PRUEBA DE HABILIDADES PRACTICAS CCNA

CARLOS EDUARDO MURCIA ANGEL

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍAS E INGENIERÍAS
DIPLOMADO DE PROFUNDIZACIÓN CISCO
PLANADAS
2019

PRUEBA DE HABILIDADES PRACTICAS CCNA

CARLOS EDUARDO MURCIA ANGEL

EVALUACIÓN FINAL PARA OPTAR POR EL TÍTULO DE
INGENIERO DE SISTEMAS

ING. NILSON ALBEIRO FERREIRA MANZANARES
DOCENTE OCASIONAL

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍAS E INGENIERÍAS
DIPLOMADO DE PROFUNDIZACION CISCO
PLANADAS
2019

CONTENIDO

TABLA DE ILUSTRACIONES

INDICE DE TABLAS

Pág.

RESUMEN

Establecer canales tecnológicos de comunicación efectivos y seguros, requiere de conocimientos específicos como los que se adquiere en la formación teórico práctico que brinda el diplomado CCNA de la plataforma CISCO, en el análisis, diagnóstico y solución de casos reales, aportando a generar habilidades y fortalecer capacidades en el profesional; estos conocimientos permite instalar y configurar infraestructuras de redes que interconectan todos los dispositivos estratégicos de las empresas.

Los escenarios planteados en la prueba de habilidades requieren la necesidad de establecer soluciones de conectividad en los diferentes host, realizando las diferentes configuraciones tanto en los router como en los switch, implementando enrutamientos dinámicos y estáticos, VLAN, asignación de protocolos, alternativas de direccionamiento, seguridad, autenticación y conexión, aspectos generales de networking.

PALABRAS CLAVE: Networking, interconexión, direccionamiento, OSPF, protocolo, VLAN.

ABSTRACT

Establishing effective and safe technological communication channels requires specific knowledge such as those acquired in the practical theoretical training provided by the CCNA diploma of the CISCO platform, in the analysis, diagnosis and solution of real cases, contributing to generate skills and strengthen professional skills; This knowledge allows installing and configure network infrastructures that interconnect all the strategic devices of the companies.

The scenarios proposed in the skills test require the need to establish connectivity solutions on the different hosts, performing the different configurations on both the routers and the switches, implementing dynamic and static routing, VLAN, protocol assignment, routing alternatives, security, authentication and connection, general aspects of networking.

INTRODUCCIÓN

La interacción con herramientas dinámicas como Cisco Packet Tracer en la que articuló aprendizajes de los conceptos como protocolo de comunicación, configuración de sistemas operativos relacionados a la red, mecanismos para acceder a dispositivos remotos y características fundamentales para el diseño, configuración y supervisión de redes dinámicos y escalables.

El aprendizaje teórico práctico de casos reales ha aportado habilidades para la solución de problemas en la implementación de redes, subredes, y protocolos buscando la seguridad de los dispositivos y salvaguardar el bien más importante para cualquier empresa, la información. El presente diplomado de profundización y la prueba de habilidades reta a dar lo mejor de sí, pues se busca fortalecer el conocimiento a través de las últimas tecnologías y responder a las necesidades del mercado.

OBJETIVOS

OBJETIVO GENERAL

Resolver los escenarios propuestos por la prueba de habilidades CISCO CCNA1 y CCNA2.

OBJETIVOS ESPECÍFICOS

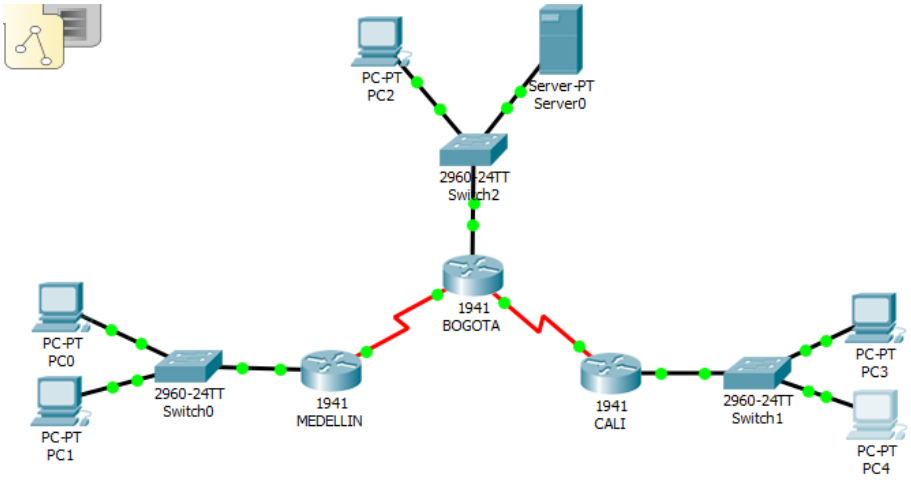
- Identificar la red propuesta y relacionar los dispositivos requeridos.
- Configurar cada uno de los dispositivos acorde a la guía.
- Implementar las listas de control de acceso ACL y establecer protocolos.
- Documentar paso a paso la configuración y resultados.

DESARROLLO DE LOS ESCENARIOS

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



Parte 1. Asignaciones de direcciones IP

- Se debe dividir (subnetear) la red creando una segmentación en ocho partes, para permitir crecimiento futuro de la red corporativa.

