DIPLOMADO DE PROFUNDIZACIÓN CISCO
Tarea 11. Evaluación – Prueba de habilidades prácticas CCNA
COMPONENTE PRÁCTICO
GRUPO 41

Presentado Por:
VICTOR ALFONSO OROZCO GIRALDO

Docente:
DIEGO EDINSON RAMIREZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA ECTBI
INGENIERIA DE SISTEMAS
BOGOTÁ, CUNDINAMARCA 2019

TABLA DE CONTENIDO

Pág.

TABLA DE ILUSTRACIONES

Pág.

RESUMEN

En el trabajo final de Habilidades prácticas de Cisco CCNA1 y CCNA2, se entrará a analizar dos clases de redes (WAN y LAN), con el fin de dar solución a las necesidades presentadas en los escenarios 1 y 2.

En el primer escenario nos muestra una red WAN con tres (03) redes LAN que conecta tres (03) ciudades en Colombia, establecer los lineamientos necesarios de enrutamientos en la red, lista de control de acceso, configuración eigrip y la seguridad necesaria para que la red sea segura y no presente problemas de ataques e intrusos.

En el segundo escenario se presenta una red WAN con tres (03) redes LAN en una empresa interconectadas a sus tres (03) ciudades, con unas solicitudes y requerimientos en cuanto a seguridad, arquitectura, accesos y usuarios, los cuales conllevan a un conocimiento aceptable necesario en redes para que la red funcione de acuerdo a la necesidad. El proceso se realiza utilizando la herramienta de simulación Packet Tracer, aplicando los conocimientos adquiridos en el diplomado que se presentó durante el presente semestre en la universidad abierta y a distancia UNAD.

ABSTRACT

In the final work of Practical Skills of Cisco CCNA1 and CCNA2, two kinds of networks (WAN and LAN) will be analyzed, in order to solve the needs presented in scenarios 1 and 2.

In the first scenario, it shows us a WAN network with three (03) LAN networks that connects three (03) cities in Colombia, establishing the necessary routing guidelines in the network, access control list, eigrip configuration and the necessary security so that The network is secure and has no problems with attacks and intruders.

In the second scenario, a WAN network is presented with three (03) LAN networks in a company interconnected to its three (03) cities, with some requests and requirements regarding security, architecture, access and users, which lead to knowledge Acceptable necessary in networks for the network to function according to need. The process is carried out using the Packet Tracer simulation tool, applying the knowledge acquired in the diploma that was presented during this semester at the UNAD open and distance university.

INTRODUCCCIÓN

En los escenarios propuestos para el desarrollo de la actividad, se requiere presentar unos conocimientos necesarios en redes estudiados en los dos módulos que se adquirieron en el diplomado, para ello se necesita realizar configuraciones en redes LAN y WAN, en materia de seguridad, listas de acceso, enrutamiento eigrip, servidor TFTP, DHCP, VLANS troncales, NAT, PAT, reglas mínimas de seguridad y acceso a los equipos de redes.

Es de anotar que cada escenario se puede presentar como las necesidades propias de una empresa prestadora de servicio o una empresa normal con sedes en diferentes ciudades, el requerimiento de poder conectar toda su infraestructura, seguridad y accesos a la internet para la sostenibilidad del negocio.

Por último, dar a conocer al tutor todos los conocimientos adquiridos en el diplomado de profundización cisco (diseño e implementación de soluciones integradas LAN / WAN).

OBJETIVOS

OBJETIVO GENERAL

Aprender a configurar redes WAN y LAN según las necesidades de las empresas para brindar las comunicaciones a las necesidades propias del cliente.

OBJETIVOS ESPECÍFICOS

- Configurar listas de acceso necesarias para las comunicaciones directas, ya sea en una red LAN o WAN.
- Realizar conexiones a través de NAT o PAT entre IP privadas y públicas según las necesidades de comunicación entre las redes de la empresa.
- Crear vlans en las redes internas, con el fin de dar comunicación exclusiva y detallada a cada uno de los segmentos de red.
- Realizar configuraciones de enrutamiento OSPF y EIGRIP según lo requerido en cada uno de los escenarios propuestos.
- Aprender a configurar servidores TFTP y DHCP, para dar mayor agilidad y velocidad al sistema en las redes y más automático

DESARROLLO DE CONTENIDO

ESCENARIO 1

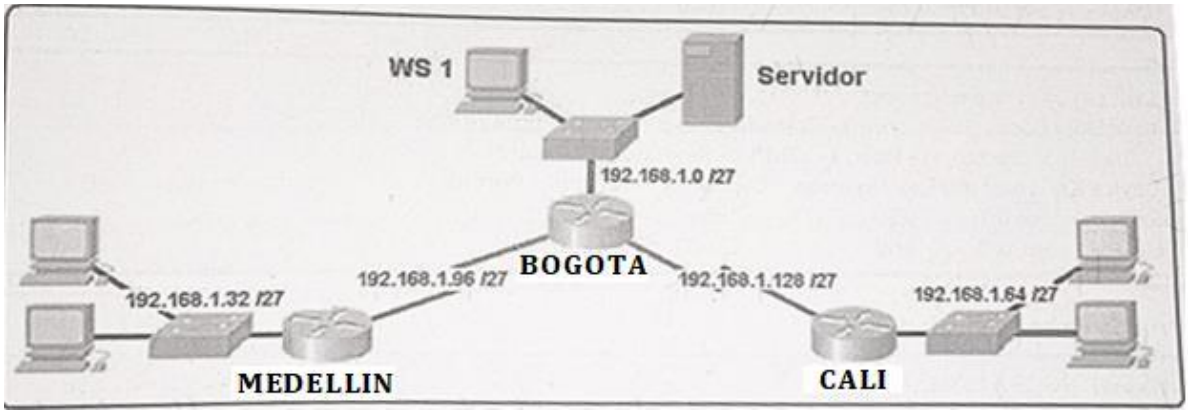
Una empresa posee sucursales distribuidas en las ciudades de Bogotá, Medellín y Cali en donde el estudiante será el administrador de la red, el cual deberá configurar e interconectar entre sí cada uno de los dispositivos que forman parte del escenario, acorde con los lineamientos establecidos para el direccionamiento IP, protocolos de enrutamiento y demás aspectos que forman parte de la topología de red.

TOPOLOGÍA DE RED

Los requerimientos solicitados son los siguientes:

Parte 1: Para el direccionamiento IP debe definirse una dirección de acuerdo con el número de hosts requeridos.
Parte 2: Considerar la asignación de los parámetros básicos y la detección de vecinos directamente conectados.
Parte 3: La red y subred establecidas deberán tener una interconexión total, todos los hosts deberán ser
visibles y poder comunicarse entre ellos sin restricciones.
Parte 4: Implementar la seguridad en la red, se debe restringir el acceso y comunicación entre hosts de
acuerdo con los requerimientos del administrador de red.
Parte 5: Comprobación total de los dispositivos y su funcionamiento en la red.
Parte 6: Configuración final.

Ilustración 1 Modelo que se requiriere en el escenario 1



Fuente: guía de la actividad final del seminario

DESARROLLO

Como trabajo inicial se debe realizar lo siguiente.

- Realizar las rutinas de diagnóstico y dejar los equipos listos para su configuración (asignar nombres de equipos, asignar claves de seguridad, etc).

  - Configuración Router Bogotá, Medellín y Cali

Configuración Router Bogotá

```
Router(config)#hostname BOGOTA
BOGOTA(config)#no ip domain-lookup
BOGOTA(config)#enable secret class
BOGOTA(config)#line console 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)#service password-encryption
BOGOTA(config)#banner motd #....PROHIBIDO ACCESO...INGRESO SOLO
PERSONAL AUTORIZADO...#
```

Configuración Router Medellin

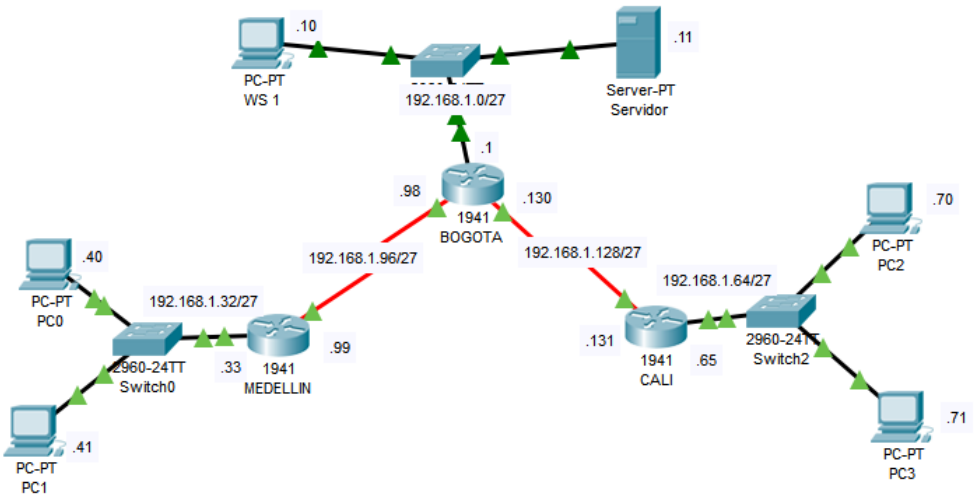
```
Router(config)#hostname MEDELLIN
MEDELLIN(config)#no ip domain-lookup
MEDELLIN(config)#enable secret class
MEDELLIN(config)#line console 0
MEDELLIN(config-line)#password cisco
MEDELLIN(config-line)#login
MEDELLIN(config-line)#line vty 0 4
MEDELLIN(config-line)#password cisco
MEDELLIN(config-line)#login
MEDELLIN(config)#service password-encryption
MEDELLIN(config)#banner motd #....PROHIBIDO ACCESO...INGRESO SOLO
PERSONAL AUTORIZADO...#
```

Configuración Router Cali

```
Router(config)#hostname CALI
CALI(config)#no ip domain-lookup
CALI(config)#enable secret class
CALI(config)#line console 0
CALI(config-line)#password cisco
CALI(config-line)#login
CALI(config-line)#line vty 0 4
CALI(config-line)#password cisco
CALI(config-line)#login
CALI(config)#service password-encryption
CALI(config)#banner motd #....PROHIBIDO ACCESO...INGRESO SOLO
PERSONAL AUTORIZADO...#
```

- Realizar la conexión física de los equipos con base en la topología de red Configurar la topología de red, de acuerdo con las siguientes especificaciones.

