthernet0/11
S1(config-if)#shutdown
S1(config-if)#
S1(config-if)#exit
S1(config)#interface FastEthernet0/12
S1(config-if)#shutdown
S1(config-if)#
S1(config-if)#exit
S1(config)#interface FastEthernet0/13
S1(config-if)#shutdown
S1(config-if)#
S1(config-if)#exit
S1(config)#interface FastEthernet0/14
S1(config-if)#shutdown
S1(config-if)#
S1(config-if)#exit
S1(config)#interface FastEthernet0/15
S1(config-if)#
S1(config-if)#exit
S1(config)#interface FastEthernet0/16
S1(config-if)#shutdown
S1(config-if)#
S1(config-if)#exit
S1(config)#interface FastEthernet0/17
S1(config-if)#shutdown
S1(config-if)#
S1(config-if)#exit
S1(config)#interface FastEthernet0/18
S1(config-if)#shutdown
S1(config-if)#
S1(config-if)#exit
S1(config)#interface FastEthernet0/19
```

```
S1(config-if)#shutdown
S1(config-if)#
S1(config-if)#exit
S1(config)#interface FastEthernet0/20
S1(config-if)#shutdown
S1(config-if)#
S1(config-if)#exit
S1(config)#interface FastEthernet0/21
S1(config-if)#shutdown
S1(config-if)#
S1(config-if)#exit
S1(config)#interface FastEthernet0/22
S1(config-if)#shutdown
S1(config-if)#
S1(config-if)#exit
S1(config)#interface FastEthernet0/23
S1(config-if)#shutdown
S1(config-if)#
S1(config-if)#exit
S1(config)#interface GigabitEthernet0/1
S1(config-if)#shutdown
S1(config-if)#
S1(config-if)#exit
S1(config)#interface GigabitEthernet0/2
S1(config-if)#shutdown
S1(config-if)#
```

Switch S3

```
S3(config)#interface FastEthernet0/2
S3(config-if)#shutdown
S3(config-if)#
S3(config-if)#exit
S3(config)#interface FastEthernet0/4
S3(config-if)#shutdown
S3(config-if)#
S3(config-if)#exit
S3(config)#interface FastEthernet0/5
S3(config-if)#shutdown
S3(config-if)#
S3(config-if)#exit
S3(config)#interface FastEthernet0/6
S3(config-if)#shutdown
S3(config-if)#
S3(config-if)#exit
S3(config)#interface FastEthernet0/7
S3(config-if)#shutdown
S3(config-if)#
S3(config-if)#exit
S3(config)#interface FastEthernet0/8
S3(config-if)#shutdown
S3(config-if)#
S3(config-if)#exit
```

```
S3(config)#interface FastEthernet0/9
S3(config-if)#shutdown
S3(config-if)#
S3(config-if)#exit
S3(config)#interface FastEthernet0/10
S3(config-if)#shutdown
S3(config-if)#
S3(config-if)#exit
S3(config)#interface FastEthernet0/11
S3(config-if)#shutdown
S3(config-if)#
S3(config-if)#exit
S3(config)#interface FastEthernet0/12
S3(config-if)#shutdown
S3(config-if)#
S3(config-if)#exit
S3(config)#interface FastEthernet0/13
S3(config-if)#shutdown
S3(config-if)#
S3(config-if)#exit
S3(config)#interface FastEthernet0/14
S3(config-if)#shutdown
S3(config-if)#
S3(config-if)#exit
S3(config)#interface FastEthernet0/15
S3(config-if)#shutdown
S3(config-if)#
S3(config-if)#exit
S3(config)#interface FastEthernet0/16
S3(config-if)#shutdown
S3(config-if)#
S3(config-if)#exit
S3(config)#interface FastEthernet0/17
S3(config-if)#shutdown
S3(config-if)#
S3(config-if)#exit
S3(config)#interface FastEthernet0/18
S3(config-if)#shutdown
S3(config-if)#
S3(config-if)#exit
S3(config)#interface FastEthernet0/19
S3(config-if)#shutdown
S3(config-if)#
S3(config-if)#exit
S3(config)#interface FastEthernet0/20
S3(config-if)#shutdown
S3(config-if)#
S3(config-if)#exit
S3(config)#interface FastEthernet0/21
S3(config-if)#shutdown
S3(config-if)#
S3(config-if)#exit
S3(config)#interface FastEthernet0/22
```