Tabla 1 Asignación de direcciones IP

DIRECCIONES IP	MASCARA SUBRED
192.168.1.0/27	255.255.255.224
192.168.1.32/27	255.255.255.224
192.168.1.64/27	255.255.255.224
192.168.1.96/27	255.255.255.224
192.168.1.128/27	255.255.255.224
192.168.1.160/27	255.255.255.224
192.168.1.192/27	255.255.255.224
192.168.1.224/27	255.255.255.224

Parte 2. Configuración básica

- Completar la siguiente tabla con la configuración básica de los routers, teniendo en cuenta las subredes diseñadas.
- Asignar el protocolo de enrutamiento EIGRP a los routers considerando el direccionamiento diseñado.

Programación R. Medellin

```
ROUTER>en
ROUTER#conf t
Enter configuration commands, one per line. End with CNTL/Z.
ROUTER(config)#hostname MEDELLIN
MEDELLIN(config)#no ip domain-lookup
MEDELLIN(config)#enable secret charly
MEDELLIN(config)#line con 0
MEDELLIN(config-line)#password class
MEDELLIN(config-line)#login
MEDELLIN(config-line)#line vty 0 4
MEDELLIN(config-line)#password class
MEDELLIN(config-line)#login
MEDELLIN(config-line)#exit
MEDELLIN(config)#service password-encryption
MEDELLIN(config)#banner motd "Equipo Protegido, Acceso Denegado"!
MEDELLIN(config)#int s0/0/0
MEDELLIN(config-if)#ip address 192.168.1.99 255.255.255.224
MEDELLIN(config-if)#no shutdown
MEDELLIN(config)#int g0/0
MEDELLIN(config-if)#ip address 192.168.1.33 255.255.255.224
MEDELLIN(config-if)#no shutdown
MEDELLIN(config-if)#exit
MEDELLIN(config)#router eigrp 200
MEDELLIN(config-router)#network 192.168.1.0 255.255.255.224
MEDELLIN(config-router)#no auto-summary
```

Programación R. Bogota

```
ROUTER>en
ROUTER#conf t
Enter configuration commands, one per line. End with CNTL/Z.
ROUTER(config)#hostname BOGOTA
```

```
BOGOTA(config)#no ip domain-lookup
BOGOTA(config)#enable secret charly
BOGOTA(config)#line con 0
BOGOTA(config-line)#password class
BOGOTA(config-line)#login
BOGOTA(config-line)#line vty 0 4
BOGOTA(config-line)#password class
BOGOTA(config-line)#login
BOGOTA(config-line)#exit
BOGOTA(config)#service password-encryption
BOGOTA(config)#banner motd "Equipo Protegido, Acceso Denegado"!
BOGOTA(config)#int s0/0/0
BOGOTA(config-if)#ip address 192.168.1.98 255.255.255.224
BOGOTA(config-if)#no shutdown
BOGOTA(config)#int s0/0/1
BOGOTA(config-if)#ip address 192.168.1.130 255.255.255.224
BOGOTA(config-if)#no shutdown
BOGOTA(config)#int g0/0
BOGOTA(config-if)#ip address 192.168.1.1 255.255.255.224
BOGOTA(config-if)#no shutdown
BOGOTA(config-if)#exit
BOGOTA(config)#router eigrp 200
BOGOTA(config-router)#network 192.168.1.0 255.255.255.224
BOGOTA(config-router)#no auto-summary
```

Programación R. Cali

```
ROUTER>en
ROUTER#conf t
Enter configuration commands, one per line. End with CNTL/Z.
ROUTER(config)#hostname CALI
CALI(config)#no ip domain-lookup
CALI(config)#enable secret charly
CALI(config)#line con 0
CALI(config-line)#password class
CALI(config-line)#login
CALI(config-line)#line vty 0 4
CALI(config-line)#password class
CALI(config-line)#login
CALI(config-line)#exit
CALI(config)#service password-encryption
CALI(config)#banner motd "Equipo Protegido, Acceso Denegado"!
```

CALI(config)#int s0/0/0
CALI(config-if)#ip address 192.168.1.131 255.255.255.224
CALI(config-if)#no shutdown
CALI(config)#int g0/0
CALI(config-if)#ip address 192.168.1.65 255.255.255.224
CALI(config-if)#no shutdown
CALI(config-if)#exit
CALI(config)#router eigrp 200
CALI(config-router)#network 192.168.1.0 255.255.255.224
CALI(config-router)#no auto-summary

Parte 3. Configuración de Enrutamiento

- 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.
- Verificar si existe vecindad con los routers configurados con EIGRP.
- Realizar la comprobación de las tablas de enrutamiento en cada uno de los routers para verificar cada una de las rutas establecidas.

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, 00:33:41, 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 [90/2684416] via 192.168.1.98, 00:33:40, 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, 00:33:40, Serial0/0/0

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 [90/2172416] via 192.168.1.99, 00:38:58, Serial0/0/0
D 192.168.1.64/27 [90/2172416] via 192.168.1.131, 00:38:57, 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

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, 00:07:35, Serial0/0/0
D 192.168.1.32/27 [90/2684416] via 192.168.1.130, 00:07:35, 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, 00:07:35, 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

a. Realizar un diagnóstico de vecinos uando el comando cdp.

