PRUEBA DE HABILIDADES PRÁCTICAS

Presenta

ANA FRANCENE BAUTISTA LARGO

1051240470

Presentado a

GIOVANNI ALBERTO BRACHO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BASICAS TECNOLOGIA E INGENIERIA
DIPLOMADO DE PROFUNDIZACIÓN CISCO (DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN / WAN)
2018

Introducción

La implantación de herramientas de simulación como *Packet Tracer* permite realizar diseños de topologías de red y/o configuración de dispositivos, ya que brinda la posibilidad de analizar cada proceso que se ejecuta de acuerdo a la capa del modelo OSI, puesto que se puede detectar y corregir errores potenciales dentro del sistema de comunicación en el cual se realizan las configuraciones básicas y necesarias que permiten interconectar entre sí cada uno de los dispositivos que forman parte del escenario. Por lo tanto se implementan los lineamientos establecidos para el direccionamiento IP, protocolos de enrutamiento y demás aspectos que forman parte de la topología de red.

Dentro del desarrollo del presente documento se realiza la simulación de un entorno de Redes de comunicaciones, creando topologías de Red mediante la selección de los dispositivos y su respectiva ubicación en el área de trabajo.

Dentro de los aspectos más importantes en el desarrollo de la topología propuesta se destaca la simulación de la implementación del Protocolo de Información de Encaminamiento RIP V2 (protocolo de puerta de enlace interna – Interior Gateway Protocol, IGP), Protocolo de Configuración Dinámica de Host (DHCP) que proporciona además de la puerta de enlace predeterminada y la máscara de subred, un host de protocolo Internet (IP) con su dirección IP automáticamente.
Así mismo, se realiza implementación de la conversión de direcciones de red o NAT, el principio de NAT consiste en utilizar una conexión de pasarela a Internet, que tenga al menos una interfaz de red conectada a la red interna y al menos una interfaz de red conectada a Internet (con una dirección IP enrutable) para poder conectar todos los equipos a la red.
De igual forma se simula el funcionamiento de las ACLs tanto extendidas como de tipo estándar. Sabemos que las primeras son más eficientes en cuanto al filtrado. Sin embargo tanto extendidas como estándar, las ACLs son mecanismos de clasificación de tráfico y direcciones.

Finalmente, aunque no menos importante, se realiza la configuración básica de los dispositivos presentes en el escenario; es decir, configuración del direccionamiento IP acorde con la topología de red, VLANs, puertos troncales y de acceso, encapsulamiento, seguridad, configuración de las listas de acceso e identificar los correctos procesos de comunicación y redireccionamiento de tráfico de datos entre terminales mediante el uso de comandos como PING y TRACEROUTE.

Objetivos

Objetivo General

Aplicar los conocimientos adquiridos sobre configuración de Redes utilizando herramientas de simulación.

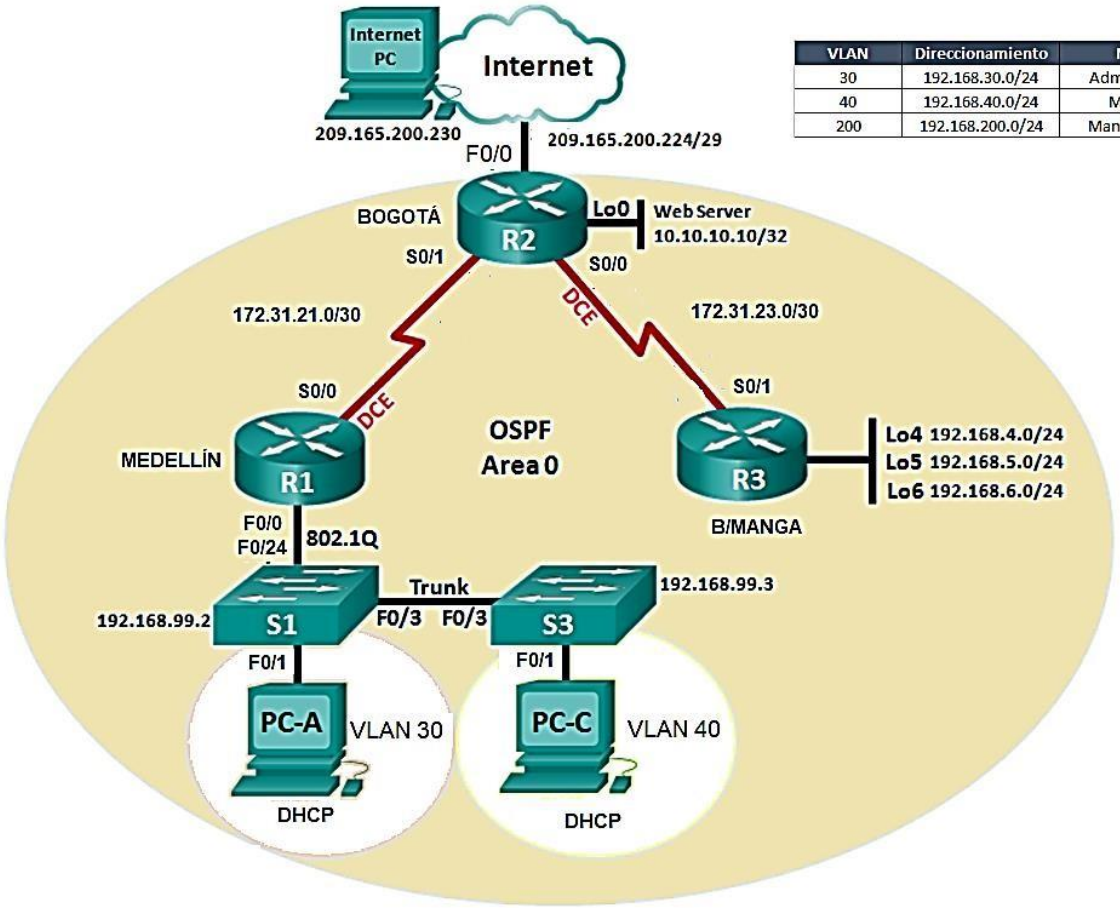
Objetivos Específicos

- Configurar el protocolo de enrutamiento OSPFv2.
- Realizar la configuración de los ajustes de los dispositivos.
- Asignar direcciones IPV4.
- Establecer la configuración y direccionamiento de las interfaces de Routers y Switches.
- Limitar el acceso a los dispositivos mediante configuración ACL.
- Configurar VLAN y enlaces troncales.