```
S3(config-if)#shutdown
S3(config-if)#
S3(config-if)#exit
S3(config)#interface FastEthernet0/23
S3(config-if)#shutdown
S3(config-if)#
S3(config-if)#exit
S3(config)#interface FastEthernet0/24
S3(config-if)#shutdown
S3(config-if)#
S3(config-if)#exit
S3(config)#interface GigabitEthernet0/1
S3(config-if)#shutdown
S3(config-if)#
S3(config-if)#exit
S3(config)#interface GigabitEthernet0/2
S3(config-if)#shutdown
S3(config-if)#
```

INCORPORACIÓN DE DHCP Y TRADUCCIÓN DE REDES NAT EN LA TOPOLOGÍA

En la topología asignada, se establecieron una serie de condiciones para incorporar el protocolo DHCP Y el sistema de traducción de redes NAT en determinadas condiciones. Los objetivos principales son:

- Crear un servidor DHCP en R1
- Incorporar el protocolo de traducción de direcciones NAT en R2 para que los hosts puedan salir a internet

Servidor de DHCP en R1

Se va a crear un servidor de DHCP en R1 con el objetivo de que asigne de forma automática las direcciones IP en las VLAN. Las condiciones que debe cumplir el servidor se presentarán en la siguiente tabla:

DHCP Pool Vlan 30	DHCP Pool Vlan 4
Name: ADMINISTRACION DNS-Server: 10.10.10.11 Domain-Name: ccna-unad.com Establecer default gateway.	Name: MERCADEO DNS-Server: 10.10.10.11 Domain-Name: ccna-unad.com Establecer default gateway.

Como una aclaración, es importante saber que debido a los límites del programa de Packet Tracer, no es posible incorporar el nombre de dominio en el servidor DHCP por lo cual la variable no será tomada en cuenta.

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

#Reservación de las primeras 30 direcciones estáticas

R1(config)#ip dhcp excluded-address 192.168.30.1 192.168.30.30
R1(config)#ip dhcp excluded-address 192.168.40.1 192.168.40.30

Creación del DHCP Pool Vlan 30


R1(config)#ip dhcp pool ADMINISTRACION
R1(dhcp-config)#network 192.168.30.0 255.255.255.0
R1(dhcp-config)#default-router 192.168.30.1
R1(dhcp-config)#dns-server 10.10.10.11
R1(dhcp-config)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console

Creación del DHCP Pool Vlan 40

R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ip dhcp pool MERCADEO
R1(dhcp-config)#network 192.168.40.0 255.255.255.0
R1(dhcp-config)#default-router 192.168.40.1
R1(dhcp-config)#dns-server 10.10.10.11
R1(dhcp-config)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#
```

Las DHCP Pool que se crean en el router R1 tienen un propósito. Se reservan las primeras 30 direcciones de cada Subred VLAN. Cuando se conecta un equipo Host, se asignará de forma automática dependiendo de la VLAN a la cual se encuentra conectado el equipo.

Para comprobar el éxito de la instalación de DHCP, se escribe el siguiente comando en el modo de prompt de comando en las PC-A y PC-C

C:\>Ipconfig /all

PC-A

```
C:\>ipconfig /all

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Physical Address.....: 00D0.5847.4335
   Link-local IPv6 Address.....: FE80::2D0:58FF:FE47:4335
   IP Address.....: 192.168.30.31
   Subnet Mask.....: 255.255.255.0
   Default Gateway.....: 192.168.30.1
   DNS Servers.....: 10.10.10.11
   DHCP Servers.....: 192.168.30.1
   DHCPv6 Client DUID.....: 00-01-00-01-57-BC-87-28-00-D0-58-47-43-35
```

PC-C

```
C:\>ipconfig /all

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Physical Address.....: 00D0.9712.1626
   Link-local IPv6 Address.....: FE80::2D0:97FF:FE12:1626
   IP Address.....: 192.168.40.31
   Subnet Mask.....: 255.255.255.0
   Default Gateway.....: 192.168.40.1
   DNS Servers.....: 10.10.10.11
   DHCP Servers.....: 192.168.40.1
   DHCPv6 Client DUID.....: 00-01-00-01-1C-97-1D-01-00-D0-97-12-16-26
```

Las primeras direcciones estáticas de cada VLAN han sido reservadas, por lo tanto las nuevas IP deberán iniciar desde 31, lo cual se ha conseguido de forma exitosa.

INCORPORACIÓN DE NAT EN R2

Para comprobar las funciones de NAT, se incorporará en el router R2 con el objetivo de permitir a los hosts en la computadora de R1 hacer ping al servidor que se encuentra instalado en el router R2. El primer paso consiste en establecer una ruta estática entre R1 y R2. Hay que tener cuidado con este paso puesto que el orden afecta el resultado, si se incorpora de forma equivocada, no se puede hacer el Ping.