MEDELLIN#show cdp neighbors detail

Device ID: Switch
Entry address(es):
Platform: cisco 2960, Capabilities: Switch
Interface: GigabitEthernet0/0, Port ID (outgoing port): FastEthernet0/1
Holdtime: 160

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: 144

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

BOGOTA#show cdp neighbors detail

Device ID: Switch
Entry address(es):
Platform: cisco 2960, Capabilities: Switch
Interface: GigabitEthernet0/0, Port ID (outgoing port): FastEthernet0/1
Holdtime: 171

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: 171

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: 171

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

CALI#show cdp neighbors detail

Device ID: Switch
Entry address(es):
Platform: cisco 2960, Capabilities: Switch
Interface: GigabitEthernet0/0, Port ID (outgoing port): FastEthernet0/1
Holdtime: 142

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: 132

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

- 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.

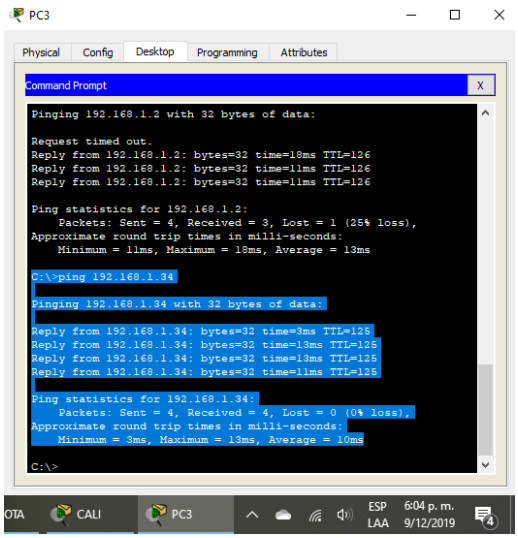


Ilustración 1 Ping red Cali a red Medellin

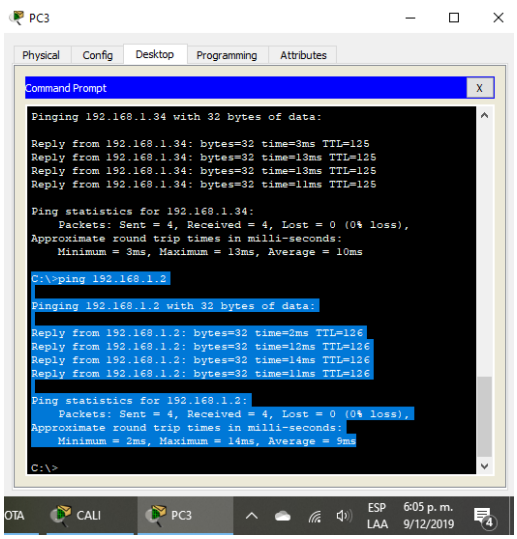


Ilustración 2 Ping red Cali a red Bogota

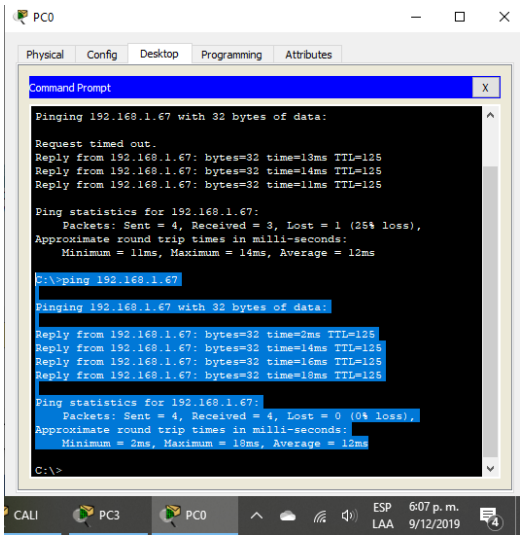


Ilustración 3 Ping red Medellin a red Cali

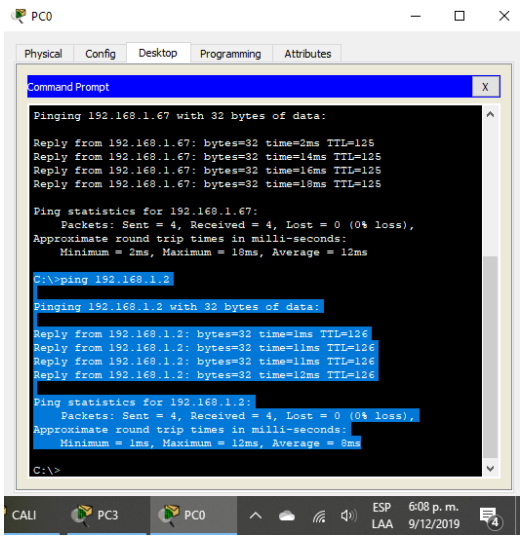


Ilustración 4 Ping red Medellin a red Bogota

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

```
CALI#conf t
Enter configuration commands, one per line. End with CNTL/Z.
CALI(config)#int g0/0
CALI(config-if)#ip access-group 101 in
CALI(config-if)#access-list 101 permit icmp any any echo-reply

CALI(config-if)#ip access-group 103 in
CALI(config-if)#access-list 103 permit tcp any any eq www

MEDELLIN#conf t
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN(config)#int g0/0
MEDELLIN(config-if)#ip access-group 101 in
MEDELLIN(config-if)#access-list 101 permit icmp any any echo-reply

MEDELLIN(config-if)#ip access-group 103 in
MEDELLIN(config-if)#access-list 103 permit tcp any any eq www
```