Descripción del escenario propuesto para la prueba de habilidades

Escenario: 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.

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

   En primer lugar inicializamos los dispositivos (Routers, switches, PCs)
   La configuración se realiza haciendo uso de los comandos:
   `enable`
   `configure terminal`
   `no ip domain-lookup`
   `hostname`

   Lo que se pretende es ingresar por el modo privilegiado `(enable)` y asignar nombre a los dispositivos (`hostname`).

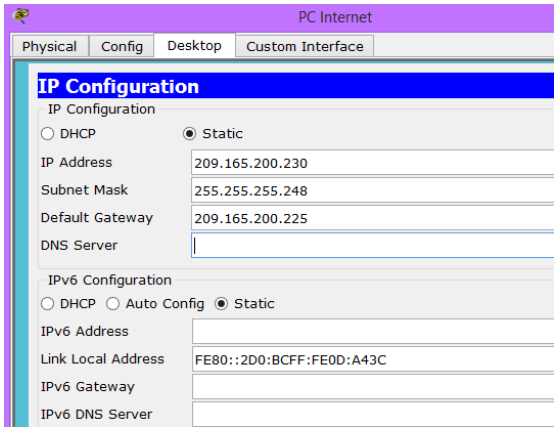


Ilustración 1. PC Internet

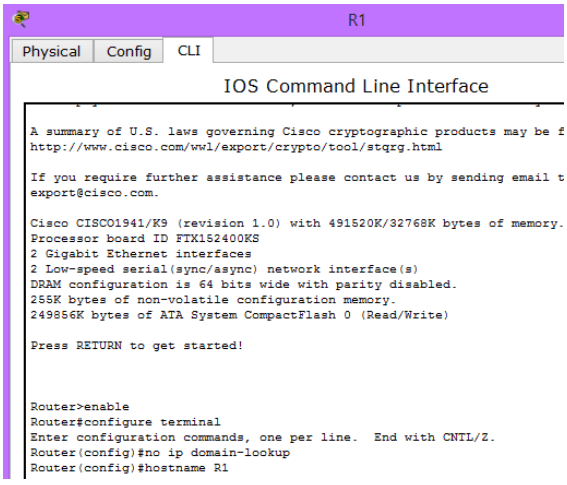


Ilustración 2. Router 1

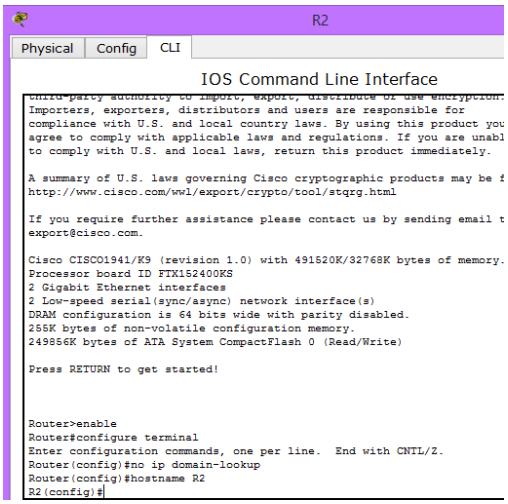


Ilustración 3. Router 2

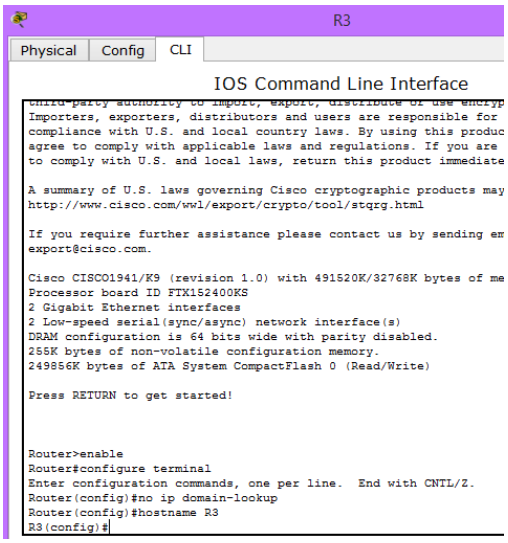


Ilustración 4. Router 3

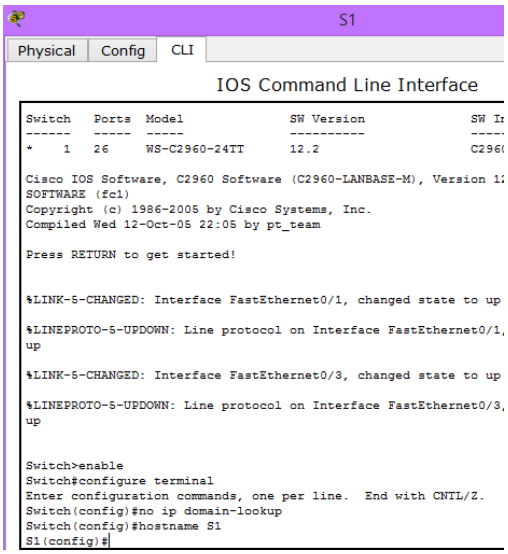


Ilustración 5. Switch 1

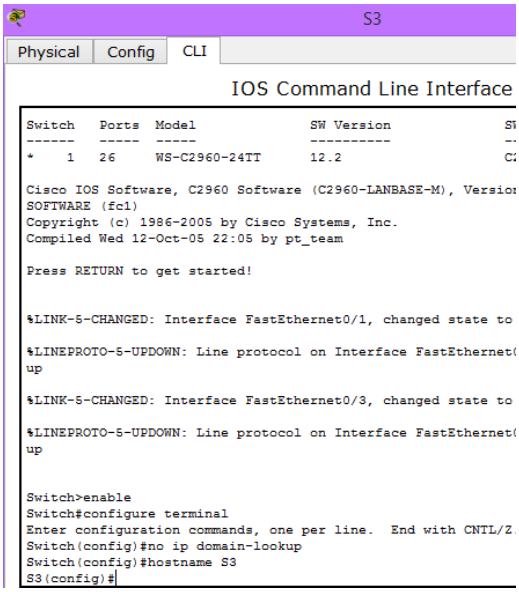


Ilustración 6. Switch 3

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