Ilustración 2 Grafico 1 Modelo de la red Montado en Packet Tracert



Fuente: Diseño realizado en la Herramienta Packet Tracert

Parte 1: Asignación de direcciones IP

a. Se debe dividir (subnetear) la red creando una segmentación en ocho partes, para permitir crecimiento futuro de la red corporativa.
Lar red 192.168.1.0 /24 se divide en 8 subredes así:

192.168.1.0/27
192.168.1.32/27
192.168.1.64/27
192.168.1.96/27
192.168.1.128/27
192.168.1.160/27
192.168.1.192/27
192.168.1.224/27

b. Asignar una dirección IP a la red.
Se asigna un segmento de red a las subredes como lo indica la figura anterior.

Parte 2: Configuración Básica

a. Completar la siguiente tabla con la configuración básica de los routers, teniendo en cuenta las subredes diseñadas.

	R1	R2	R3
Nombre de Host	**MEDELLIN**	**BOGOTA**	**CALI**
Dirección de Ip en interfaz Serial 0/0/0	192.168.1.99	192.168.1.98	192.168.1.131
Dirección de Ip en interfaz Serial 0/0/1	N/A	192.168.1.130	N/A
Dirección de Ip en interfaz G 0/0	192.168.1.33	192.168.1.1	192.168.1.65
Protocolo de enrutamiento	**Eigrp**	**Eigrp**	**Eigrp**
Sistema Autónomo	200	200	200
Afirmaciones de red	192.168.0.1	192.168.0.1	192.168.0.1
PC 0	192.168.1.40/27		
PC 1	192.168.1.41/27		
PC 2			192.168.1.70/27
PC 3			192.168.1.71/27
PC WS 1		192.168.1.10/27	
Servidor		192.168.1.11/27	

Configuración IP Router Bogotá

```
BOGOTA>enable
BOGOTA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA(config)#interface serial 0/0/0
BOGOTA(config-if)#ip address 192.168.1.98 255.255.255.224
BOGOTA(config-if)#no shutdown
BOGOTA(config-if)#interface serial 0/0/1
BOGOTA(config-if)#ip address 192.168.1.130 255.255.255.224
BOGOTA(config-if)#clock rate 128000
BOGOTA(config-if)#no shutdown
BOGOTA(config)#interface gigabitEthernet 0/0
BOGOTA(config-if)#ip address 192.168.1.1 255.255.255.224
BOGOTA(config-if)#no shutdown
```

Configuración IP Router Medellín

```
MEDELLIN>enable
MEDELLIN#conf t
MEDELLIN(config)#interface serial 0/0/0
MEDELLIN(config-if)#ip address 192.168.1.99 255.255.255.224
MEDELLIN(config-if)#clock rate 128000
MEDELLIN(config-if)#no shutdown
MEDELLIN(config)#interface gigabitEthernet 0/0
MEDELLIN(config-if)#ip address 192.168.1.33 255.255.255.224
MEDELLIN(config-if)#no shutdown
```

Configuración IP Router Cali

```
CALI>enable
CALI#conf t
CALI(config)#interface serial 0/0/0
CALI(config-if)#ip address 192.168.1.131 255.255.255.224
CALI(config-if)#clock rate 128000
CALI(config-if)#no shutdown
CALI(config)#interface gigabitEthernet 0/0
CALI(config-if)#192.168.1.65 255.255.255.224
CALI(config-if)#ip address 192.168.1.65 255.255.255.224
```

```
CALI(config-if)#no shutdown
```

b. Después de cargada la configuración en los dispositivos, verificar la tabla de enrutamiento en cada uno de los routers para comprobar las redes y sus rutas.

```
BOGOTA#show ip route
```

```
BOGOTA#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     192.168.1.0/24 is variably subnetted, 6 subnets, 2 masks
C       192.168.1.0/27 is directly connected, GigabitEthernet0/0
L       192.168.1.1/32 is directly connected, GigabitEthernet0/0
C       192.168.1.96/27 is directly connected, Serial0/0/0
L       192.168.1.98/32 is directly connected, Serial0/0/0
C       192.168.1.128/27 is directly connected, Serial0/0/1
L       192.168.1.130/32 is directly connected, Serial0/0/1
```

```
MEDELLIN#show ip route
```

```
MEDELLIN#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     192.168.1.0/24 is variably subnetted, 4 subnets, 2 masks
C       192.168.1.32/27 is directly connected, GigabitEthernet0/0
L       192.168.1.33/32 is directly connected, GigabitEthernet0/0
C       192.168.1.96/27 is directly connected, Serial0/0/0
L       192.168.1.99/32 is directly connected, Serial0/0/0
```

```
CALI#show ip route
```

```
CALI#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     192.168.1.0/24 is variably subnetted, 4 subnets, 2 masks
C       192.168.1.64/27 is directly connected, GigabitEthernet0/0
L       192.168.1.65/32 is directly connected, GigabitEthernet0/0
C       192.168.1.128/27 is directly connected, Serial0/0/0
L       192.168.1.131/32 is directly connected, Serial0/0/0
```

c. Verificar el balanceo de carga que presentan los routers.

Se verifica el balanceo de cargas en cada uno de los routers y hasta el momento no hay vias configuradas por donde pasa el tráfico, ya que los router aún no tienen comunicación entre sí.

d. Realizar un diagnóstico de vecinos usando el comando cdp.

Router Bogotá

BOGOTA>**show cdp neighbors detail**

```
BOGOTA>show cdp neighbors detail

Device ID: Switch
Entry address(es):
Platform: cisco 2960, Capabilities: Switch
Interface: GigabitEthernet0/0, Port ID (outgoing port): FastEthernet0/3
Holdtime: 120

Version :
Cisco IOS Software, C2960 Software (C2960-LANBASE-M), Version 12.2(25)FX, RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Wed 12-Oct-05 22:05 by pt_team

advertisement version: 2
Duplex: full
---------------------------

Device ID: CALI
Entry address(es):
  IP address : 192.168.1.131
Platform: cisco C1900, Capabilities: Router
Interface: Serial0/0/1, Port ID (outgoing port): Serial0/0/0
Holdtime: 176

Version :
Cisco IOS Software, C1900 Software (C1900-UNIVERSALK9-M), Version 15.1(4)M4, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Thurs 5-Jan-12 15:41 by pt_team

advertisement version: 2
Duplex: full
---------------------------

Device ID: MEDELLIN
Entry address(es):
  IP address : 192.168.1.99
Platform: cisco C1900, Capabilities: Router
Interface: Serial0/0/0, Port ID (outgoing port): Serial0/0/0
Holdtime: 125

Version :
Cisco IOS Software, C1900 Software (C1900-UNIVERSALK9-M), Version 15.1(4)M4, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Thurs 5-Jan-12 15:41 by pt_team

advertisement version: 2
Duplex: full
```

Router Medellín

MEDELLIN>**show cdp neighbors detail**

```
MEDELLIN>show cdp neighbors detail

Device ID: Switch
Entry address(es):
Platform: cisco 2960, Capabilities: Switch
Interface: GigabitEthernet0/0, Port ID (outgoing port): GigabitEthernet0/1
Holdtime: 177

Version :
Cisco IOS Software, C2960 Software (C2960-LANBASE-M), Version 12.2(25)FX, RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Wed 12-Oct-05 22:05 by pt_team

advertisement version: 2
Duplex: full
---------------------------

Device ID: BOGOTA
Entry address(es):
  IP address : 192.168.1.98
Platform: cisco C1900, Capabilities: Router
Interface: Serial0/0/0, Port ID (outgoing port): Serial0/0/0
Holdtime: 168

Version :
Cisco IOS Software, C1900 Software (C1900-UNIVERSALK9-M), Version 15.1(4)M4, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Thurs 5-Jan-12 15:41 by pt_team

advertisement version: 2
Duplex: full
```

Router Cali

CALI>**show cdp neighbors detail**

```
CALI>show cdp neighbors detail

Device ID: Switch
Entry address(es):
Platform: cisco 2960, Capabilities: Switch
Interface: GigabitEthernet0/0, Port ID (outgoing port): GigabitEthernet0/1
Holdtime: 123

Version :
Cisco IOS Software, C2960 Software (C2960-LANBASE-M), Version 12.2(25)FX, RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Wed 12-Oct-05 22:05 by pt_team

advertisement version: 2
Duplex: full
---------------------------

Device ID: BOGOTA
Entry address(es):
  IP address : 192.168.1.130
Platform: cisco C1900, Capabilities: Router
Interface: Serial0/0/0, Port ID (outgoing port): Serial0/0/1
Holdtime: 179

Version :
Cisco IOS Software, C1900 Software (C1900-UNIVERSALK9-M), Version 15.1(4)M4, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Thurs 5-Jan-12 15:41 by pt_team

advertisement version: 2
Duplex: full
```

e. Realizar una prueba de conectividad en cada tramo de la ruta usando Ping.

Ping desde el Router Bogotá a Medellín

```
BOGOTA>ping 192.168.1.99

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.99, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/7 ms
```

Ping desde el Router Bogotá a Cali

```
BOGOTA>ping 192.168.1.131

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.131, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/7 ms
```

Ping desde el PC0 al Router Medellín

```
C:\>ping 192.168.1.33

Pinging 192.168.1.33 with 32 bytes of data:

Reply from 192.168.1.33: bytes=32 time=1ms TTL=255
Reply from 192.168.1.33: bytes=32 time<1ms TTL=255
Reply from 192.168.1.33: bytes=32 time<1ms TTL=255
Reply from 192.168.1.33: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.33:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Ping desde el WS 1 al Router Bogotá

```
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time=3ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 3ms, Average = 0ms
```

Ping desde el PC2 al Router Cali

```
C:\>ping 192.168.1.65

Pinging 192.168.1.65 with 32 bytes of data:

Reply from 192.168.1.65: bytes=32 time=1ms TTL=255
Reply from 192.168.1.65: bytes=32 time<1ms TTL=255
Reply from 192.168.1.65: bytes=32 time<1ms TTL=255
Reply from 192.168.1.65: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.65:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Se hacen todos los pings necesarios para verificar la conectividad entre los routers y las LAN internas de cada Ciudad, cabe aclarar que solo hay comunicación en cada ciudad.