- 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.

```
MEDELLIN(config)#int g0/0
MEDELLIN(config-if)#ip access-group 102 in
MEDELLIN(config-if)#access-list 102 deny tcp any any eq 23
MEDELLIN(config)#access-list 102 permit ip any any

CALI(config)#int g0/0
CALI(config-if)#ip access-group 102 in
CALI(config-if)#access-list 102 deny tcp any any eq 23
CALI(config)#access-list 102 permit ip any any
```

- 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.

```
BOGOTA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA(config)#int g0/0
BOGOTA(config-if)#access-list 1 deny 192.168.1.3
```

```
BOGOTA(config)#access-list 1 permit any
BOGOTA(config)#ip access-group in
BOGOTA(config)#int g0/0
BOGOTA(config-if)#ip access-group 1 in
BOGOTA(config-if)#
```

Parte 5. Comprobación de la red instalada

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

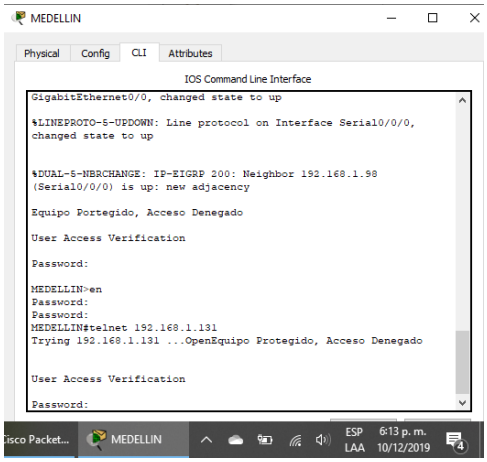


Ilustración 5 Telnet R Bogota a R. Medellin

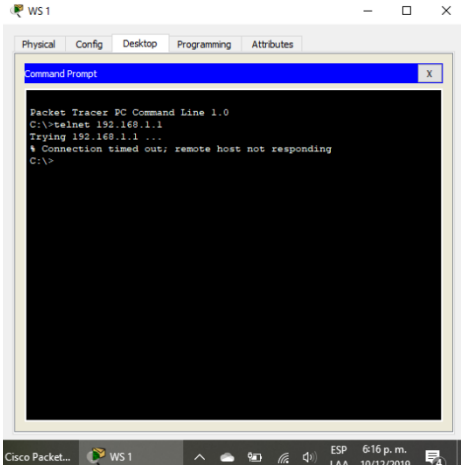


Ilustración 6 Telnet WS_1 a R. Bogota

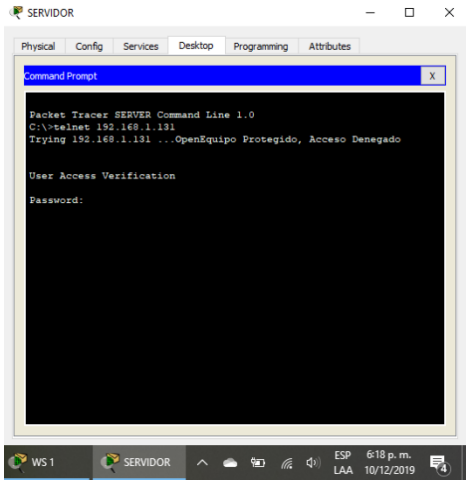


Ilustración 8 Telnet Servidor a R. Cali

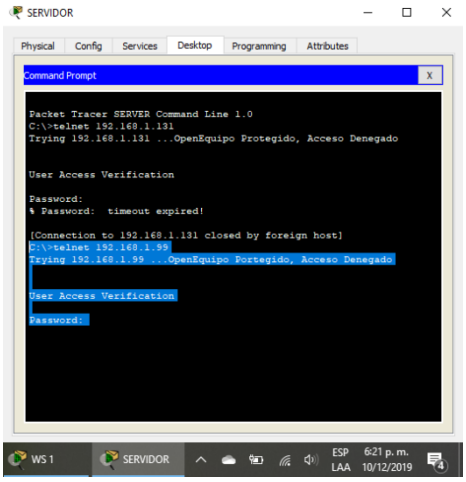


Ilustración 7 Telnet Servidor a R. Medellin

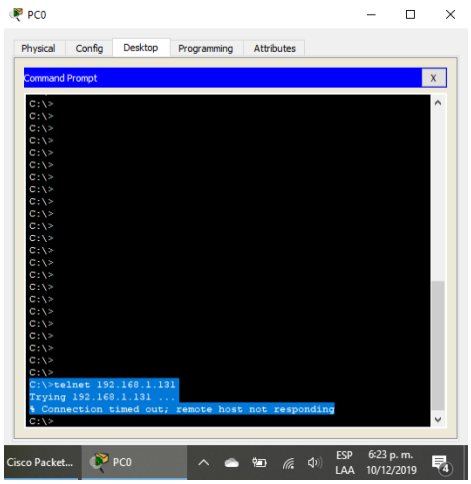


Ilustración 9 Telnet host red Medellin a R. Cali

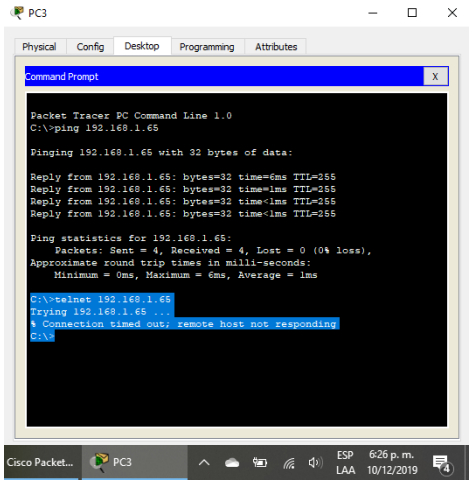


Ilustración 10 Telnet host red Cali a R. Cali

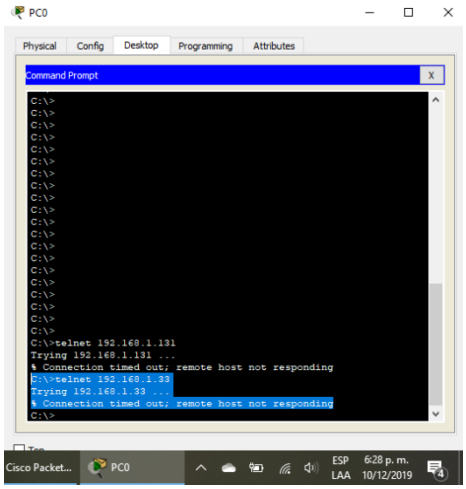


Ilustración 12 Telnet host red Medellin a R. Medellin

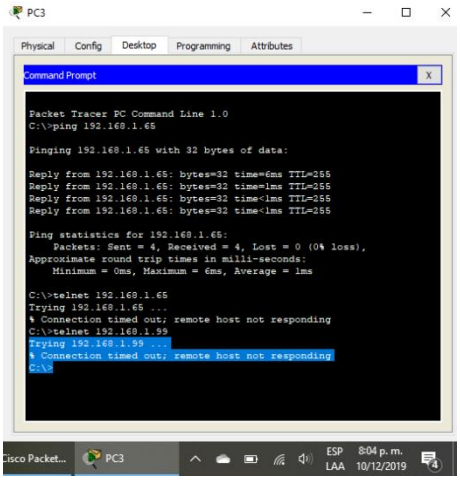


Ilustración 11 Telnet host red Cali a R. Medellin

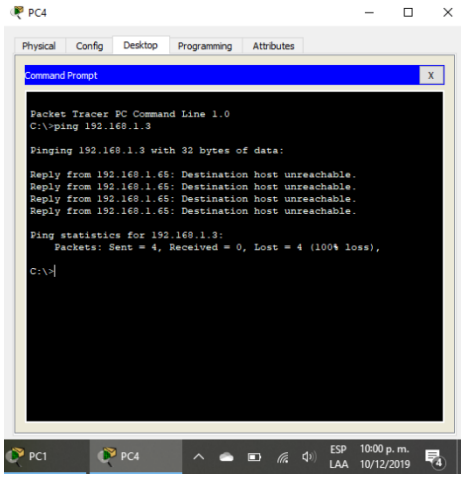


Ilustración 13 Ping host R. Cali a WS_1