OSPFv2 area 0

Configuration Item or Task	Specification
Router ID R1	1.1.1.1
Router ID R2	2.2.2.2
Router ID R3	3.3.3.3

Configurar todas las interfaces LAN como pasivas	
Establecer el ancho de banda para enlaces seriales en	128 Kb/s
Ajustar el costo en la métrica de S0/0 a	7500

Verificar información de OSPF

• Visualizar tablas de enrutamiento y routers conectados por OSPFv2

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

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

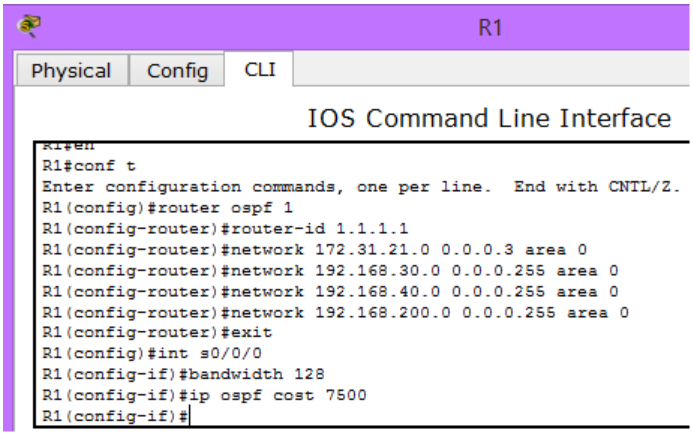


Ilustración 7. OSPF en Router 1

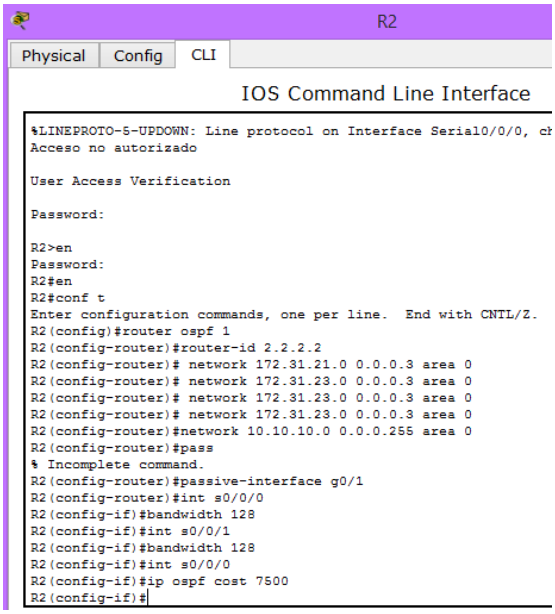


Ilustración 8. OSPF en Router 2

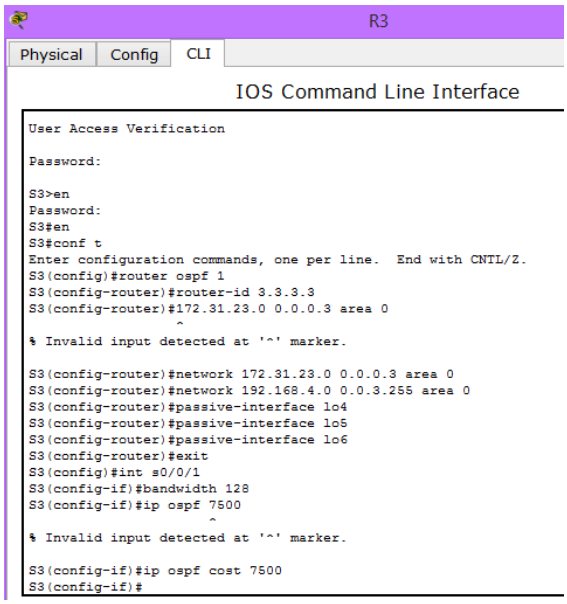


Ilustración 9. OSPF en Router 3

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

   En la configuración de las VLAN hacemos uso de los comandos:
   `vlan`
   `name`

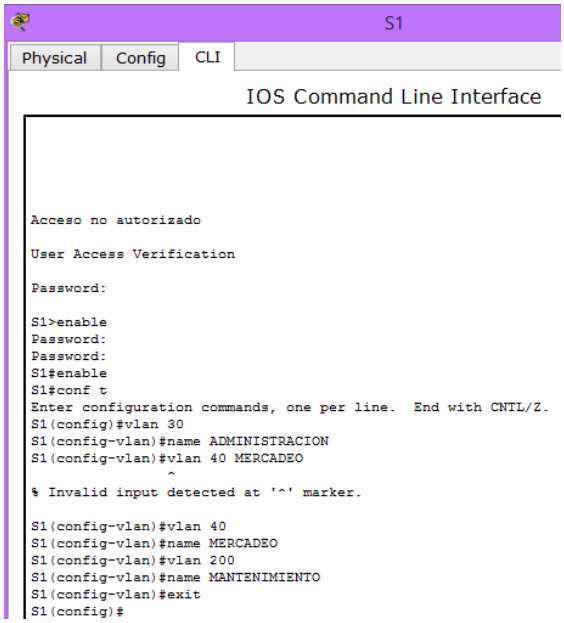


Ilustración 10. VLAN (Switch 1)