PARTE 3: CONFIGURACIÓN DE ENRUTAMIENTO

a. Asignar el protocolo de enrutamiento EIGRP a los routers considerando el direccionamiento diseñado.

Protocolo de enrutamiento EIGRP para el router Bogotá

```
BOGOTA(config)#router eigrp 1
BOGOTA(config-router)#no auto-summary
BOGOTA(config-router)#network 192.168.1.96 0.0.0.31
BOGOTA(config-router)#network 192.168.1.0 0.0.0.31
BOGOTA(config-router)#network 192.168.1.128 0.0.0.31
```

Protocolo de enrutamiento EIGRP para el router Medellín

```
MEDELLIN(config)#router eigrp 1
MEDELLIN(config-router)#no auto-summary
MEDELLIN(config-router)#network 192.168.1.32 0.0.0.31
MEDELLIN(config-router)#network 192.168.1.96 0.0.0.31
```

Protocolo de enrutamiento EIGRP para el router Cali

```
CALI(config)#router eigrp 1
CALI(config-router)#no auto-summary
```

```
CALI(config-router)#network 192.168.1.128 0.0.0.31
CALI(config-router)#network 192.168.1.64 0.0.0.31
```

b. Verificar si existe vecindad con los routers configurados con EIGRP.

Vecinos Router Medellín: se muestra la conexión con su vecino Router Bogotá

```
MEDELLIN#show ip eigrp neighbors
MEDELLIN#show ip eigrp neighbors
IP-EIGRP neighbors for process 1
H   Address         Interface       Hold Uptime    SRTT   RTO   Q   Seq
                                    (sec)          (ms)       Cnt Num
0   192.168.1.98    Se0/0/0         14   00:01:23  40     1000  0   5
```

Vecinos Router Bogotá: se muestra la conexión con sus vecinos Router Medellín y Cali

```
BOGOTA#show ip eigrp neighbors
BOGOTA#show ip eigrp neighbors
IP-EIGRP neighbors for process 1
H   Address         Interface       Hold Uptime    SRTT   RTO   Q   Seq
                                    (sec)          (ms)       Cnt Num
0   192.168.1.99    Se0/0/0         11   00:06:26  40     1000  0   7
1   192.168.1.131   Se0/0/1         10   00:06:21  40     1000  0   7
```

Vecinos Router Cali: se muestra la conexión con su vecino Router Bogotá

```
CALI#show ip eigrp neighbors
CALI#show ip eigrp neighbors
IP-EIGRP neighbors for process 1
H   Address         Interface       Hold Uptime    SRTT   RTO   Q   Seq
                                    (sec)          (ms)       Cnt Num
0   192.168.1.130   Se0/0/0         10   00:12:10  40     1000  0   6
```

c. Realizar la comprobación de las tablas de enrutamiento en cada uno de los routers para verificar cada una de las rutas establecidas.

```
BOGOTA#show ip route
BOGOTA>show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     192.168.1.0/24 is variably subnetted, 8 subnets, 2 masks
C       192.168.1.0/27 is directly connected, GigabitEthernet0/0
L       192.168.1.1/32 is directly connected, GigabitEthernet0/0
D       192.168.1.32/27 [90/2170112] via 192.168.1.99, 00:26:36, Serial0/0/0
D       192.168.1.64/27 [90/2170112] via 192.168.1.131, 00:24:17, Serial0/0/1
C       192.168.1.96/27 is directly connected, Serial0/0/0
L       192.168.1.98/32 is directly connected, Serial0/0/0
C       192.168.1.128/27 is directly connected, Serial0/0/1
L       192.168.1.130/32 is directly connected, Serial0/0/1
```

```
MEDELLIN#show ip route
MEDELLIN>show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     192.168.1.0/24 is variably subnetted, 7 subnets, 2 masks
D       192.168.1.0/27 [90/2172416] via 192.168.1.98, 00:27:52, Serial0/0/0
C       192.168.1.32/27 is directly connected, GigabitEthernet0/0
L       192.168.1.33/32 is directly connected, GigabitEthernet0/0
D       192.168.1.64/27 [90/2682112] via 192.168.1.98, 00:25:53, Serial0/0/0
C       192.168.1.96/27 is directly connected, Serial0/0/0
L       192.168.1.99/32 is directly connected, Serial0/0/0
D       192.168.1.128/27 [90/2681856] via 192.168.1.98, 00:27:36, Serial0/0/0
```

```
CALI#show ip route
CALI>show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     192.168.1.0/24 is variably subnetted, 7 subnets, 2 masks
D       192.168.1.0/27 [90/2172416] via 192.168.1.130, 00:28:19, Serial0/0/0
D       192.168.1.32/27 [90/2682112] via 192.168.1.130, 00:28:19, Serial0/0/0
C       192.168.1.64/27 is directly connected, GigabitEthernet0/0
L       192.168.1.65/32 is directly connected, GigabitEthernet0/0
D       192.168.1.96/27 [90/2681856] via 192.168.1.130, 00:28:19, Serial0/0/0
C       192.168.1.128/27 is directly connected, Serial0/0/0
L       192.168.1.131/32 is directly connected, Serial0/0/0
```

d. Realizar un diagnóstico para comprobar que cada uno de los puntos de la red se puedan ver y tengan
conectividad entre sí. Realizar esta prueba desde un host de la red LAN del router CALI, primero a la red de MEDELLIN y luego al servidor.

Ping PC2 LAN Cali a PC0 LAN Medellín

```
C:\>ping 192.168.1.40

Pinging 192.168.1.40 with 32 bytes of data:

Reply from 192.168.1.40: bytes=32 time=2ms TTL=125
Reply from 192.168.1.40: bytes=32 time=5ms TTL=125
Reply from 192.168.1.40: bytes=32 time=5ms TTL=125
Reply from 192.168.1.40: bytes=32 time=2ms TTL=125

Ping statistics for 192.168.1.40:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 5ms, Average = 3ms
```

Ping PC3 LAN Cali al Servidor LAN Bogotá

```
C:\>ping 192.168.1.11

Pinging 192.168.1.11 with 32 bytes of data:

Reply from 192.168.1.11: bytes=32 time=4ms TTL=126
Reply from 192.168.1.11: bytes=32 time=1ms TTL=126
Reply from 192.168.1.11: bytes=32 time=1ms TTL=126
Reply from 192.168.1.11: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.1.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 4ms, Average = 1ms
```

Parte 4: Configuración de las listas de Control de Acceso

En este momento cualquier usuario de la red tiene acceso a todos sus dispositivos y estaciones de trabajo. El jefe de redes le solicita implementar seguridad en la red. Para esta labor se decide configurar listas de control de acceso (ACL) a los routers. Las condiciones para crear las ACL son las siguientes:

a. Cada router debe estar habilitado para establecer conexiones Telnet con los demás routers y tener
acceso a cualquier dispositivo en la red.

Habilitar conexiones telnet al Router Bogotá

```
BOGOTA(config)#access-list 101 permit tcp any 192.168.1.128 0.0.0.31 eq telnet
BOGOTA(config)#access-list 101 permit tcp any 192.168.1.96 0.0.0.31 eq telnet
```

Habilitar conexiones telnet al Router Medellin

```
MEDELLIN(config)#access-list 101 permit tcp any 192.168.1.128 0.0.0.31 eq telnet
MEDELLIN(config)#access-list 101 permit tcp any 192.168.1.96 0.0.0.31 eq telnet
```

Acceso a la LAN de Medellín desde el router de Medellin, Bogotá y Cali

```
MEDELLIN(config)#access-list 101 permit ip 192.168.1.32 0.0.0.31 192.168.1.131 0.0.0.31
MEDELLIN(config)#access-list 101 permit ip 192.168.1.32 0.0.0.31 192.168.1.98 0.0.0.31
MEDELLIN(config)#access-list 101 permit ip 192.168.1.32 0.0.0.31 192.168.1.131 0.0.0.31
```

Habilitar conexiones telnet al Router Cali

```
CALI(config)#access-list 101 permit tcp any 192.168.1.128 0.0.0.31 eq telnet
```

```
CALI(config)#access-list 101 permit tcp any 192.168.1.96 0.0.0.31 eq
telnet
```

Acceso a la LAN de Cali desde el router de Medellin, Bogotá y Cali

```
CALI(config)#access-list 101 permit ip 192.168.1.64 0.0.0.31
192.168.1.99 0.0.0.31
CALI(config)#access-list 101 permit ip 192.168.1.64 0.0.0.31
192.168.1.130 0.0.0.31
CALI(config)#access-list 101 permit ip 192.168.1.64 0.0.0.31
192.168.1.64 0.0.0.31
```

b. El equipo WS1 y el servidor se encuentran en la subred de administración. Solo el servidor de la subred de administración debe tener acceso a cualquier otro dispositivo en cualquier parte de la red.

Solo permite el acceso al servidor desde la LAN de Medellín

```
MEDELLIN(config)#access-list 101 permit ip 192.168.1.32 0.0.0.31 host
192.168.1.11
```

Solo permite el acceso al servidor desde la LAN de Cali

```
CALI(config)#access-list 101 permit ip 192.168.1.64 0.0.0.31 host
192.168.1.11
```

Se puede evidenciar que con esta configuración el servidor puede ingresar a todas las redes.

c. Las estaciones de trabajo en las LAN de MEDELLIN y CALI no deben tener acceso a ningún dispositivo fuera de su subred, excepto para interconectar con el servidor.

LAN de Medellin no tiene acceso a ninguna otra red excepto el servidor

```
MEDELLIN(config)#interface gigabitEthernet 0/0
MEDELLIN(config-if)#ip access-group 101 in
```

Se da acceso a las redes que se necesita en la lista de acceso, las otras por defecto el ACL las deshabilita y no deja ingresar a las redes como se solicitan en este punto. En el cuadro final de comprobación de los pings, se agrega los pantallazos de las pruebas.

LAN de Cali no tiene acceso a ninguna otra red excepto el servidor

```
CALI(config)#interface gigabitEthernet 0/0
CALI(config-if)#ip access-group 101 in
```

Se da acceso a las redes que se necesita en la lista de acceso, las otras por defecto el ACL las deshabilita y no deja ingresar a las redes como se solicitan en este punto. En el cuadro final de comprobación de los pings, se agrega los pantallazos de las pruebas.