Ruta estática en R1

```
R1(config)#ip route 209.165.200.224 255.255.255.248 172.31.21.2
```

Ruta predeterminada en R2

```
R2(config)#ip route 0.0.0.0 0.0.0.0 172.31.21.1
```

Creadas las rutas estáticas en el orden correcto indica que es hora de incorporar el protocolo de NAT. Los pasos a seguir son los siguientes:

Crear una lista ACL para permitir hosts

R2(config)#access-list 1 permit 192.168.99.0 0.0.0.255

La primera ACL permite que se conecten las direcciones que provienen de la red 192.168.99.0

Crear las direcciones que van a traducirse

R2(config)#ip nat pool public_access 209.165.201.225 209.165.201.230 netmask 255.255.255.248

Se crea allí una serie de direcciones a las cuales se traducirían, estableciendo un rango de todas las direcciones IP posibles.

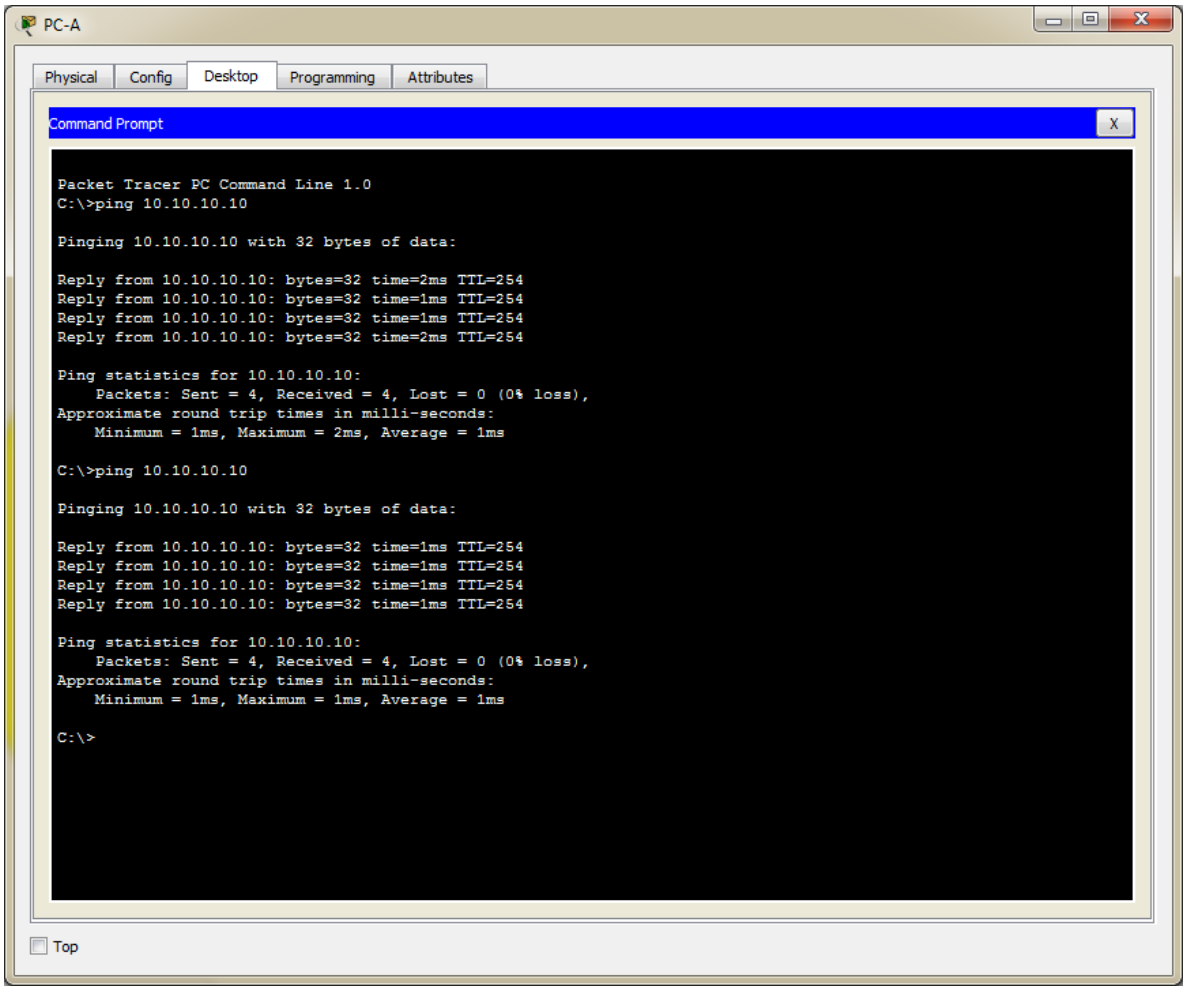
Conectar la ACL al conjunto

```
R2(config)#ip nat inside source list 1 pool public_access overload
```

Especificar interfaces internas e interfaces externas

```
R2(config)#interface s0/0/0
R2(config-if)#ip nat outside
R2(config-if)#interface s0/0/1
R2(config-if)#ip nat inside
```

Para comprobar si la lista NAT funciona, desde la PC A se hará ping al servidor 10.10.10.10



CREACIÓN DE LISTAS ACL

El último punto consiste en crear listas ACL para probar diferentes restricciones y configuraciones para probar lo que los routers pueden hacer. El control del tráfico es importante, no solo para que el rendimiento de la red sea eficiente si no también evitar cualquier problema de seguridad que se pueda presentar.