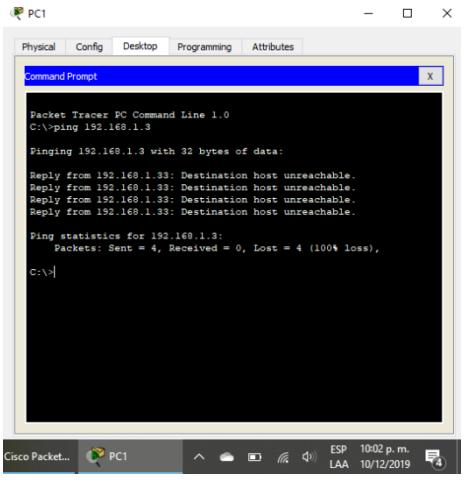


Ilustración 14 Ping host R. Medellin a WS_1

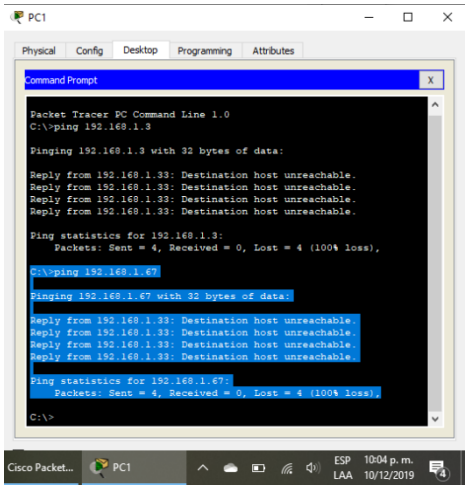


Ilustración 15 Ping host R. Medellin a host R. Cali

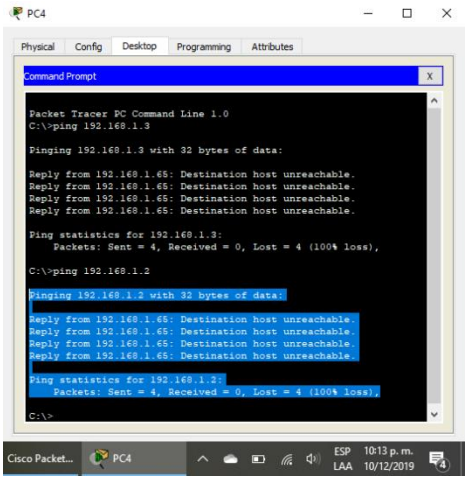


Ilustración 16 Ping host R. Cali a Servidor

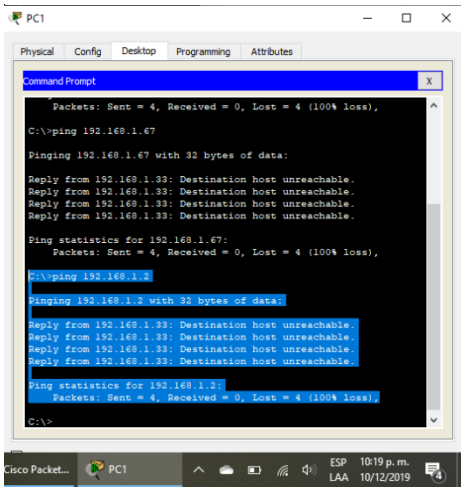


Ilustración 18 Ping host R. Medellin a Servidor

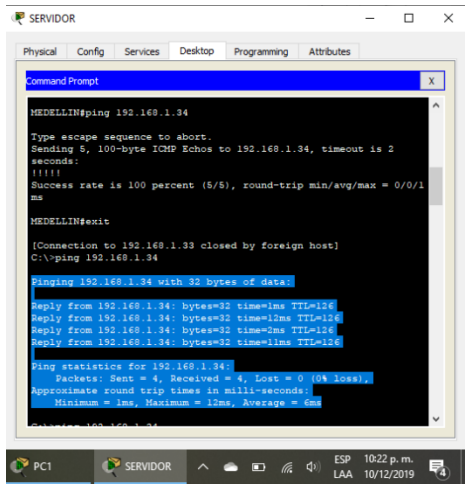


Ilustración 17 Ping servidor a host R. Medellin

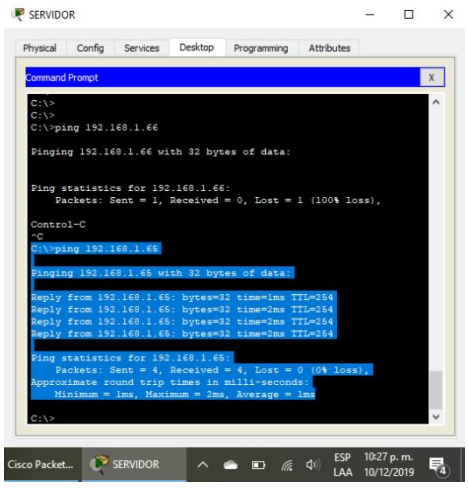


Ilustración 20 Ping Servidor a host R. Cali

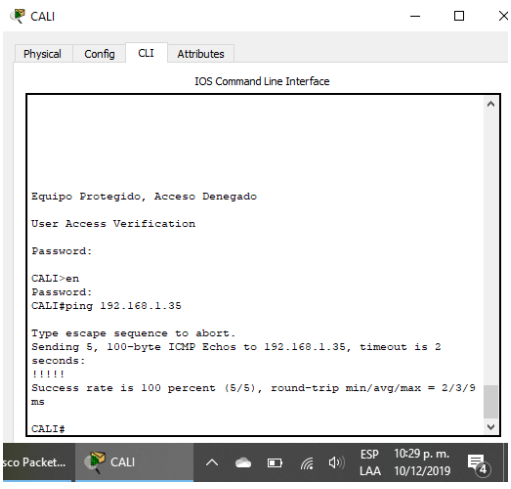


Ilustración 19 Ping R. Cali a host R. Medellin

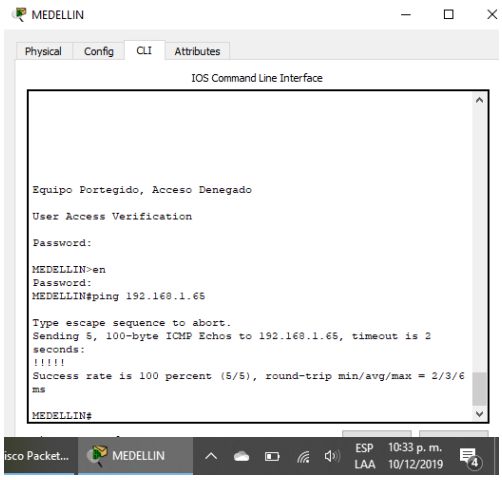


Ilustración 21 Ping R. Medellin a host R. Cali

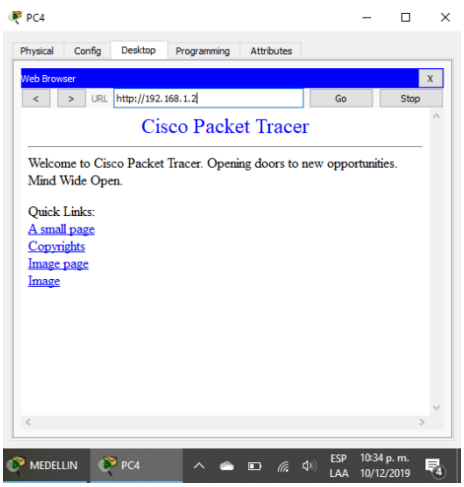


Ilustración 22 Acceso de host R. Cali a Servidor mediante protocolo www (puerto 80).