Parte 5: Comprobación de la red instalada

a. Se debe probar que la configuración de las listas de acceso fue exitosa.

Lista de Acceso ACL en el router de Medellin

```
MEDELLIN#show access-lists
Extended IP access list 101
    10 permit ip 192.168.1.32 0.0.0.31 host 192.168.1.11 (12 match(es))
    20 permit ip 192.168.1.32 0.0.0.31 192.168.1.32 0.0.0.31 (4 match(es))
    30 permit ip 192.168.1.32 0.0.0.31 192.168.1.128 0.0.0.31 (8 match(es))
    40 permit tcp any 192.168.1.96 0.0.0.31 eq telnet
    50 permit ip 192.168.1.32 0.0.0.31 192.168.1.96 0.0.0.31 (5 match(es))
    60 permit tcp any 192.168.1.128 0.0.0.31 eq telnet
```

Lista de Acceso ACL en el router de Cali

```
CALI#show access-lists
Extended IP access list 101
    10 permit ip 192.168.1.64 0.0.0.31 host 192.168.1.11 (11 match(es))
    20 permit ip 192.168.1.64 0.0.0.31 192.168.1.96 0.0.0.31 (8 match(es))
    30 permit ip 192.168.1.64 0.0.0.31 192.168.1.128 0.0.0.31 (8 match(es))
    40 permit ip 192.168.1.64 0.0.0.31 192.168.1.64 0.0.0.31
    50 permit tcp any 192.168.1.128 0.0.0.31 eq telnet
    60 permit tcp any 192.168.1.96 0.0.0.31 eq telnet
```

b. Comprobar y Completar la siguiente tabla de condiciones de prueba para confirmar el óptimo funcionamiento de la red e.

	ORIGEN	DESTINO	RESULTADO
TELNET	Router MEDELLIN	Router CALI	exitoso
	WS_1	Router BOGOTA	exitoso
	Servidor	Router CALI	exitoso
	Servidor	Router MEDELLIN	exitoso
TELNET	LAN del Router MEDELLIN	Router CALI	exitoso
	LAN del Router CALI	Router CALI	exitoso
	LAN del Router MEDELLIN	Router MEDELLIN	exitoso
	LAN del Router CALI	Router MEDELLIN	exitoso
PING	LAN del Router CALI	WS_1	falló
	LAN del Router MEDELLIN	WS_1	falló
	LAN del Router MEDELLIN	LAN del Router CALI	falló
PING	LAN del Router CALI	Servidor	exitoso
	LAN del Router MEDELLIN	Servidor	exitoso
	Servidor	LAN del Router MEDELLIN	exitoso
	Servidor	LAN del Router CALI	exitoso
	Router CALI	LAN del Router MEDELLIN	exitoso
	Router MEDELLIN	LAN del Router CALI	exitoso

Telnet Router Medellin a Router Cali

```
MEDELLIN>telnet 192.168.1.131
Trying 192.168.1.131 ...Open....PROHIBIDO ACCESO...INGRESO SOLO PERSONAL AUTORIZADO...


User Access Verification

Password:
CALI>
```

Telnet WS_1 a Router Bogotá

```
C:\>telnet 192.168.1.1
Trying 192.168.1.1 ...Open....PROHIBIDO ACCESO...INGRESO SOLO PERSONAL AUTORIZADO...


User Access Verification

Password:
BOGOTA>
```

Telnet Servidor al Router Cali

```
C:\>telnet 192.168.1.131
Trying 192.168.1.131 ...Open....PROHIBIDO ACCESO...INGRESO SOLO PERSONAL AUTORIZADO...


User Access Verification

Password:
CALI>
```

Telnet Servidor al Router Medellin

```
C:\>telnet 192.168.1.99
Trying 192.168.1.99 ...Open....PROHIBIDO ACCESO...INGRESO SOLO PERSONAL AUTORIZADO...


User Access Verification

Password:
MEDELLIN>
```

LAN Router Medellín al Router de Cali

```
C:\>telnet 192.168.1.131
Trying 192.168.1.131 ...Open....PROHIBIDO ACCESO...INGRESO SOLO PERSONAL AUTORIZADO...


User Access Verification

Password:
CALI>
```

LAN Router Cali al Router de Cali

```
C:\>telnet 192.168.1.131
Trying 192.168.1.131 ...Open....PROHIBIDO ACCESO...INGRESO SOLO PERSONAL AUTORIZADO...


User Access Verification

Password:
CALI>
```

LAN Router Medellín al Router de Medellín

```
C:\>telnet 192.168.1.99
Trying 192.168.1.99 ...Open....PROHIBIDO ACCESO...INGRESO SOLO PERSONAL AUTORIZADO...


User Access Verification

Password:
MEDELLIN>
```

LAN Router Cali al Router de Medellin

```
C:\>telnet 192.168.1.99
Trying 192.168.1.99 ...Open....PROHIBIDO ACCESO...INGRESO SOLO PERSONAL AUTORIZADO...

User Access Verification

Password:
MEDELLIN>
```

LAN Router Cali al WS_1

```
C:\>ping 192.168.1.10

Pinging 192.168.1.10 with 32 bytes of data:

Reply from 192.168.1.65: Destination host unreachable.
Reply from 192.168.1.65: Destination host unreachable.
Reply from 192.168.1.65: Destination host unreachable.
Reply from 192.168.1.65: Destination host unreachable.

Ping statistics for 192.168.1.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

LAN Router Medellín al WS_1

```
C:\>ping 192.168.1.10

Pinging 192.168.1.10 with 32 bytes of data:

Reply from 192.168.1.33: Destination host unreachable.
Reply from 192.168.1.33: Destination host unreachable.
Reply from 192.168.1.33: Destination host unreachable.
Reply from 192.168.1.33: Destination host unreachable.

Ping statistics for 192.168.1.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

LAN Router Medellín a LAN Router Cali

```
C:\>ping 192.168.1.70

Pinging 192.168.1.70 with 32 bytes of data:

Reply from 192.168.1.33: Destination host unreachable.
Reply from 192.168.1.33: Destination host unreachable.
Reply from 192.168.1.33: Destination host unreachable.
Reply from 192.168.1.33: Destination host unreachable.

Ping statistics for 192.168.1.70:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

LAN Router Cali al Servidor

```
Pinging 192.168.1.11 with 32 bytes of data:

Reply from 192.168.1.11: bytes=32 time=3ms TTL=126
Reply from 192.168.1.11: bytes=32 time=1ms TTL=126
Reply from 192.168.1.11: bytes=32 time=2ms TTL=126
Reply from 192.168.1.11: bytes=32 time=2ms TTL=126

Ping statistics for 192.168.1.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 3ms, Average = 2ms
```

LAN Router Medellín al Servidor

```
C:\>ping 192.168.1.11

Pinging 192.168.1.11 with 32 bytes of data:

Reply from 192.168.1.11: bytes=32 time=1ms TTL=126
Reply from 192.168.1.11: bytes=32 time=1ms TTL=126
Reply from 192.168.1.11: bytes=32 time=1ms TTL=126
Reply from 192.168.1.11: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.1.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

Servidor a LAN Router Medellín

```
C:\>ping 192.168.1.41

Pinging 192.168.1.41 with 32 bytes of data:

Reply from 192.168.1.41: bytes=32 time=1ms TTL=126
Reply from 192.168.1.41: bytes=32 time=1ms TTL=126
Reply from 192.168.1.41: bytes=32 time=1ms TTL=126
Reply from 192.168.1.41: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.1.41:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

Servidor a LAN Router Cali

```
C:\>ping 192.168.1.71

Pinging 192.168.1.71 with 32 bytes of data:

Reply from 192.168.1.71: bytes=32 time=1ms TTL=126
Reply from 192.168.1.71: bytes=32 time=1ms TTL=126
Reply from 192.168.1.71: bytes=32 time=4ms TTL=126
Reply from 192.168.1.71: bytes=32 time=3ms TTL=126

Ping statistics for 192.168.1.71:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 4ms, Average = 2ms
```

Router Cali a LAN Router Medellín

```
CALI>ping 192.168.1.40

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.40, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/4/9 ms
```

Router Medellín a LAN Router Cali

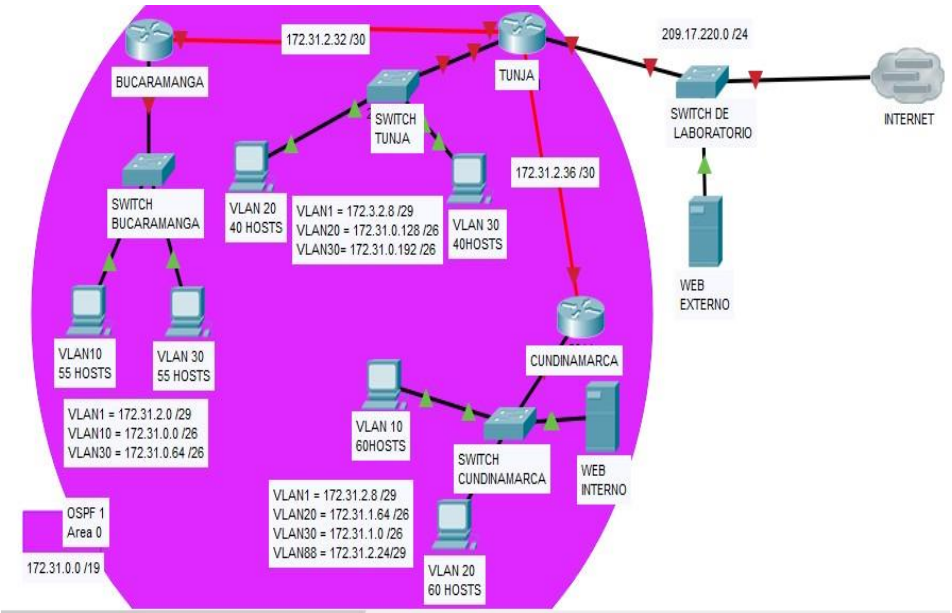
```
MEDELLIN>ping 192.168.1.71