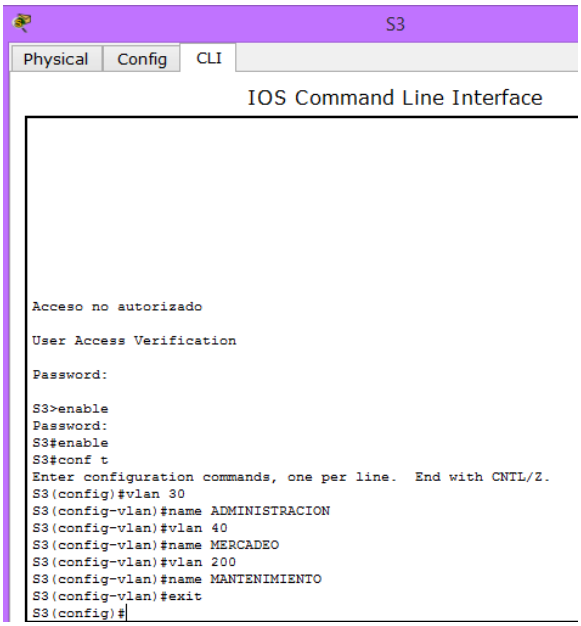


Ilustración 11. VLAN (Switch 3)

En el caso de los puertos troncales utilizamos los comandos:

`switchport mode trunk`

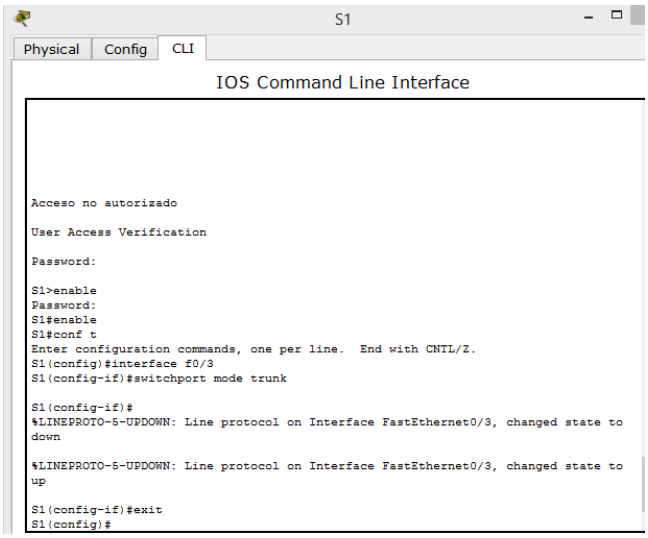


Ilustración 12. Puerto Troncal Switch 1

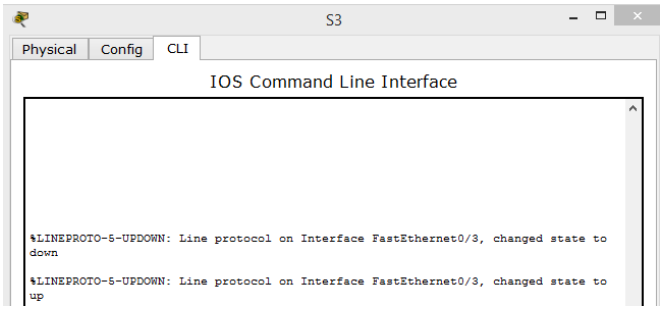


Ilustración 13. . Puerto Troncal Switch 3

A continuación se configura Inter-VLAN Routing y Seguridad en los Switches:

```
no ip domain-lookup
hostname S1
enable secret class
line console 0
password cisco
login
line vty 0 4
password cisco
login
service password-encryption
banner motd %Acceso no autorizado%
```

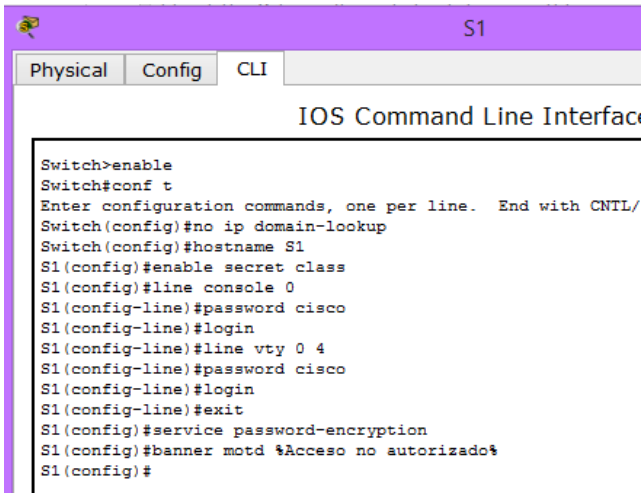


Ilustración 14. Switch 1

Ilustración 15. Switch 3

4. **En el Switch 3 deshabilitar DNS lookup**

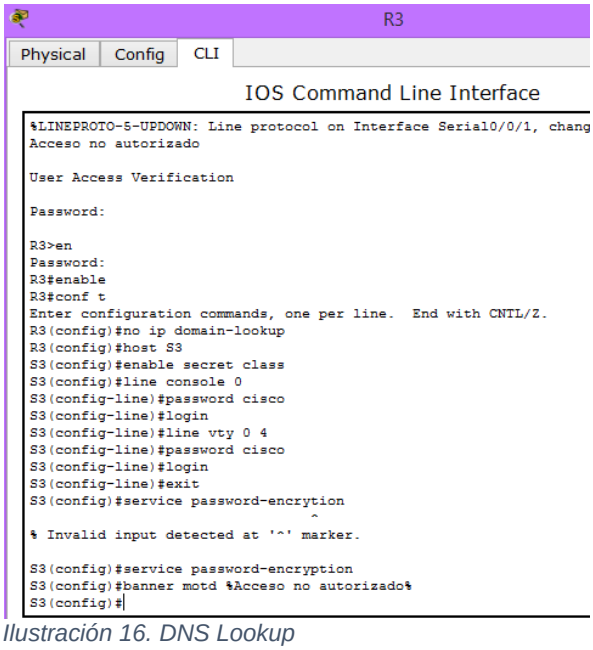


Ilustración 16. DNS Lookup

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

Se asigna la dirección IP al Switch 1 (192.168.99.2)

```
ip address
no shutdown
```