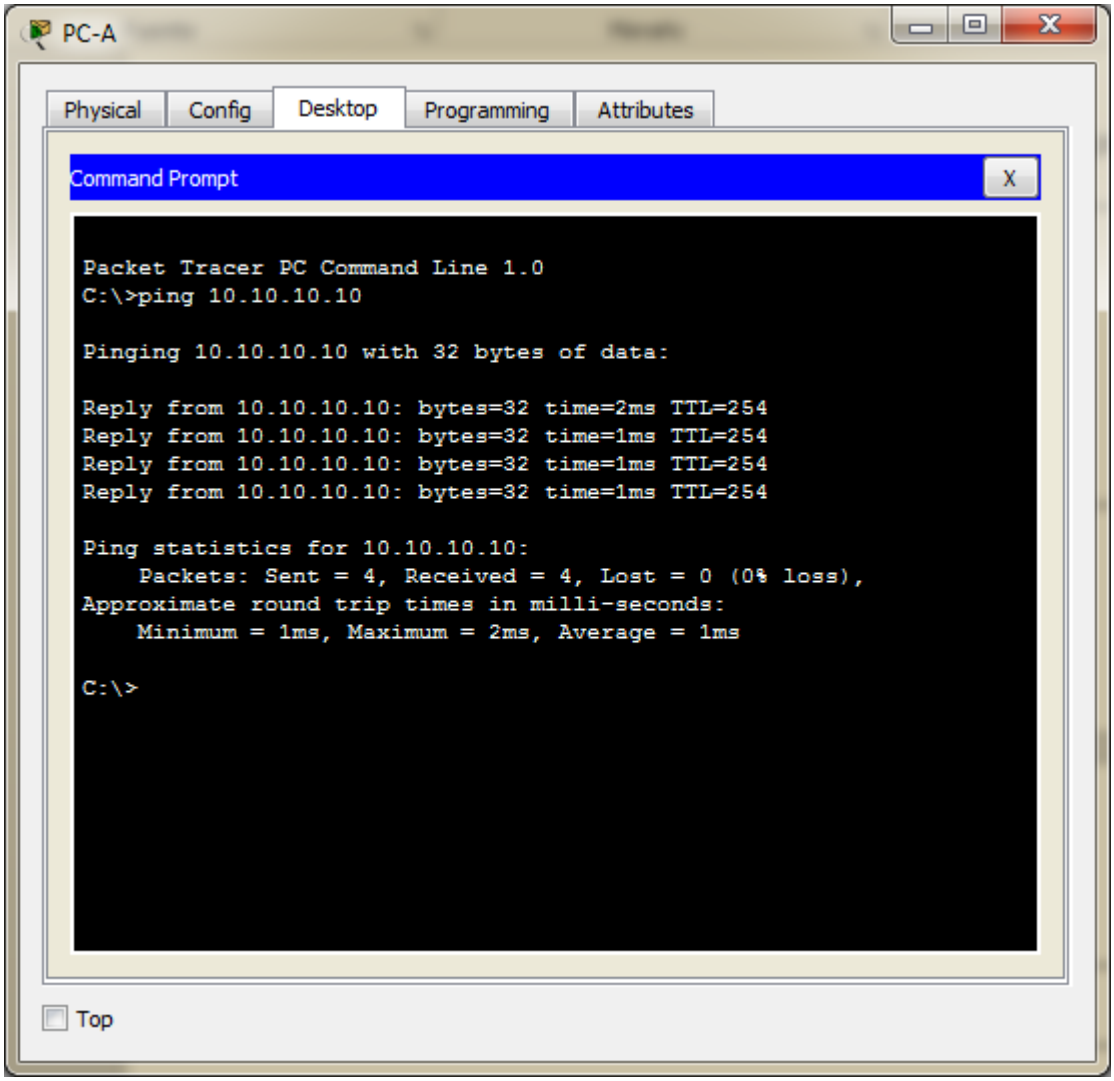
Creación de listas ACL estándar

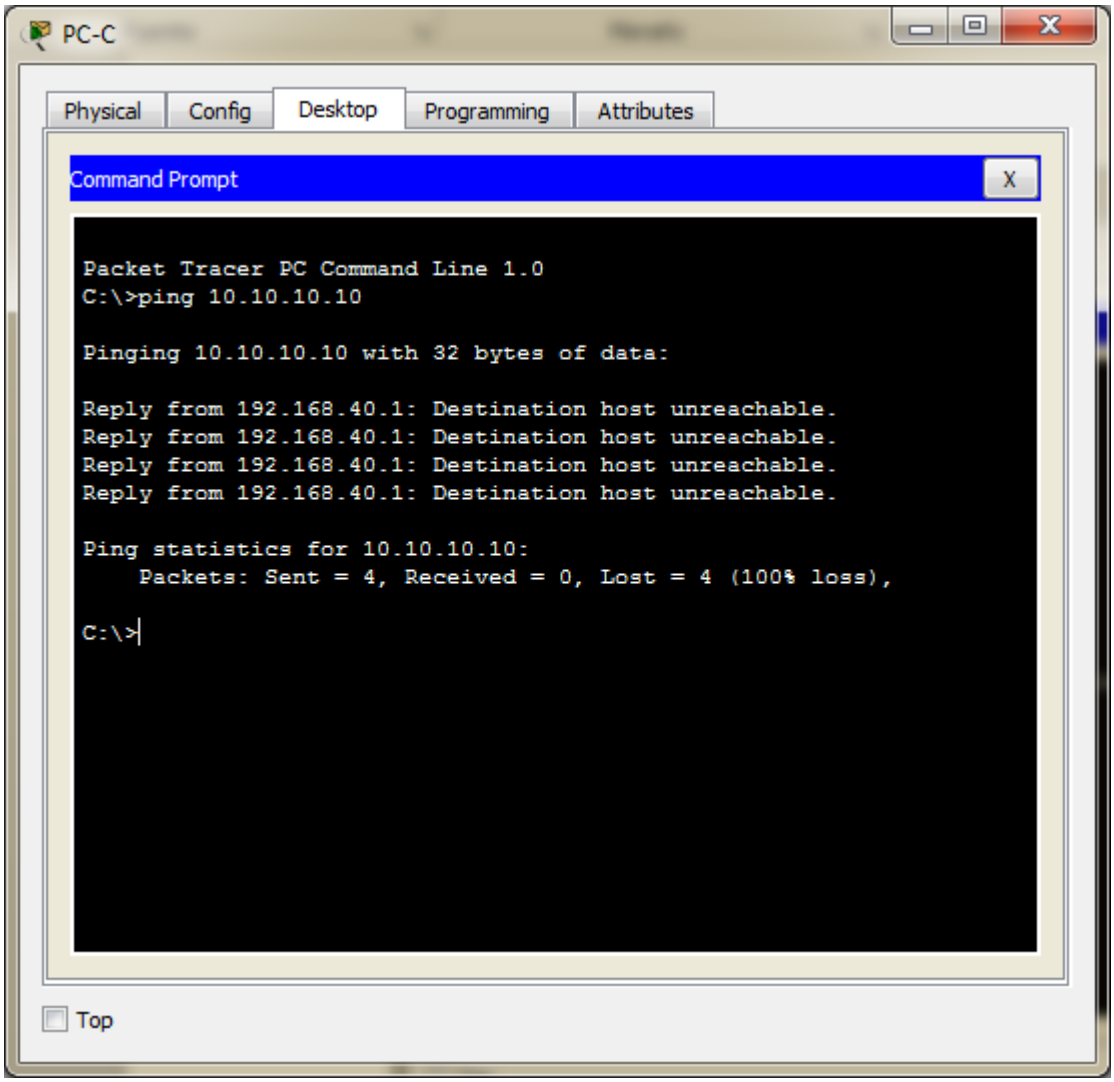
Se creará una ACL estándar de modo que solo la PC-A pueda hacer ping al servidor Web-Server en el Router 2.

```
R1(config)#ip access-list standart Denyhost
^
% Invalid input detected at '^' marker.
R1(config)#ip access-list standard Denyhost
R1(config-std-nacl)#permit host 192.168.30.31
```

```
R1(config-std-nacl)#deny any
R1(config-std-nacl)#interface s0/0/0
R1(config-if)#ip access-group Denyhost
% Incomplete command.
R1(config-if)#ip access-group Denyhost out
R1(config-if)#
```

Resultados:





La PC-C ya no puede acceder al servidor gracias a la ACL que se ha programado mientras que la PC-A aún puede hacer ping al servidor.