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.71, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/3/6 ms
```

ESCENARIO 2

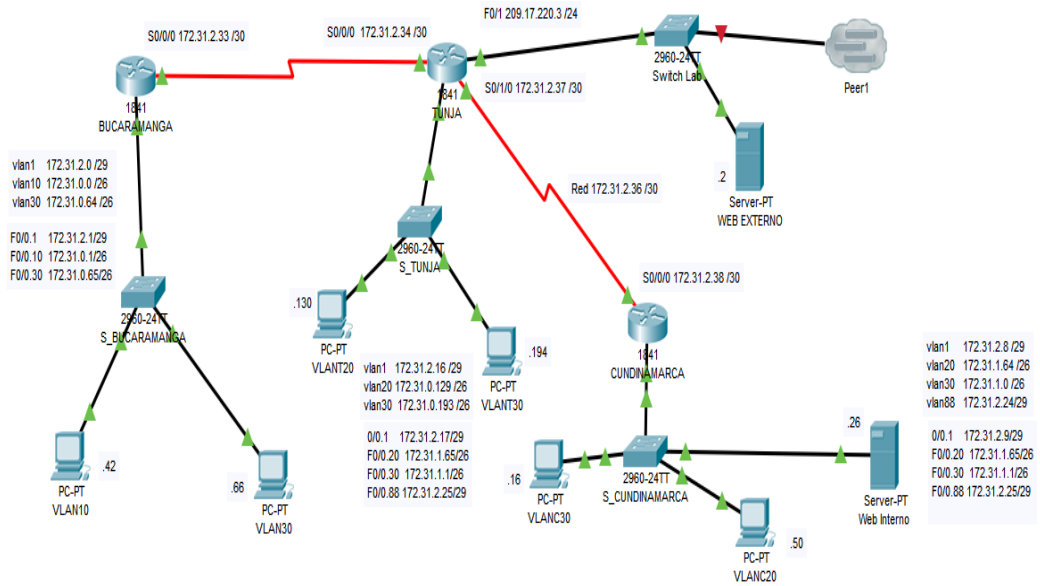
Una empresa tiene la conexión a internet en una red Ethernet, lo cual deben adaptarlo para facilitar que sus routers y las redes que incluyen puedan, por esa vía, conectarse a internet, pero empleando las direcciones de la red LAN original.

Ilustración 3. Diseño escenario 2 Guía de Actividades



Fuente: Guía de Actividades UNAD Trabajo final Seminario Cisco

Ilustración 4. Diseño Realizado para Ejercicio del Escenario 2



Fuente: Ejercicio Realizado en la Herramienta Packet Tracert de Cisco

DESARROLLO

Los siguientes son los requerimientos necesarios:

1. Todos los routers deberán tener los siguiente:

Configuración Básica de los Routers.

Configuración Router Bucaramanga

```
Router(config)#hostname R_BUCARAMANGA
R_BUCARAMANGA(config)#no ip domain-lookup
R_BUCARAMANGA(config)#enable secret class
R_BUCARAMANGA(config)#line console 0
R_BUCARAMANGA(config-line)#password cisco
R_BUCARAMANGA(config-line)#login
R_BUCARAMANGA(config-line)#line vty 0 4
R_BUCARAMANGA(config-line)#password cisco
R_BUCARAMANGA(config-line)#login
R_BUCARAMANGA(config-line)#service password-encryption
R_BUCARAMANGA(config)#banner motd #....PROHIBIDO ACCESO...INGRESO SOLO
PERSONAL AUTORIZADO...#
R_BUCARAMANGA(config)#int s0/0/0
R_BUCARAMANGA(config-if)#ip address 172.31.2.33 255.255.255.252
R_BUCARAMANGA(config-if)#clock rate 128000
R_BUCARAMANGA(config)#interface f0/0
R_BUCARAMANGA(config-if)#ip address 172.31.2.1 255.255.255.248
R_BUCARAMANGA(config-if)#no sh
```

Configuración básica Switch Bucaramanga

```
Switch(config)#no ip domain-lookup
Switch(config)#hostname S-BUCARAMAGA
S-BUCARAMAGA(config)#enable password class
S-BUCARAMAGA(config)#line con 0
S-BUCARAMAGA(config-line)#password cisco
S-BUCARAMAGA(config-line)#login
S-BUCARAMAGA(config-line)#line vty 0 15
S-BUCARAMAGA(config-line)#password cisco
S-BUCARAMAGA(config-line)#login
S-BUCARAMAGA(config-line)#line con 0
S-BUCARAMAGA(config-line)#logging synchronous
S-BUCARAMAGA(config-line)#exit
```

Configuración Vlan 1

```
S-BUCARAMAGA(config)#interface vlan 1
S-BUCARAMAGA(config-if)#ip add 172.31.2.2 255.255.255.248
S-BUCARAMAGA(config-if)#ip default-gateway 172.31.2.1
```

Configuración Vlan 10

```
Switch(config)#vlan 10
Switch(config-vlan)#name VLAN10
```

```
Switch(config-vlan)#exit
Switch(config)#interface range f0/1-10
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 10
```

Configuración Vlan 30

```
Switch(config-vlan)#Vlan 30
Switch(config-vlan)#name VLAN30
Switch(config-vlan)#exit
Switch(config)#interface range f0/11-20
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 30
Switch(config-if-range)#exit
```

Configuración Enlace Troncal

```
Switch(config)#interface f0/23
Switch(config-if)#switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan 10,20
```

Configuración Router Bucaramanga entre Vlans basado en enlaces troncales

Valn 1

```
R_BUCARAMANGA(config)#interface f0/0.1
R_BUCARAMANGA(config-subif)#encapsulation dot1q 1 native
R_BUCARAMANGA(config-subif)#ip add 172.31.2.1 255.255.255.248
```

Vlan 10

```
R_BUCARAMANGA(config)#interface f0/0.10
R_BUCARAMANGA(config-subif)#encapsulation dot1q 10
R_BUCARAMANGA(config-subif)#ip address 172.31.0.1 255.255.255.192
```

Vlan 30

```
R_BUCARAMANGA(config)#interface f0/0.30
R_BUCARAMANGA(config-subif)#encapsulation dot1q 30
R_BUCARAMANGA(config-subif)#ip address 172.31.0.65 255.255.255.192
```

Configuración Router Tunja

```
Router(config)#hostname R_TUNJA
R_TUNJA(config)#no ip domain-lookup
R_TUNJA(config)#enable secret class
R_TUNJA(config)#line console 0
R_TUNJA(config-line)#password cisco
R_TUNJA(config-line)#login
R_TUNJA(config-line)#line vty 0 4
R_TUNJA(config-line)#password cisco
R_TUNJA(config-line)#login
R_TUNJA(config-line)#service password-encryption
R_TUNJA(config)#banner motd #....PROHIBIDO ACCESO...INGRESO SOLO PERSONAL
AUTORIZADO...#
R_TUNJA(config)#int s0/0/0
```

```
R_TUNJA(config-if)#ip address 172.31.2.34 255.255.255.252
R_TUNJA(config-if)#exit
R_TUNJA(config)#int s0/1/0
R_TUNJA(config-if)#ip address 172.31.2.37 255.255.255.252
R_TUNJA(config-if)#no sh
R_TUNJA(config)#interface FastEthernet0/0
R_TUNJA(config-if)#ip address 172.31.2.18 255.255.255.248
```

Nota: se configura red fast ethernet 0/0 con ip 172.31.2.18 para poder realizar el ejercicio ya que la que trae el ejercicio es la 172.3.2.8

Configuración Switch Tunja

```
Switch(config)#no ip domain-lookup
Switch(config)#hostname S_TUNJA
S_TUNJA(config)#enable password class
S_TUNJA(config)#Line console 0
S_TUNJA(config-line)#Password cisco
S_TUNJA(config-line)#login
S_TUNJA(config-line)#line vty 0 15
S_TUNJA(config-line)#Password cisco
S_TUNJA(config-line)#login
S_TUNJA(config)#line console 0
S_TUNJA(config-line)#logging synchronous
```

Configuración Vlan 1

```
S_TUNJA(config-line)#interface vlan 1
S_TUNJA(config-if)#ip add 172.31.2.18 255.255.255.248
S_TUNJA(config-if)#ip default-gateway 172.31.2.1
```

Configuración Vlan 20

```
S_TUNJA(config)#vlan 20
S_TUNJA(config-vlan)#name VLAN20
S_TUNJA(config-vlan)#exit
S_TUNJA(config)#int range f0/1-10
S_TUNJA(config-if-range)#switchport mode access
S_TUNJA(config-if-range)#switchport access vlan 20
```

Configuración Vlan 30

```
S_TUNJA(config)#vlan 30
S_TUNJA(config-vlan)#name VLAN30
S_TUNJA(config-vlan)#exit
S_TUNJA(config)#int range f0/11-20
S_TUNJA(config-if-range)#switchport mode access
S_TUNJA(config-if-range)#switchport access vlan 30
```

Configuración Enlace Troncal

```
S_TUNJA(config)#interface f0/23
S_TUNJA(config-if)#switchport mode trunk
```

```
Switch(config-if)#switchport trunk allowed vlan 20,30
```

Configuración Router TUNJA entre Vlans basado en enlaces troncales

Valn 1

```
R_TUNJA(config)#interface f0/0.1
R_TUNJA(config-subif)#encapsulation dot1q 1 native
R_TUNJA(config-subif)#ip add 172.31.2.17 255.255.255.248
```

Vlan 20

```
R_TUNJA(config)#int f0/0.20
R_TUNJA(config-subif)#encapsulation dot1Q 20
R_TUNJA(config-subif)#ip add 172.31.0.129 255.255.255.192
```

Vlan 30

```
R_TUNJA(config)#int f0/0.30
R_TUNJA(config-subif)#encapsulation dot1Q 30
R_TUNJA(config-subif)#ip add 172.31.0.193 255.255.255.192
```

Configuración router Cundinamarca

```
Router(config)#hostname R_CUNDINAMARCA
R_CUNDINAMARCA(config)#no ip domain-lookup
R_CUNDINAMARCA(config)#enable secret class
R_CUNDINAMARCA(config)#line console 0
R_CUNDINAMARCA(config-line)#password cisco
R_CUNDINAMARCA(config-line)#login
R_CUNDINAMARCA(config-line)#line vty 0 4
R_CUNDINAMARCA(config-line)#password cisco
R_CUNDINAMARCA(config-line)#login
R_CUNDINAMARCA(config-line)#service password-encryption
R_CUNDINAMARCA(config)#banner motd #....PROHIBIDO ACCESO...INGRESO SOLO
PERSONAL AUTORIZADO...#
R_CUNDINAMARCA(config)#int s0/0/0
R_CUNDINAMARCA(config-if)#ip address 172.31.2.38 255.255.255.252
R_CUNDINAMARCA(config-if)#clock rate 128000
```

Cofiguracion Switch Cundinamarca