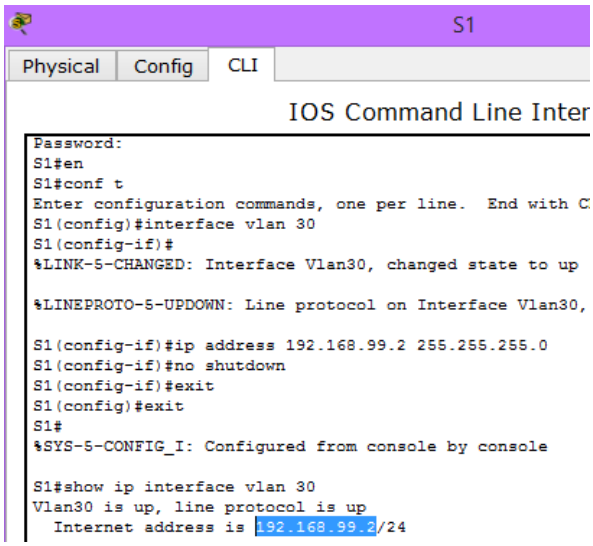


Ilustración 17. IP Switch 1

Se asigna la IP al Switch 3 (192.168.99.3)

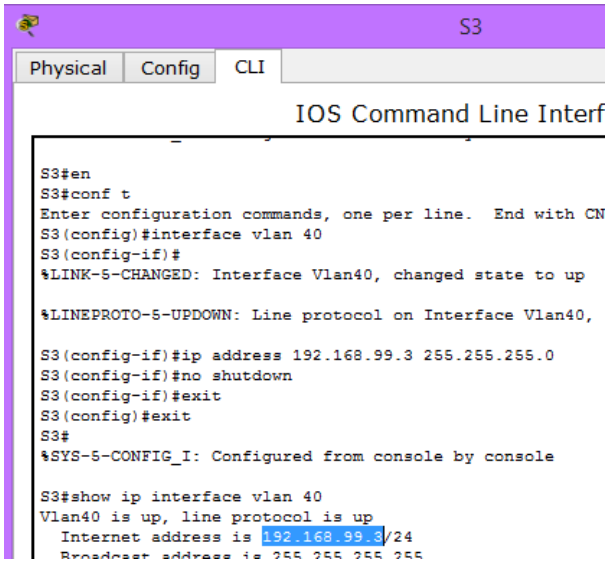


Ilustración 18. IP Switch 3

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

   Para ello ingresamos al Switch 3, donde ingresamos el comando `int range:`

Ilustración 19. Interfaces no utilizadas

7. **Implement DHCP and NAT for IPv4.**

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

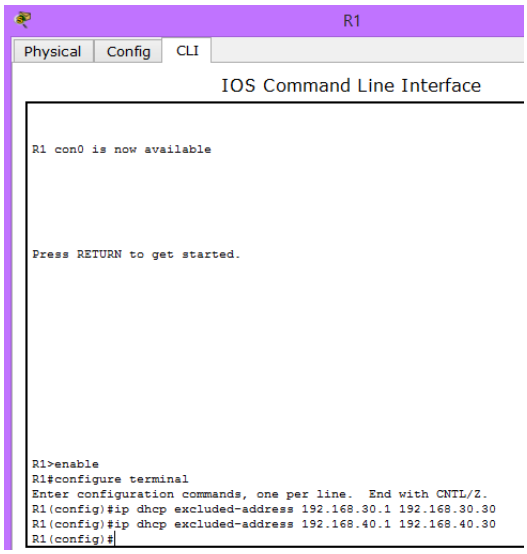


Ilustración 20. Servidor DHCP

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

   Para esta configuración ingresamos los comandos:

   ```
   ip dhcp pool
   network
   dns-server
   domain-name
   default router
   ```