Creación de listas ACL extendidas

Hay dos ACL extendidas en el siguiente ejemplo en el router R1. El propósito de esta ACL es el de impedir que entre los hosts de PC-A y PC-B se puedan transferir archivos en FTP. Una segunda lista de acceso se diseña para crear una excepción para las demás rutas.

```
R1(config)#ip access-list extended NOFTP
R1(config-ext-nacl)#deny tcp 192.168.30.31 0.0.0.255 192.168.40.0 0.0.0.255 eq ftp
R1(config-ext-nacl)#deny tcp 192.168.40.31 0.0.0.255 192.168.30.31 0.0.0.255 eq ftp
```

```
R1(config-ext-nacl)#exit

R1(config)#ip access-list extended RULER
R1(config-ext-nacl)#permit tcp any 192.168.30.0 0.0.0.255
R1(config-ext-nacl)#permit tcp any 192.168.30.0 0.0.0.255 established
R1(config-ext-nacl)#permit tcp any 192.168.40.0 0.0.0.255 established
R1(config-ext-nacl)#exit
R1(config)#interface f0/0
R1(config-if)#ip access-group NOFTP in
R1(config-if)#ip access-group RULER out
R1(config-if)#^Z
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#show access-lists
Extended IP access list NOFTP
10 deny tcp 192.168.30.0 0.0.0.255 192.168.40.0 0.0.0.255 eq ftp
20 deny tcp 192.168.40.0 0.0.0.255 192.168.30.0 0.0.0.255 eq ftp
Extended IP access list RULER
10 permit tcp any 192.168.30.0 0.0.0.255
20 permit tcp any 192.168.30.0 0.0.0.255 established
30 permit tcp any 192.168.40.0 0.0.0.255 established

R1#
```

PRUEBAS DE CONECTIVIDAD

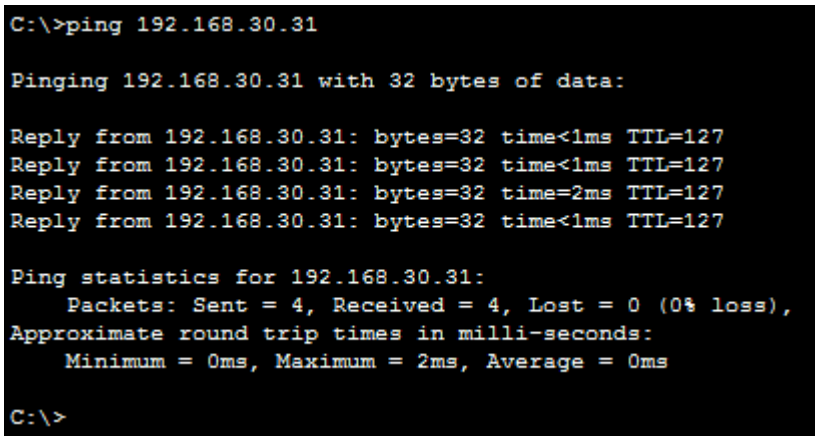
El último paso consiste en crear pruebas de conectividad entre los dispositivos. Va a hacerse una demostración de funcionalidad de los dispositivos existentes para probar si hacen ping a cada uno de los diferentes dispositivos.