```
Switch(config)#no ip domain-lookup
Switch(config)#hostname S_CUNDINAMARCA
S_CUNDINAMARCA(config)#enable password class
S_CUNDINAMARCA(config)#Line console 0
S_CUNDINAMARCA(config-line)#Password cisco
S_CUNDINAMARCA(config-line)#login
S_CUNDINAMARCA(config-line)#line vty 0 15
S_CUNDINAMARCA(config-line)#Password cisco
S_CUNDINAMARCA(config-line)#login
S_TUNJA(config)#line console 0
S_TUNJA(config-line)#logging synchronous
```

Configuración Vlan 1

```
S-CUNDINAMARCA(config)#int vlan 1
S-CUNDINAMARCA(config-if)#ip add 172.31.2.10 255.255.255.248
S-CUNDINAMARCA(config-if)#ip default-gateway 172.31.2.9
```

Configuración Vlan 20

```
S-CUNDINAMARCA(config)#vlan 20
S-CUNDINAMARCA(config-vlan)#name VLAN20
S-CUNDINAMARCA(config-vlan)#exit
S-CUNDINAMARCA(config)#int range f0/1-10
S-CUNDINAMARCA(config-if-range)#switchport mode access
S-CUNDINAMARCA(config-if-range)#switchport access vlan 20
```

Configuración Vlan 30

```
S-CUNDINAMARCA(config)#vlan 30
S-CUNDINAMARCA(config-vlan)#name VLAN30
S-CUNDINAMARCA(config-vlan)#exit
S-CUNDINAMARCA(config)#int range f0/11-20
S-CUNDINAMARCA(config-if-range)#switchport mode access
S-CUNDINAMARCA(config-if-range)#switchport access vlan 30
```

Configuración Vlan 88

```
S-CUNDINAMARCA(config)#vlan 88
S-CUNDINAMARCA(config-vlan)#name VLAN88
S-CUNDINAMARCA(config-vlan)#exit
S-CUNDINAMARCA(config)#int f0/21
S-CUNDINAMARCA(config-if)#switchport mode access
S-CUNDINAMARCA(config-if)#switchport access vlan 88
```

Configuración Enlace Troncal

```
S_TUNJA(config)#interface f0/23
S_TUNJA(config-if)#switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan 20,30,88
```

Configuración Router CUNDINAMARCA entre Vlans basado en enlaces troncales

Valn 1

```
R_CUNDINAMARCA(config)#interface f0/0.1
R_CUNDINAMARCA(config-subif)#encapsulation dot1q 1 native
R_CUNDINAMARCA(config-subif)#ip add 172.31.2.9 255.255.255.248
```

Vlan 20

```
R_CUNDINAMARCA(config)#int f0/0.20
R_CUNDINAMARCA(config-subif)#encapsulation dot1Q 20
R_CUNDINAMARCA(config-subif)#ip add 172.31.1.65 255.255.255.192
```

Vlan 30

```
R_CUNDINAMARCA(config)#int f0/0.30
R_CUNDINAMARCA(config-subif)#encapsulation dot1Q 30
R_CUNDINAMARCA(config-subif)#ip add 172.31.1.1 255.255.255.192
```

Vlan 88

```
R_CUNDINAMARCA(config)#int f0/0.88
R_CUNDINAMARCA(config-subif)#encapsulation dot1Q 88
R_CUNDINAMARCA(config-subif)#ip add 172.31.2.25 255.255.255.248
```

Enrutamiento OSPF Bucaramanga

```
R_BUCARAMANGA(config)#router ospf 1
R_BUCARAMANGA(config-router)# network 171.31.2.0 0.0.0.7 area 0
R_BUCARAMANGA(config-router)# network 171.31.2.0 0.0.0.7 area 0
R_BUCARAMANGA(config-router)# network 172.31.2.32 0.0.0.3 area 0
R_BUCARAMANGA(config-router)# network 172.31.0.64 0.0.0.63 area 0
R_BUCARAMANGA(config-router)# network 172.31.0.0 0.0.0.63 area 0
```

Enrutamiento OSPF Tunja

```
R_TUNJA(config)#router ospf 1
R_TUNJA(config-router)#network 172.31.2.36 0.0.0.3 area 0
R_TUNJA(config-router)#network 172.31.2.36 0.0.0.3 area 0
R_TUNJA(config-router)#network 172.31.2.32 0.0.0.3 area 0
R_TUNJA(config-router)#network 209.17.220.0 0.0.0.255 area 0
R_TUNJA(config-router)#network 172.31.2.16 0.0.0.7 area 0
R_TUNJA(config-router)#network 172.31.0.128 0.0.0.63 area 0
R_TUNJA(config-router)#network 172.31.0.192 0.0.0.63 area 0
```

Enrutamiento OSPF Cundinamarca

```
R_CUNDINAMARCA(config)#router ospf 1
R_CUNDINAMARCA(config-router)#network 172.31.2.36 0.0.0.3 area 0
R_CUNDINAMARCA(config-router)#network 172.31.2.8 0.0.0.7 area 0
R_CUNDINAMARCA(config-router)#network 172.31.1.64 0.0.0.63 area 0
R_CUNDINAMARCA(config-router)#network 172.31.1.0 0.0.0.63 area 0
R_CUNDINAMARCA(config-router)#network 172.31.2.24 0.0.0.7 area 0
```

Autenticación local con AAA.

Configuración Router Bucaramanga

```
R_BUCARAMANGA(config)#aaa new-model
R_BUCARAMANGA(config)#aaa authentication login default group radius local
R_BUCARAMANGA(config)#username cisco password cisco
```

Configuración Router Tunja

```
R_TUNJA(config)#aaa new-model
R_TUNJA(config)#aaa authentication login default group radius
R_TUNJA(config)#username cisco password cisco
```

Configuración Router Cundinamarca

```
R_CUNDINAMARCA(config)#aaa new-model
R_CUNDINAMARCA(config)#aaa authentication login default group radius local
R_CUNDINAMARCA(config)#username cisco password cisco
```

Cifrado de contraseñas.

```
R_BUCARAMANGA(config-line)#service password-encryption
R_TUNJA(config-line)#service password-encryption
R_CUNDINAMARCA(config-line)#service password-encryption
```

Máximo de internos para acceder al router.

```
R_BUCARAMANGA(config)#username sysadmin
R_BUCARAMANGA(config)#username sysad privilege 15 password 0 cisco
R_BUCARAMANGA(config)#username user1 password 0 cisco
R_BUCARAMANGA(config)#aaa new-model
R_BUCARAMANGA(config)#aaa local authentication attempts max-fail 2

R_TUNJA(config)#username sysadmin
R_TUNJA(config)#username sysad privilege 15 password 0 cisco
R_TUNJA(config)#username user1 password 0 cisco
R_TUNJA(config)#aaa new-model
R_TUNJA(config)#aaa local authentication attempts max-fail 2

R_CUNDINAMARCA(config)#username sysadmin
R_CUNDINAMARCA(config)#username sysad privilege 15 password 0 cisco
R_CUNDINAMARCA(config)#username user1 password 0 cisco
R_CUNDINAMARCA(config)#aaa new-model
R_CUNDINAMARCA(config)#aaa local authentication attempts max-fail 2
```

Máximo tiempo de acceso al detectar ataques.

```
R_BUCARAMANGA(config)#login block-for 5 attempts 5 within 5
R_BUCARAMANGA(config)#login mode-quit access-class ACL
R_BUCARAMANGA(config)#login delay segundos

R_TUNJA(config)#login block-for 5 attempts 5 within 5
R_TUNJA(config)#login mode-quit access-class ACL
R_TUNJA(config)#login delay segundos

R_CUNDINAMARCA(config)#login block-for 5 attempts 5 within 5
R_CUNDINAMARCA(config)#login mode-quit access-class ACL
R_CUNDINAMARCA(config)#login delay segundos
```

Establezca un servidor TFTP y almacene todos los archivos necesarios de los routers.

Configuración Router Bucaramanga

```
R_BUCARAMANGA#copy running-config tftp:
Address or name of remote host []? 172.31.2.26
R_BUCARAMANGA#show flash
System flash directory:
File Length Name/status
3 33591768 c1841-advipservicesk9-mz.124-15.T1.bin
2 28282 sigdef-category.xml
```

```
1 227537 sigdef-default.xml
[33847587 bytes used, 30168797 available, 64016384 total]
63488K bytes of processor board System flash (Read/Write)

R_BUCARAMANGA#copy flash tftp:
Source filename []? c1841-advipservicesk9-mz.124-15.T1.bin
Address or name of remote host []? 172.31.2.26
Destination filename [c1841-advipservicesk9-mz.124-15.T1.bin]? <cr>

Writing c1841-advipservicesk9-mz.124-
15.T1.bin...!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!
[OK - 33591768 bytes]

33591768 bytes copied in 11.275 secs (312815 bytes/sec)
R_BUCARAMANGA#
```

Configuración Router Tunja

```
R_TUNJA#copy running-config tftp:
Address or name of remote host []? 172.31.2.26
Destination filename [R_TUNJA-confg]? <cr>

Writing running-config...!!
[OK - 1692 bytes]

1692 bytes copied in 0.087 secs (19448 bytes/sec)

R_TUNJA#show flash

System flash directory:
File Length Name/status
3 33591768 c1841-advipservicesk9-mz.124-15.T1.bin
2 28282 sigdef-category.xml
1 227537 sigdef-default.xml
[33847587 bytes used, 30168797 available, 64016384 total]
63488K bytes of processor board System flash (Read/Write)

R_TUNJA#copy flash tftp:
Source filename []? c1841-advipservicesk9-mz.124-15.T1.bin
Address or name of remote host []? 172.31.2.26
Destination filename [c1841-advipservicesk9-mz.124-15.T1.bin]? <cr>