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

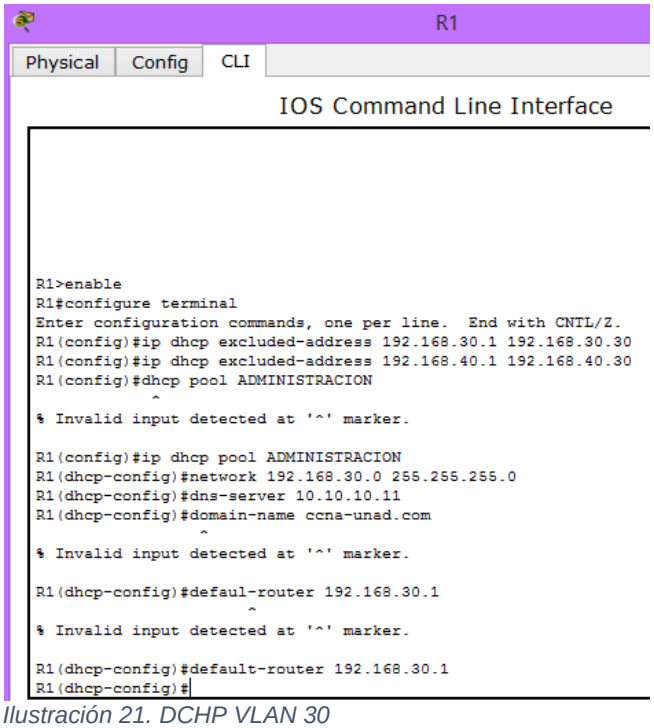


Ilustración 21. DCHP VLAN 30

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

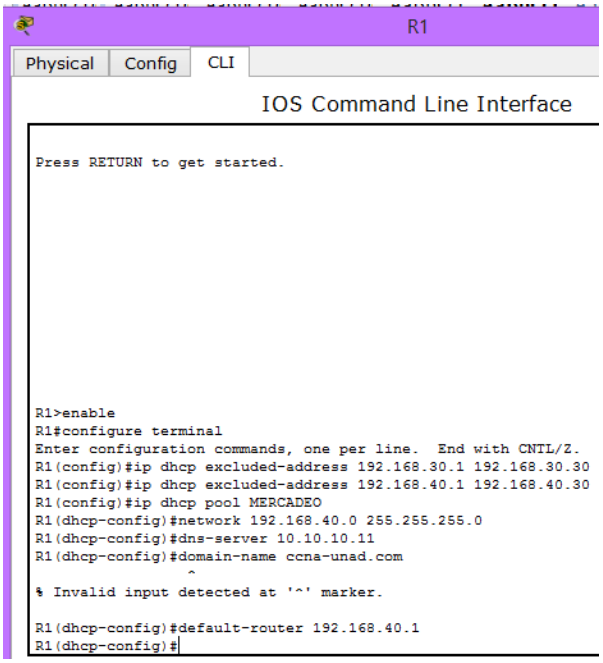
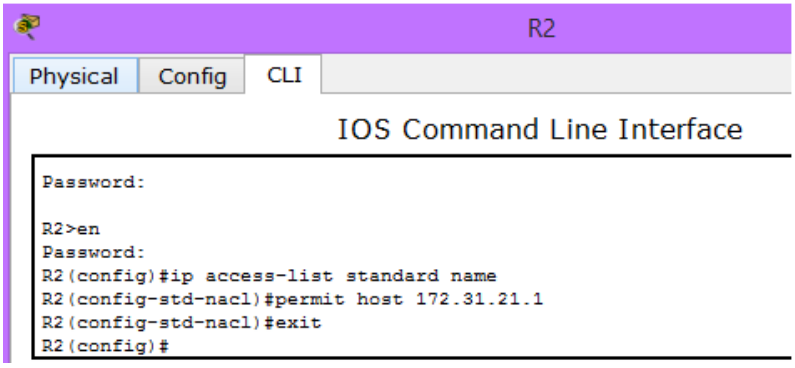


Ilustración 22. DCHP VLAN 40

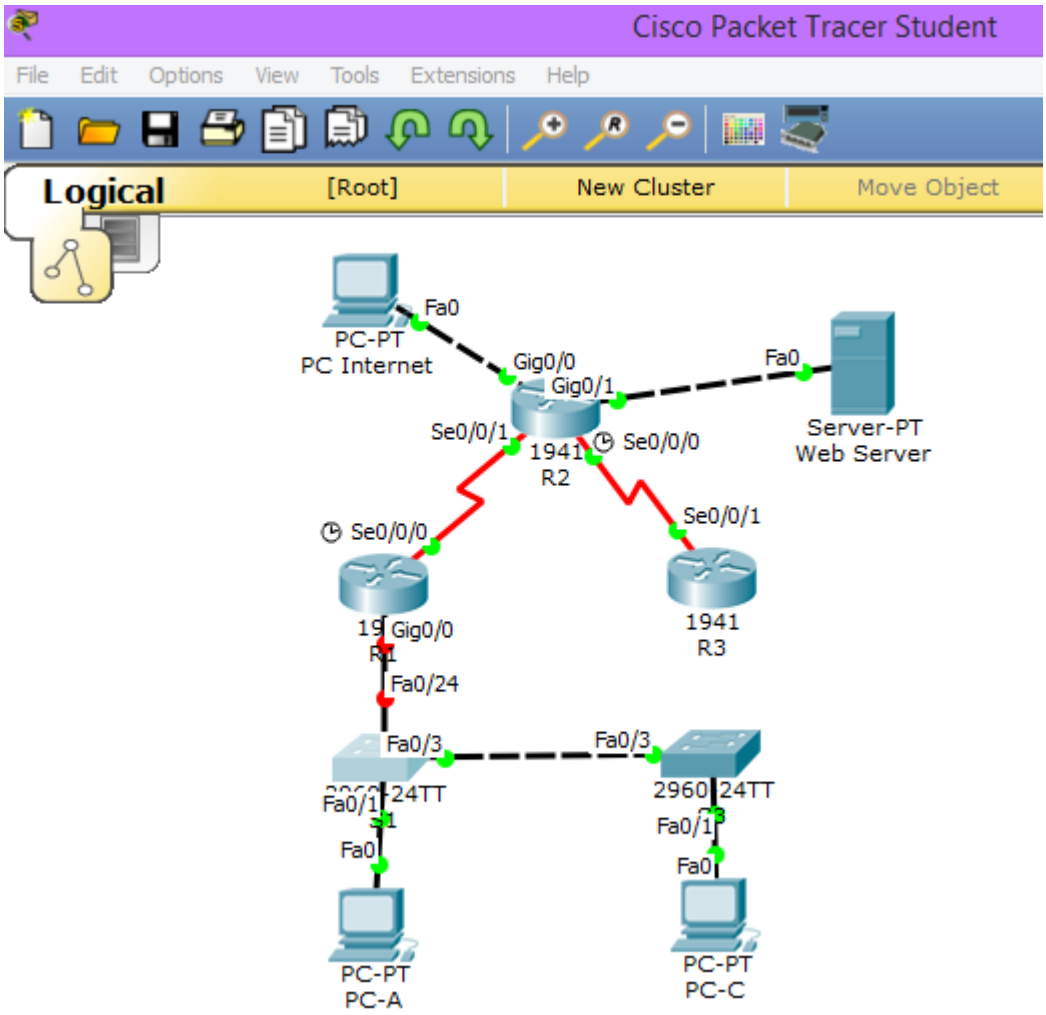
10. **Configurar NAT en R2 para permitir que los host puedan salir a internet.**
11. Configurar al menos dos listas de acceso de tipo extendido o nombradas a su criterio en para restringir o permitir tráfico desde R1 o R3 hacia R2.
12. **Configurar al menos dos listas de acceso de tipo estándar a su criterio para restringir o permitir tráfico desde R1 o R3 hacia R2.**