PC-A ping a PC-C

```
C:\>PING 192.168.40.31

Pinging 192.168.40.31 with 32 bytes of data:

Reply from 192.168.40.31: bytes=32 time=1ms TTL=127
Reply from 192.168.40.31: bytes=32 time<1ms TTL=127
Reply from 192.168.40.31: bytes=32 time<1ms TTL=127
Reply from 192.168.40.31: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.40.31:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

El ping que se hace a la PC-C la cual tiene una dirección de 192.168.40.31 se realizó de forma exitosa. Por lo tanto las direcciones DHCP y conexiones se realizaron de forma exitosa.

PC-C ping a PC-A



El ping que se realiza entre la PC-C a la PC-A funciona de manera exitosa. La configuración se hizo de forma exitosa.

Comprobar conexión con el Router 3

En el Router 3 se planeaba probar las conexiones de la PC-A a cualquiera de las redes del Router R3. Sin embargo no se presentaba ninguna conexión por lo que se hicieron algunos ajustes:

- Agregar una ruta estática entre el Router R2 al Router R1
- Agregar una ruta estática entre el router R2 al R3

Ruta estática en R2

R2(config)#ip route 0.0.0.0 0.0.0.0 172.31.23.2

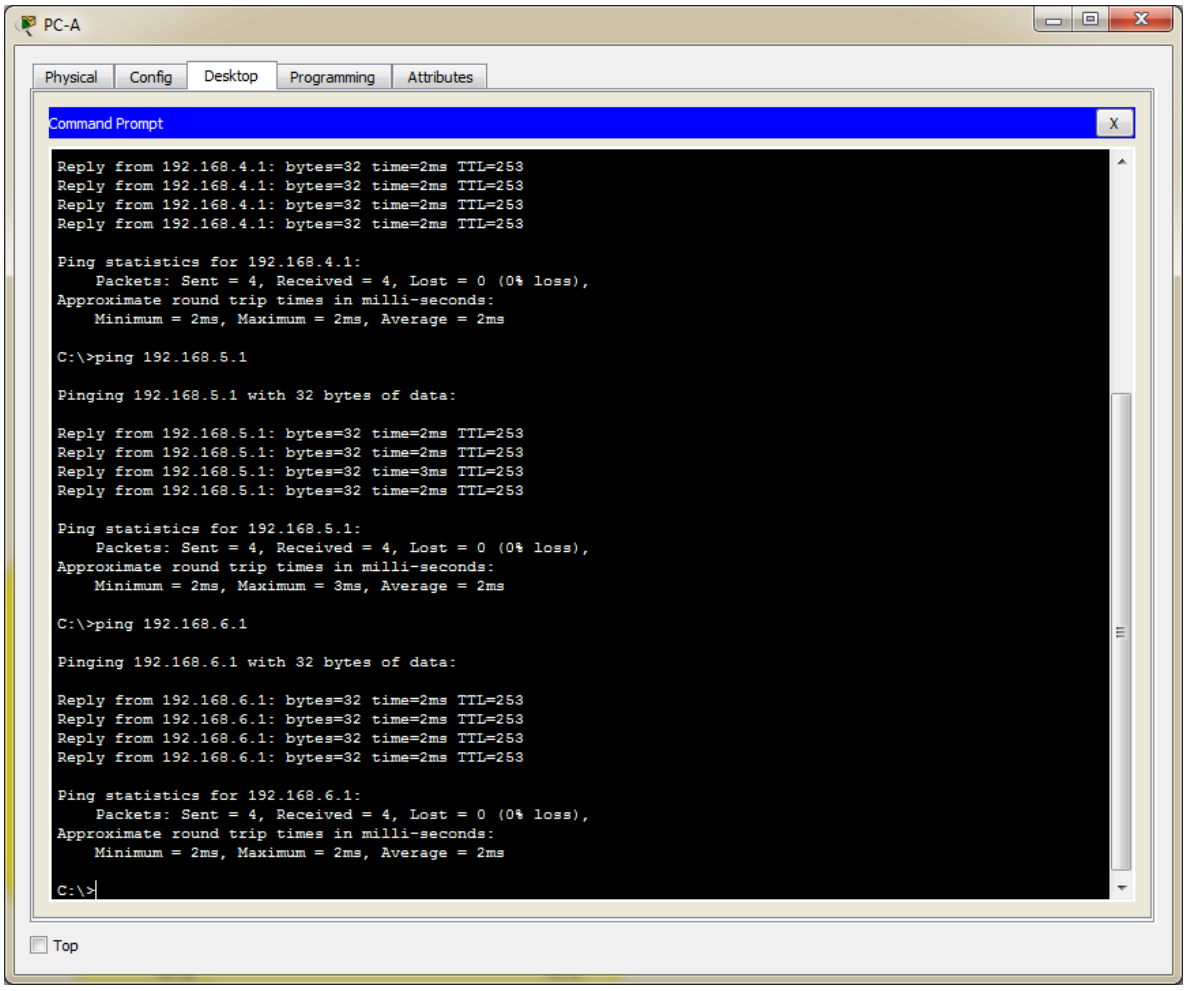
Ruta estática en R3

R3(config)#ip route 0.0.0.0 0.0.0.0 172.31.23.1

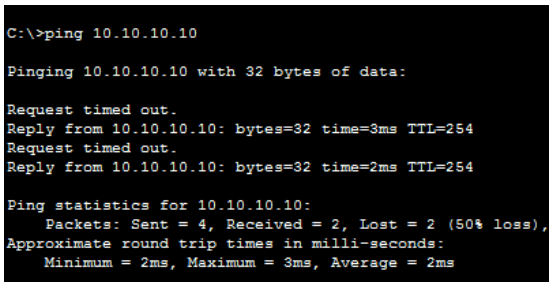
Luego se prosiguió a configurar una dirección NAT en R3

```
R3(config)#access-list 1 permit 192.168.99.0 0.0.0.255
R3(config)#ip nat pool public_access 209.165.200.226 209.165.200.229 netmask 255.255.255.248
R3(config)#ip nat inside source list 1 pool public_access overload
R3(config)#interface Serial0/0/1
R3(config-if)#ip nat inside
```

Prueba de Ping en la PC-A



El único inconveniente que se presenta reside en que el Ping hacia R2 no se realiza de forma exacta debido a que las rutas estáticas interfieren entre sí.



La PC-C de todos modos no puede acceder y hacer ping a las otras redes debido a las restricciones que se han establecido en las listas ACL.

PC-A a PC Internet

```
Pinging 209.165.205.230 with 32 bytes of data:

Reply from 209.165.205.230: bytes=32 time=3ms TTL=125
Reply from 209.165.205.230: bytes=32 time=4ms TTL=125
Reply from 209.165.205.230: bytes=32 time=3ms TTL=125
Reply from 209.165.205.230: bytes=32 time=3ms TTL=125

Ping statistics for 209.165.205.230:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 4ms, Average = 3ms
```

PC-A a PC Internet 2

```
Reply from 209.165.200.230: bytes=32 time=3ms TTL=124
Reply from 209.165.200.230: bytes=32 time=4ms TTL=124
Reply from 209.165.200.230: bytes=32 time=3ms TTL=124
Reply from 209.165.200.230: bytes=32 time=3ms TTL=124

Ping statistics for 209.165.200.230:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 4ms, Average = 3ms
```

PC Internet 2 a PC-A

```
Pinging 192.168.30.31 with 32 bytes of data:

Reply from 192.168.30.31: bytes=32 time=1ms TTL=126
Reply from 192.168.30.31: bytes=32 time=3ms TTL=126
Reply from 192.168.30.31: bytes=32 time=3ms TTL=126
Reply from 192.168.30.31: bytes=32 time=7ms TTL=126

Ping statistics for 192.168.30.31:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 7ms, Average = 3ms
```

PC Internet 2 a PC Internet

```
Reply from 209.165.200.230: bytes=32 time<1ms TTL=128
Reply from 209.165.200.230: bytes=32 time=4ms TTL=128
Reply from 209.165.200.230: bytes=32 time=3ms TTL=128
Reply from 209.165.200.230: bytes=32 time=10ms TTL=128

Ping statistics for 209.165.200.230:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 10ms, Average = 4ms
```

PC Internet a PC-A

```
Pinging 192.168.30.31 with 32 bytes of data:

Reply from 192.168.30.31: bytes=32 time=6ms TTL=125
Reply from 192.168.30.31: bytes=32 time=3ms TTL=125
Reply from 192.168.30.31: bytes=32 time=9ms TTL=125
Reply from 192.168.30.31: bytes=32 time=3ms TTL=125

Ping statistics for 192.168.30.31:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 9ms, Average = 5ms
```

PC Internet a PC Internet 2

```
C:\>ping 209.165.205.230

Pinging 209.165.205.230 with 32 bytes of data:

Reply from 209.165.205.230: bytes=32 time<1ms TTL=128
Reply from 209.165.205.230: bytes=32 time=3ms TTL=128
Reply from 209.165.205.230: bytes=32 time=5ms TTL=128
Reply from 209.165.205.230: bytes=32 time<1ms TTL=128

Ping statistics for 209.165.205.230:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 5ms, Average = 2ms
```

CONCLUSIONES

Como resultado de la práctica final, se consiguió solucionar los diferentes problemas que se presentaron en la topología. El curso de Cisco ha sido muy útil para aprender de forma dinámica y sencilla el cómo diseñar una red e implementar las diferentes medidas para mejorar su rendimiento. Estos conocimientos pueden aplicarse desde las pequeñas empresas hasta las más grandes, las prácticas de laboratorio permitieron practicar de forma constante las lecciones de las cuales se compone el curso de Cisco.

Considero la experiencia del curso gratificante y es un paso más para terminar mis estudios en el área de ingeniería de sistemas. Se ha explorado con mayor detalle sobre el funcionamiento de las redes, sus componentes y como se pueden hacer mejores diseños. La práctica final y los otros ejercicios de laboratorio desarrollados en todo el curso permitieron ampliar mis conocimientos en el tema de las redes y mantenerme al tanto de las nuevas tecnologías que existen para su diseño.

Gracias a la práctica final y los cursos de Cisco, he logrado dar pasos significativos para terminar mis estudios en el área de ingeniería de sistema, y la estructura del curso fue muy bien diseñada para aprender de manera fácil y efectiva cada una de las lecciones correspondientes al tema del manejo de las redes, lo que se ha logrado con dedicación, trabajo duro y un contacto constante con los compañeros de curso y los tutores asignados quienes han ayudado en el curso de diplomado de profundización de redes.

BIBLIOGRAFIA

Cisco NetAcademy- Capitulo 3 Vlan. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE50ES/module3/index.html

Cisco NetAcademy- Capítulo 6 Enrutamiento estático. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE50ES/module6/index.html#6.0.1.1

Cisco NetAcademy- Capítulo 8 OSPF de área única. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE50ES/module8/index.html#8.0.1.1

Cisco NetAcademy- Capítulo 9 Lista de control de acceso. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE50ES/module9/index.html#9.0.1.1

Cisco NetAcademy- Capítulo 11 traducciones de direcciones de red para IPv4. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE50ES/module11/index.html#11.0.1.1