Writing c1841-advipservicesk9-mz.124-
15.T1.bin...!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!
[OK - 33591768 bytes]

33591768 bytes copied in 11.275 secs (312815 bytes/sec)
R_TUNJA#
```

Configuracion Router Cundinamarca

```
R_CUNDINAMARCA#copy running-config tftp:
Address or name of remote host []? 172.31.2.26
Destination filename [R_CUNDINAMARCA-confg]? <cr>

Writing running-config...!!
[OK - 1692 bytes]

1692 bytes copied in 0.087 secs (19448 bytes/sec)

R_CUNDINAMARCA #show flash

System flash directory:
File Length Name/status
3 33591768 c1841-advipservicesk9-mz.124-15.T1.bin
2 28282 sigdef-category.xml
1 227537 sigdef-default.xml
[33847587 bytes used, 30168797 available, 64016384 total]
63488K bytes of processor board System flash (Read/Write)

R_CUNDINAMARCA #copy flash tftp:
Source filename []? c1841-advipservicesk9-mz.124-15.T1.bin
Address or name of remote host []? 172.31.2.26
Destination filename [c1841-advipservicesk9-mz.124-15.T1.bin]? <cr>

Writing c1841-advipservicesk9-mz.124-
15.T1.bin...!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!
[OK - 33591768 bytes]

33591768 bytes copied in 11.275 secs (312815 bytes/sec)
```

El DHCP deberá proporcionar solo direcciones a los hosts de Bucaramanga y Cundinamarca

Router Tunja – vlans Bucaramanga

VLAN10

```
R_TUNJA(config)#ip dhcp pool B-V10
R_TUNJA(dhcp-config)#network 172.31.0.0 255.255.255.192
R_TUNJA(dhcp-config)#default-router 172.31.0.1
R_TUNJA(dhcp-config)#exit
R_TUNJA(config)#ip dhcp excluded-address 172.31.0.1
```

VLAN30

```
R_TUNJA(config)#ip dhcp pool B-V30
R_TUNJA(dhcp-config)#network 172.31.0.64 255.255.255.192
R_TUNJA(dhcp-config)#default-router 172.31.0.65
R_TUNJA(config)#ip dhcp excluded-address 172.31.0.65
```

DHCP router ip helper Bucarmanga

```
R_BUCARAMANGA(config)#interface f0/0.10
R_BUCARAMANGA(config-subif)#ip helper-address 172.31.2.34
R_BUCARAMANGA(config)#interface f0/0.30
R_BUCARAMANGA(config-subif)#ip helper-address 172.31.2.34
```

DHCP router ip helper Cundinamarca

```
R_CUNDINAMARCA(config)#int f0/0.20
R_CUNDINAMARCA(config-subif)#ip helper-address 172.31.2.37
R_CUNDINAMARCA(config-subif)#exit
R_CUNDINAMARCA(config)#int f0/0.30
R_CUNDINAMARCA(config-subif)#ip helper-address 172.31.2.37
R_CUNDINAMARCA(config-subif)#int f0/0.88
R_CUNDINAMARCA(config-subif)#exit
R_CUNDINAMARCA(config)#int f0/0.88
R_CUNDINAMARCA(config-subif)#ip helper-address 172.31.2.37
```

El web server deberá tener NAT estático y el resto de los equipos de la topología emplearan NAT de sobrecarga (PAT).

Configuración NAT estática del servidor Web

```
R_CUNDINAMARCA(config)#ip nat inside source static 172.31.2.13 172.31.2.10
R_CUNDINAMARCA(config)#interface fastEthernet 0/0
R_CUNDINAMARCA(config-if)#ip nat inside
R_CUNDINAMARCA(config-if)#exit
R_CUNDINAMARCA(config)#interface serial 0/0/0
R_CUNDINAMARCA(config-if)#ip nat outside
```

Configuración NAT de sobrecarga o PAT

```
R_TUNJA(config-if)#access-list 1 permit 209.17.220.3 0.0.0.255
R_TUNJA(config)#ip nat inside source list 1 interface f0/1 overload
R_TUNJA(config)#int s0/0/0
R_TUNJA(config-if)#ip nat inside
```

```
R_TUNJA(config-if)#int f0/1
R_TUNJA(config-if)#ip nat outside
R_TUNJA(config-if)#int s0/1/0
R_TUNJA(config-if)#ip nat inside
R_TUNJA(config-if)#int f0/1
R_TUNJA(config-if)#ip nat outside
```

El enrutamiento deberá tener autenticación.

Autenticación OSPF router Bucaramanga

```
R_BUCARAMANGA(config)#int s0/0/0
R_BUCARAMANGA(config-if)#ip ospf message-digest-key 1 md5 cisco
R_BUCARAMANGA(config-if)#ip ospf authentication message-digest
R_BUCARAMANGA#sh ip ospf interface s0

Serial0/0/0 is up, line protocol is up
Internet address is 172.31.2.33/30, Area 0
Process ID 1, Router ID 172.31.2.33, Network Type POINT-TO-POINT, Cost:
64
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
Suppress hello for 0 neighbor(s)
Message digest authentication enabled
Youngest key id is 1
```

Autenticación OSPF router Tunja

```
R_TUNJA(config)#int s0/0/0
R_TUNJA(config-if)#ip ospf message-digest-key 1 md5 cisco
R_TUNJA(config-if)#ip ospf authentication message-digest
R_TUNJA#sh ip ospf interface s0/0/0

Serial0/0/0 is up, line protocol is up
Internet address is 172.31.2.34/30, Area 0
Process ID 1, Router ID 209.17.220.3, Network Type POINT-TO-POINT, Cost:
64
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 00:00:09
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 1 , Adjacent neighbor count is 1
```

```
Adjacent with neighbor 172.31.2.33
Suppress hello for 0 neighbor(s)
Message digest authentication enabled
Youngest key id is 1

R_TUNJA(config)#int s0/1/0
R_TUNJA(config-if)#ip ospf message-digest-key 1 md5 cisco
R_TUNJA(config-if)#ip ospf authentication message-digest
R_TUNJA#sh ip ospf interface s0/1/0

Serial0/1/0 is up, line protocol is up
Internet address is 172.31.2.37/30, Area 0
Process ID 1, Router ID 209.17.220.3, Network Type POINT-TO-POINT, Cost:
64
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
Index 6/6, 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 172.31.2.38
Suppress hello for 0 neighbor(s)
Message digest authentication enabled
Youngest key id is 1
R_TUNJA#
```

Autenticación OSPF router Cundinamarca

```
R_CUNDINAMARCA(config)#int s0/0/0
R_CUNDINAMARCA(config-if)#ip ospf message-digest-key 1 md5 cisco
R_CUNDINAMARCA(config-if)#ip ospf authentication message-digest
R_CUNDINAMARCA(config-if)#

R_CUNDINAMARCA#sh ip ospf interface s0/1/0
%Invalid interface type and number
R_CUNDINAMARCA#sh ip ospf interface s0/0/0

Serial0/0/0 is up, line protocol is up
Internet address is 172.31.2.38/30, Area 0
Process ID 1, Router ID 172.31.2.38, Network Type POINT-TO-POINT, Cost:
64
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 00:00:09
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 1 , Adjacent neighbor count is 1
```

```
Adjacent with neighbor 209.17.220.3
Suppress hello for 0 neighbor(s)
Message digest authentication enabled
Youngest key id is 1
R_CUNDINAMARCA#
```

Listas de control de acceso:

Los hosts de VLAN 20 en Cundinamarca no acceden a internet, solo a la red interna de Tunja.

```
R_CUNDINAMARCA(config)#access-list 101 permit ip 172.31.1.64 0.0.0.63
172.31.0.128 0.0.0.63
R_CUNDINAMARCA(config)#access-list 101 permit ip 172.31.1.64 0.0.0.63
172.31.0.192 0.0.0.63
R_CUNDINAMARCA(config)#access-list 101 deny tcp 172.31.0.192 0.0.0.63 host
209.17.220.2 eq www
R_CUNDINAMARCA(config)#access-list 101 deny tcp 172.31.0.192 0.0.0.63 host
209.17.220.2 eq 443
R_CUNDINAMARCA(config)#interface f0/0.20
R_CUNDINAMARCA(config-subif)#ip access-group 101 in
```

Los hosts de VLAN 10 en Cundinamarca si acceden a internet y no a la red interna de Tunja.
Se corrige Los hosts de VLAN 30 en Cundinamarca si acceden a internet y no a la red interna de Tunja.

```
R_CUNDINAMARCA(config-subif)#access-list 102 permit ip 172.31.1.0
0.0.0.63 209.17.220.2 0.0.0.255
R_CUNDINAMARCA(config)#access-list 102 deny ip 172.31.1.0 0.0.0.63
172.31.0.128 0.0.0.63
R_CUNDINAMARCA(config)#access-list 102 deny ip 172.31.1.0 0.0.0.63
172.31.0.192 0.0.0.63
R_CUNDINAMARCA(config)#access-list 102 deny ip 172.31.1.0 0.0.0.63
172.31.2.16 0.0.0.7
R_CUNDINAMARCA(config)#interface f0/0.30
R_CUNDINAMARCA(config-subif)#ip access-group 102 in
```

Los hosts de VLAN 30 en Tunja solo acceden a servidores web y ftp de internet.

```
R_TUNJA(config)#access-list 103 permit tcp 172.31.0.192 0.0.0.63
host 209.17.220.2 eq www
R_TUNJA(config)#access-list 103 permit tcp 172.31.0.192 0.0.0.63
host 209.17.220.2 eq 443
R_TUNJA(config)#access-list 103 permit tcp 172.31.0.192 0.0.0.63
host 209.17.220.2 eq ftp
R_TUNJA(config)#interface fastEthernet 0/0.30
R_TUNJA(config-subif)#ip access-group 103 in
```

Los hosts de VLAN 20 en Tunja solo acceden a la VLAN 20 de Cundinamarca y VLAN 10 de Bucaramanga.

```
R_TUNJA(config)#access-list 104 permit ip 172.31.0.128 0.0.0.63
172.31.1.64 0.0.0.63
R_TUNJA(config)#access-list 104 permit ip 172.31.0.128 0.0.0.63
172.31.0.0 0.0.0.63
R_TUNJA(config)#interface fastEthernet 0/0.20
R_TUNJA(config-subif)#ip access-group 104 in
```

Los hosts de VLAN 30 de Bucaramanga acceden a internet y a cualquier equipo de VLAN 10.