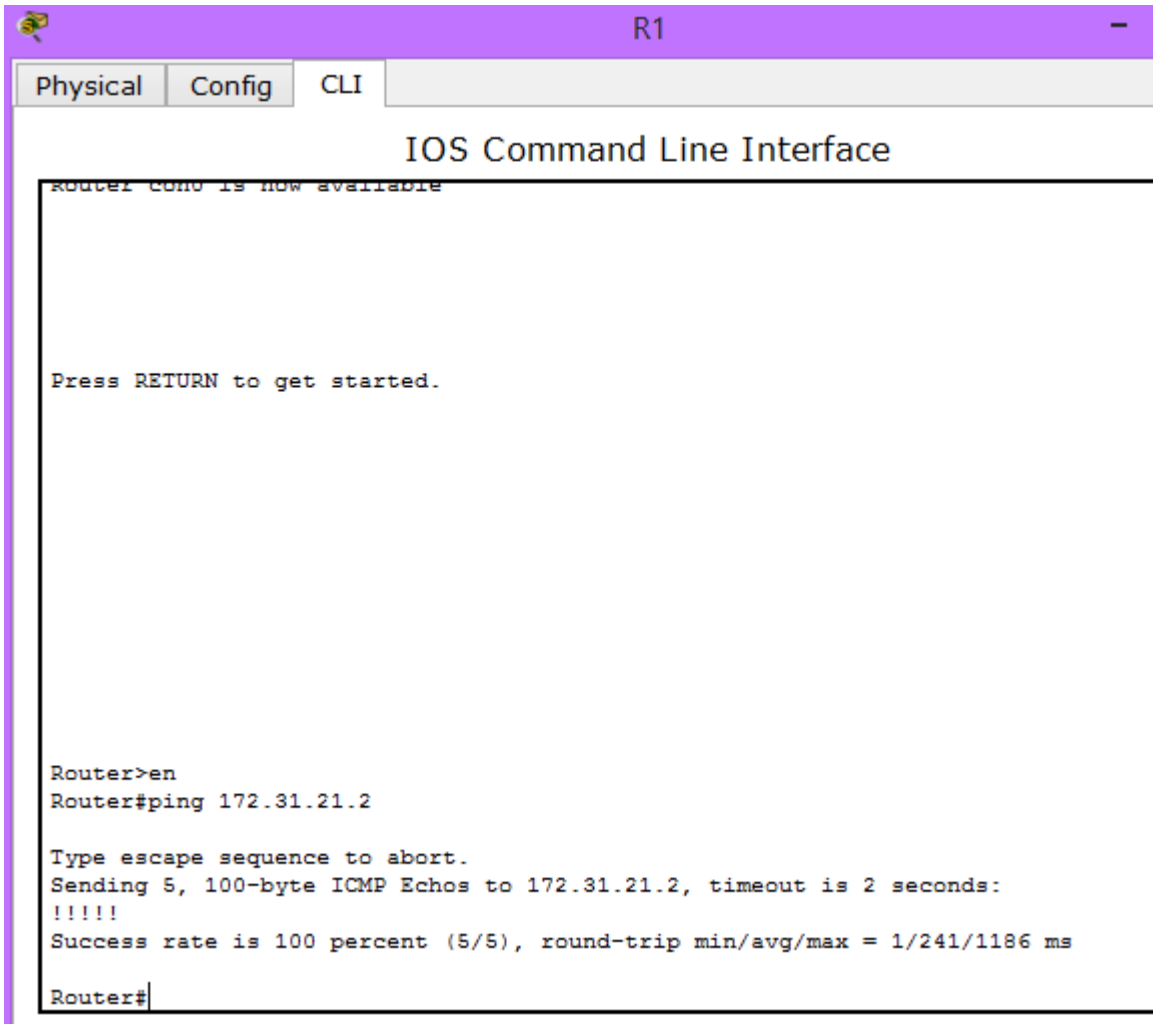
    En este caso implementamos el comando `permit` host para autorizar a R1 enviar tráfico a R3:

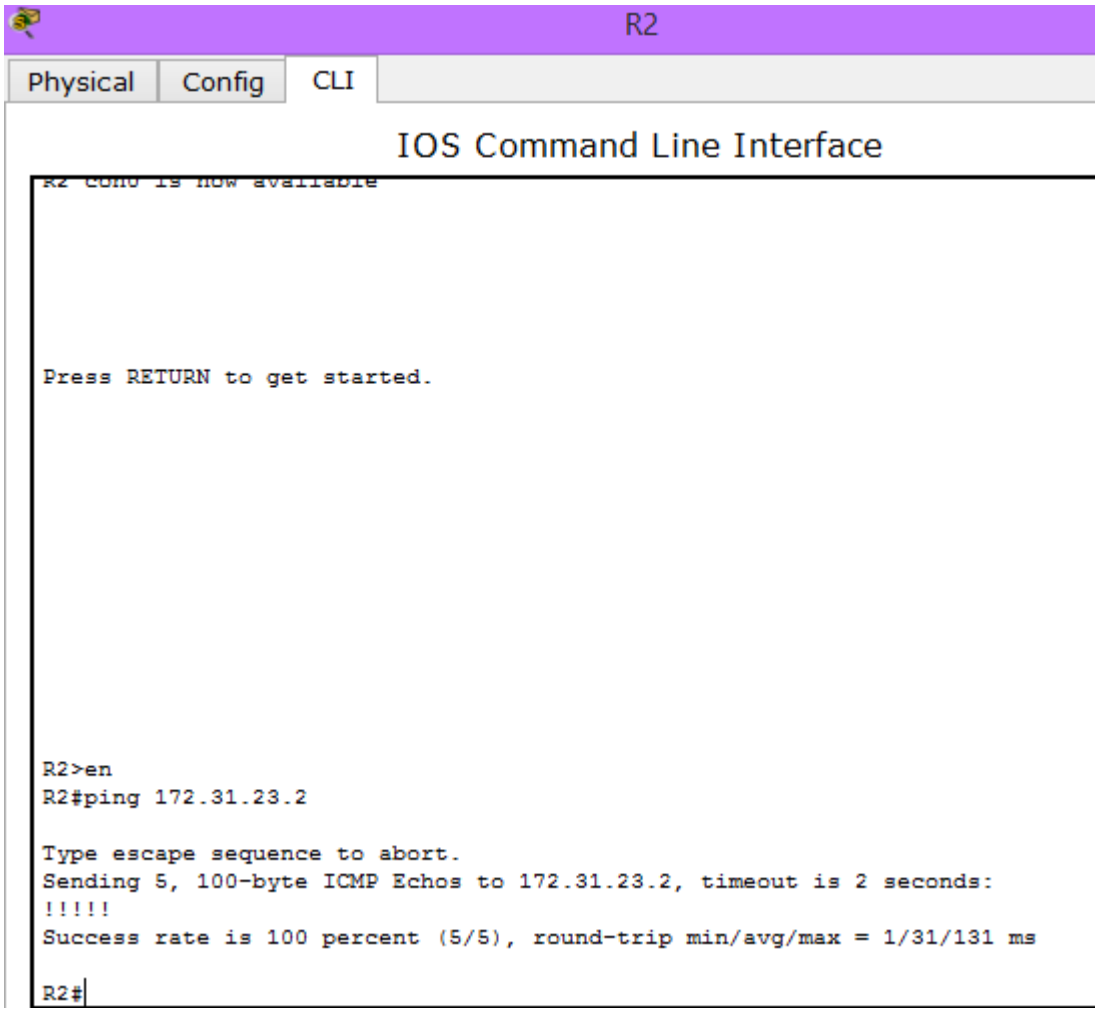
    `ip access-list standar`



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


Cisco Packet Tracer Student
File
Edit
Options
View
Tools
Extensions
Help
Logical
[Root]
New Cluster
Move Object
PC-PT
PC Internet
Fa0
Gig0/0
Gig0/1
Fa0
Server-PT
Web Server
Se0/0/1
1941
R2
Se0/0/0
Se0/0/0
Se0/0/1
1941
R3
Gig0/0
Fa0/24
Fa0/3
Fa0/3
2960 24TT
Fa0/1
Fa0/1
Fa0
Fa0
PC-PT
PC-A
PC-PT
PC-C


R1
Physical
Config
CLI
IOS Command Line Interface
Router con0 is now available
Press RETURN to get started.
Router>en
Router#ping 172.31.21.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.31.21.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/241/1186 ms
Router#


R2
Physical
Config
CLI
IOS Command Line Interface
R2 con0 is now available
Press RETURN to get started.
R2>en
R2#ping 172.31.23.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.31.23.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/31/131 ms
R2#

Conclusiones

Tras realizar el procedimiento para la configuración de OPSF, se entiende que en primera medida se entra por el modo de configuración global (configure terminal) el cual activa el protocolo OSPF en el Router.

Se comprenden los conceptos básicos de los protocolos de enrutamiento y su funcionamiento principal; el cual se ejecuta de manera simultánea en varios routers con el objetivo de completar y actualizar su tabla de enrutamiento recorriendo los menores caminos posibles para intercambiar información con otras redes.

Se distingue el protocolo RIP (Rourter Information Protocol) por ser uno de los más importantes en implementarse y servir de base para la evolución de los protocolos de enrutamiento dinámico.

Se implementó la configuración DHCP; haciendo uso del comando ip dhcp pool, el cual crea un conjunto de IPs con el nombre asignado y provoca que el Router entre en el modo de configuración DHCP.

Se comprendió el concepto de NAT estática, como el mecanismo usado por los Routers para intercambiar paquetes entre dos redes que tienen distintas direcciones.
De igual forma se adquieron conocimientos acerca de NAT dinámica, donde el Router va elegir qué direccionamiento agregarle al paquete para que pueda salir a internet, dicha elección la realiza dentro de una lista de direcciones disponibles.

Se verificó conexión entre distintos dispositivos, con el objetivo de comprobar si la misma era estable, para ello se implentó el comando ping.
Así mismo, se efectuaron verificaciones de diagnóstico en las conexiones, con el comando Traceroute, la diferencia encontrada es que al enviar una serie de paquetes nos muestra además la ruta que toma hasta llegar al destino, indicando además, los hosts por los que va pasando y el tiempo que toma en cada salto. En conjunto tanto ping como traceroute nos indican si tenemos una pérdida de paquetes y dónde exactamente se presentó la falla.

Bibliografía

Omarbetas. (2016). Protocolos DHCP, ICMP, NAT y ARP. Recuperado de https://telematicos2.wordpress.com/2016/06/07/protocolos-dhcp-icmp-nat-y-arp/

CISCO. (2014). Protocolos y comunicaciones de red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#3.0.1.1

CISCO. (2014). Acceso a la red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#4.0.1.1

CISCO. (2014). Ethernet. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#5.0.1.1

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

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

CISCO. (2014). Asignación de direcciones IP. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN50ES/module8/index.html#8.0.1.1

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

CISCO. (2014). Capa de Aplicación. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN50ES/module10/index.html#10.0.1.1

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

UNAD (2014). Configuración de Switches y Routers [OVA]. Recuperado de: https://1drv.ms/u/s!AmIJYei-NT1IhgL9QChD1m9EuGqC

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

CISCO. (2014). VLANs. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE50ES/module3/index.html#3.0.1.1

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

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

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

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