```
R_BUCARAMANGA(config)#access-list 106 permit tcp 172.31.0.64
0.0.0.63 host 209.17.220.2 eq www
R_BUCARAMANGA(config)#access-list 106 permit tcp 172.31.0.64
0.0.0.63 host 209.17.220.2 eq 443
R_BUCARAMANGA(config)#access-list 106 permit ip 172.31.0.64 0.0.0.63
172.31.0.0 0.0.0.63
R_BUCARAMANGA(config)#interface f0/0.30
R_BUCARAMANGA(config-subif)#ip access-group 106 in
```

Los hosts de VLAN 10 en Bucaramanga acceden a la red de Cundinamarca (VLAN 20) y Tunja (VLAN 20), no internet.

```
R_BUCARAMANGA(config)#access-list 105 permit ip 172.31.0.0 0.0.0.63
172.31.0.128 0.0.0.63
R_BUCARAMANGA(config)#access-list 105 permit ip 172.31.0.0 0.0.0.63
172.31.1.64 0.0.0.63
R_BUCARAMANGA(config)#access-list 105 deny tcp 172.31.0.0 0.0.0.63
host 209.17.220.2 eq www
R_BUCARAMANGA(config)#access-list 105 deny tcp 172.31.0.0 0.0.0.63
host 209.17.220.2 eq 443
R_BUCARAMANGA(config)#interface f0/0.10
R_BUCARAMANGA(config-subif)#ip access-group 105 in
```

Los hosts de una VLAN no pueden acceder a los de otra VLAN en una ciudad. Este punto se realiza y se entienda que las Vlans de una ciudad no se pueden ver entre sí.

```
R_BUCARAMANGA(config)#access-list 107 deny ip 172.31.0.0 0.0.0.63
172.31.0.64 0.0.0.63
R_BUCARAMANGA(config)#interface f0/0.10
R_BUCARAMANGA(config-subif)#ip access-group 107 in

R_BUCARAMANGA(config)#access-list 108 deny ip 172.31.0.64 0.0.0.63
172.31.0.0 0.0.0.63
R_BUCARAMANGA(config)#interface f0/0.30
R_BUCARAMANGA(config-subif)#ip access-group 108 in
```

```
R_TUNJA(config)#access-list 109 deny ip 172.31.0.128 0.0.0.63
172.31.0.192 0.0.0.63
R_TUNJA(config)#interface f0/0.20
R_TUNJA (config-subif)#ip access-group 109 in

R_TUNJA(config)#access-list 110 deny ip 172.31.0.192 0.0.0.63
172.31.0.128 0.0.0.63
R_TUNJA(config)#interface f0/0.30
R_TUNJA (config-subif)#ip access-group 110 in

R_CUNDINAMARCA(config)#access-list 111 deny ip 172.31.1.64 0.0.0.63
172.31.0.128 0.0.0.63
R_CUNDINAMARCA(config)#access-list 111 deny ip 172.31.1.64 0.0.0.63
172.31.2.24 0.0.0.7
R_CUNDINAMARCA (config)#interface f0/0.20
R_CUNDINAMARCA (config-subif)#ip access-group 111 in
R_CUNDINAMARCA(config)#access-list 112 deny ip 172.31.1.0 0.0.0.63
172.31.1.64 0.0.0.63
R_CUNDINAMARCA(config)#access-list 111 deny ip 172.31.1.0 0.0.0.63
172.31.2.24 0.0.0.7
R_CUNDINAMARCA (config)#interface f0/0.30
R_CUNDINAMARCA (config-subif)#ip access-group 112 in
R_CUNDINAMARCA(config)#access-list 112 deny ip 172.31.2.24 0.0.0.7
172.31.1.64 0.0.0.63
R_CUNDINAMARCA(config)#access-list 111 deny ip 172.31.2.24 0.0.0.7
172.31.1.0 0.0.0.63
R_CUNDINAMARCA (config)#interface f0/0.30
R_CUNDINAMARCA (config-subif)#ip access-group 112 in
```

Solo los hosts de las VLAN administrativas y de la VLAN de servidores tienen acceso a los routers e internet.

Acceso Vlan 1 Bucaramanga a los router e internet

```
R_BUCARAMANGA(config)#access-list 113 permit ip 172.31.2.1 0.0.0.7
172.31.2.1 0.0.0.7
R_BUCARAMANGA(config)#access-list 113 permit ip 172.31.2.1 0.0.0.7
172.31.2.34 0.0.0.3
R_BUCARAMANGA(config)#access-list 113 permit ip 172.31.2.1 0.0.0.7
172.31.2.38 0.0.0.3
R_BUCARAMANGA(config)#access-list 113 permit tcp 172.31.2.1 0.0.0.7 host
209.17.220.2 eq 443
R_BUCARAMANGA(config)#access-list 113 permit tcp 172.31.2.1 0.0.0.7 host
209.17.220.2 eq www
R_BUCARAMANGA(config)#interface f0/0.1
R_BUCARAMANGA(config-subif)#ip access-group 113 in
```

Acceso Vlan 1 Tunja a los router e internet

```
R_TUNJA (config)#access-list 114 permit ip 172.31.2.16 0.0.0.7
172.31.2.17 0.0.0.7
R_TUNJA (config)#access-list 114 permit ip 172.31.2.16 0.0.0.7
172.31.2.33 0.0.0.3
```

```
R_TUNJA (config)#access-list 114 permit ip 172.31.2.16 0.0.0.7
172.31.2.38 0.0.0.3
R_TUNJA (config)#access-list 114 permit tcp 172.31.2.16 0.0.0.7 host
209.17.220.2 eq 443
R_TUNJA (config)#access-list 114 permit tcp 172.31.2.16 0.0.0.7 host
209.17.220.2 eq www
R_TUNJA (config)#interface f0/0.1
R_TUNJA (config-subif)#ip access-group 114 in
```

Acceso Vlan 1 Cundinamarca a los router e internet

```
R_CUNDINAMARCA config)#access-list 115 permit ip 172.31.2.8 0.0.0.7
172.31.2.9 0.0.0.7
R_CUNDINAMARCA (config)#access-list 115 permit ip 172.31.2.8 0.0.0.7
172.31.2.37 0.0.0.3
R_CUNDINAMARCA (config)#access-list 115 permit ip 172.31.2.8 0.0.0.7
172.31.2.33 0.0.0.3
R_CUNDINAMARCA (config)#access-list 115 permit tcp 172.31.2.8 0.0.0.7 host
209.17.220.2 eq 443
R_CUNDINAMARCA (config)#access-list 115 permit tcp 172.31.2.8 0.0.0.7 host
209.17.220.2 eq www
R_CUNDINAMARCA (config)#interface f0/0.1
R_CUNDINAMARCA (config-subif)#ip access-group 115 in
```

Acceso servidor interno a los router e internet

```
R_CUNDINAMARCA config)#access-list 116 permit ip 172.31.2.24 0.0.0.7
172.31.2.9 0.0.0.7
R_CUNDINAMARCA (config)#access-list 116 permit ip 172.31.2.24 0.0.0.7
172.31.2.37 0.0.0.3
R_CUNDINAMARCA (config)#access-list 116 permit ip 172.31.2.24 0.0.0.7
172.31.2.33 0.0.0.3
R_CUNDINAMARCA (config)#access-list 116 permit tcp 172.31.2.24 0.0.0.7
host 209.17.220.2 eq 443
R_CUNDINAMARCA (config)#access-list 116 permit tcp 172.31.2.24 0.0.0.7
host 209.17.220.2 eq www
R_CUNDINAMARCA (config)#interface f0/0.88
R_CUNDINAMARCA (config-subif)#ip access-group 116 in
```

Acceso servidor externo a los router

```
R_TUNJA (config)#access-list 117 permit ip 209.17.220.0 0.0.0.255
209.17.220.1 0.0.0.255
R_TUNJA (config)#access-list 117 permit ip 209.17.220.0 0.0.0.255
172.31.2.33 0.0.0.3
R_TUNJA (config)#access-list 117 permit ip 209.17.220.0 0.0.0.255
172.31.2.38 0.0.0.3
R_TUNJA (config)#interface f0/1
R_TUNJA (config-subif)#ip access-group 117 in
```

VLSM: utilizar la dirección 172.31.0.0 /18 para el direccionamiento.

Se utiliza el direccionamiento mencionado para toda la red, por eso se corrige la dirección ip mal asignada a la Vlan 1 de tunja.

Aspectos a tener en cuenta

- Habilitar VLAN en cada switch y permitir su enrutamiento.
- Enrutamiento OSPF con autenticación en cada router.
- Servicio DHCP en el router Tunja, mediante el helper address, para los routers Bucaramanga y
  Cundinamarca.
- Configuración de NAT estático y de sobrecarga.
- Establecer una lista de control de acceso de acuerdo con los criterios señalados.
- Habilitar las opciones en puerto consola y terminal virtual.

CONCLUSIONES

- Se aprendió a configurar redes WAN y LAN según las necesidades de las redes de comunicaciones descritas en los escenarios.
- Se configuró las listas de acceso necesarias para las comunicaciones directas, ya sea en una red LAN o WAN.
- Se realizó las conexiones a través de NAT o PAT entre IP privadas y públicas según los requerimientos de cada red.
- Se crearon vlans en las redes internas, y se brindó comunicación segura y detallada a cada uno de los segmentos de red.
- Se realizaron configuraciones de enrutamiento OSPF y EIGRIP según lo requerido en cada uno de los escenarios propuestos.
- Se aprendió a configurar servidores TFTP y DHCP, y se dio mayor agilidad y velocidad al sistema en las redes y más automáticas.

BIBLIOGRAFÍA

- CISCO. (2014). Configuración de un sistema operativo de red. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#2.0.1.1

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

- Vesga, J. (2014). PING y TRACER como estrategia en procesos de Networking [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgTCtKY-7F5KIRC3

- CISCO. (2014). Enrutamiento entre VLANs. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module5/index.html#5.0.1.1

- CISCO. (2014). Configuración y conceptos básicos de Switching. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module2/index.html#2.0.1.1

- CISCO. (2014). Listas de control de acceso. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module9/index.html#9.0.1.1

- 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