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

Tabla 2 Condiciones de prueba

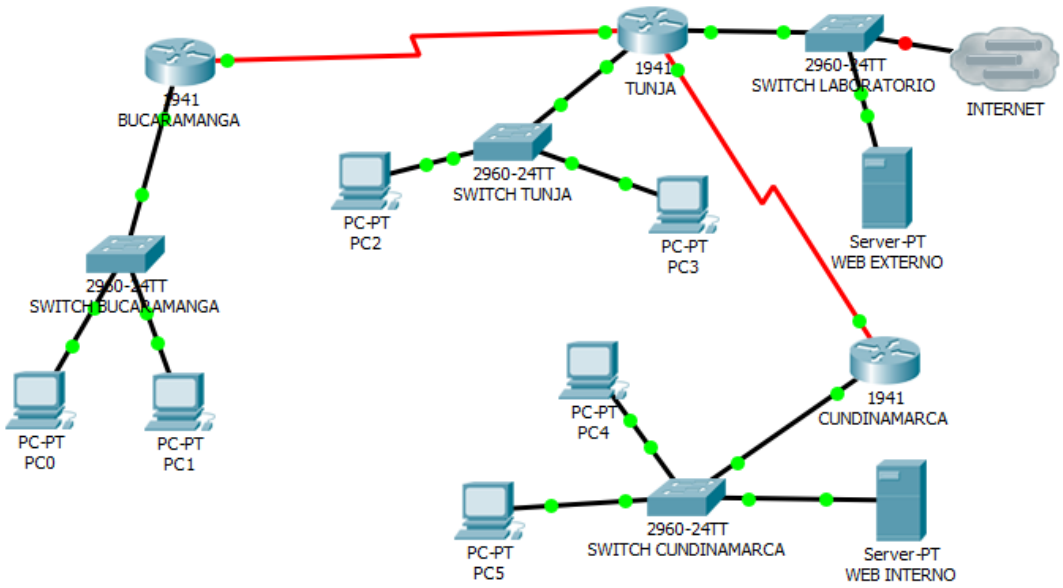
	ORIGEN	DESTINO	RESULTADO
TELNET	Router MEDELLIN	Router CALI	User Access Verification
	WS_1	Router BOGOTA	% Connection timed out; remote host not responding
	Servidor	Router CALI	User Access Verification
	Servidor	Router MEDELLIN	User Access Verification
TELNET	LAN del Router MEDELLIN	Router CALI	% Connection timed out; remote host not responding
	LAN del Router CALI	Router CALI	% Connection timed out; remote host not responding
	LAN del Router MEDELLIN	Router MEDELLIN	% Connection timed out; remote host not responding
	LAN del Router CALI	Router MEDELLIN	% Connection timed out; remote host not responding
PING	LAN del Router CALI	WS_1	Destination host unreachable
	LAN del Router MEDELLIN	WS_1	Destination host unreachable
	LAN del Router MEDELLIN	LAN del Router CALI	Destination host unreachable
PING	LAN del Router	Servidor	Destination host unreachable

	CALI		
	LAN del Router MEDELLIN	**Servidor**	Destination host unreachable
	Servidor	**LAN del Router MEDELLIN**	Destino host alcanzable
	Servidor	**LAN del Router CALI**	Destino host alcanzable
	Router CALI	**LAN del Router MEDELLIN**	Destino host alcanzable
	Router MEDELLIN	**LAN del Router CALI**	Destino host alcanzable

Se denegaron protocolos de los host en la LAN Medellín y Cali, imposibilitando la comunicación con otros dispositivos (telnet, ICMP), pero si se logró interconectar con el Servidor mediante el protocolo WWW (puerto 80).

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.



Los siguientes son los requerimientos necesarios:

1. Todos los routers deberán tener lo siguiente:

   - Configuración básica

```
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname BUCARAMANGA
BUCARAMANGA(config-if)#int g0/0.1
BUCARAMANGA(config-subif)#encapsulation dot1q 1 native
BUCARAMANGA(config-subif)#ip address 172.31.2.1 255.255.255.248
BUCARAMANGA(config-subif)#int g0/0.10
BUCARAMANGA(config-subif)#encapsulation dot1q 10
BUCARAMANGA(config-subif)#ip address 172.31.0.1 255.255.255.192
BUCARAMANGA(config-subif)#ip helper-address 172.31.2.34
BUCARAMANGA(config-subif)#ip access-group 101 in
BUCARAMANGA(config)#int g0/0.30
BUCARAMANGA(config-subif)#encapsulation dot1q 30
BUCARAMANGA(config-subif)#ip address 172.31.0.64 255.255.255.192
BUCARAMANGA(config-subif)#ip helper-address 172.31.2.34
BUCARAMANGA(config-subif)#ip access-group 103 in
BUCARAMANGA(config-subif)#exit
BUCARAMANGA(config)#int s0/0/0
BUCARAMANGA(config-if)#ip address 172.31.2.33 255.255.255.252
BUCARAMANGA(config-if)#ip ospf message-digest-key 1 md5 7 network
```

```
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname TUNJA
TUNJA(config)#router ospf 1
TUNJA(config-router)#log-adjacency-changes
TUNJA(config-router)#area 0 authentication message-digest
TUNJA(config-router)#network 172.31.0.128 0.0.0.63 area 0
TUNJA(config-router)#network 172.31.0.192 0.0.0.63 area 0
TUNJA(config-router)#network 172.31.2.8 0.0.0.7 area 0
TUNJA(config-router)#network 172.31.2.32 0.0.0.7 area 0
TUNJA(config-router)#default-information originate
TUNJA(config)#int g0/0
TUNJA(config-if)#no shutdown
```

```
TUNJA(config)#ip nat inside source list 20 interface g0/1 overload
TUNJA(config)#ip nat inside source static 172.31.2.26 209.17.220.10

TUNJA(config)#login block-for 240 attempts 4 within 120
TUNJA(config)#enable secret 1234
TUNJA(config)#aaa new-model
TUNJA(config)#aaa authentication login default local

TUNJA(config)#int g0/0
TUNJA(config-if)#ip address 209.17.220.220 255.255.255.0
TUNJA(config-if)#ip address 209.17.220.1 255.255.255.0
TUNJA(config-if)#int g0/0
TUNJA(config-if)#ip address 209.17.220.1 255.255.255.0
TUNJA(config-if)#ip nat outside
TUNJA(config-if)#duplex auto
TUNJA(config-if)#speed auto
TUNJA(config-if)#int g0/1
TUNJA(config-if)#no ip address
TUNJA(config-if)#ip nat outside
TUNJA(config-if)#duplex auto
TUNJA(config-if)#speed auto

TUNJA(config-if)#int g0/1.1
TUNJA(config-subif)#encapsulation dot1q 1 native
TUNJA(config-subif)#ip address 172.31.2.9 255.255.255.248
TUNJA(config-subif)#int g0/1.20
TUNJA(config-subif)#encapsulation dot1q 20
TUNJA(config-subif)#ip address 172.31.0.129 255.255.255.192
TUNJA(config-subif)#ip access-group 102 in
TUNJA(config-subif)#int g0/1.30
TUNJA(config-subif)#encapsulation dot1q 30
TUNJA(config-subif)#ip address 172.31.0.193 255.255.255.192
TUNJA(config-subif)#ip access-group 103 in
TUNJA(config-subif)#exit

TUNJA(config)#int s0/0/0
TUNJA(config-if)#ip address 172.31.2.34 255.255.255.252
TUNJA(config-if)#ip ospf message-digest-key 1 md5 7 network
TUNJA(config-if)#ip nat inside
TUNJA(config-if)#clock rate 64000

TUNJA(config-if)#int s0/0/1
TUNJA(config-if)#ip address 172.31.2.38 255.255.255.252
TUNJA(config-if)#ip ospf message-digest-key 1 md5 7 network
```

```
TUNJA(config-if)#ip nat inside
TUNJA(config-if)#clock rate 64000
TUNJA(config-if)#interface vlan1
TUNJA(config-if)#no ip address
TUNJA(config-if)#shutdown

TUNJA(config)#ip dhcp pool bucaramanga-30
TUNJA(dhcp-config)#network 172.31.0.64 255.255.255.192
TUNJA(dhcp-config)#default-router 172.31.0.65
TUNJA(dhcp-config)#ip dhcp pool t-10
TUNJA(dhcp-config)#network 172.31.1.0 255.255.255.192
TUNJA(dhcp-config)#default-router 172.31.1.1
TUNJA(dhcp-config)#ip dhcp pool t-20
TUNJA(dhcp-config)#network 172.31.1.64 255.255.255.192
TUNJA(dhcp-config)#default-router 172.31.1.65
TUNJA(dhcp-config)#ip dhcp pool t-20
TUNJA(dhcp-config)#ip dhcp pool bucaramanga-10
TUNJA(dhcp-config)#network 172.31.0.0 255.255.255.192
TUNJA(dhcp-config)#default-router 172.31.0.1


Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname CUNDINAMARCA
CUNDINAMARCA(config)#login block-for 240 attempts 4 within 120
CUNDINAMARCA(config)#enable secret 1234
CUNDINAMARCA(config)#int g0/0
CUNDINAMARCA(config-if)#no ip address
CUNDINAMARCA(config-if)#duplex auto
CUNDINAMARCA(config-if)#speed auto
CUNDINAMARCA(config-if)#int g0/0.1
CUNDINAMARCA(config-subif)#encapsulation dot1q 1 native
CUNDINAMARCA(config-subif)#ip address 172.31.2.17 255.255.255.248
CUNDINAMARCA(config-subif)#int g0/0.10
CUNDINAMARCA(config-subif)#encapsulation dot1q 10
CUNDINAMARCA(config-subif)#ip address 172.31.1.65 255.255.255.192
CUNDINAMARCA(config-subif)#ip helper-address 172.31.2.38
CUNDINAMARCA(config-subif)#ip access-group 101 in
CUNDINAMARCA(config-subif)#int g0/1.20
CUNDINAMARCA(config-subif)#encapsulation dot1q 20
CUNDINAMARCA(config-subif)#ip address 172.31.1.1 255.255.255.192
CUNDINAMARCA(config-subif)#ip helper-address 172.31.2.38
CUNDINAMARCA(config-subif)#ip access-group 102 in
```

```
CUNDINAMARCA(config-subif)#int g0/0.88
CUNDINAMARCA(config-subif)#encapsulation dot1q 88 native
CUNDINAMARCA(config-subif)#ip address 172.31.2.25 255.255.255.248
CUNDINAMARCA(config-subif)#int s0/0/0
CUNDINAMARCA(config-if)#ip address 172.31.2.37 255.255.255.252
CUNDINAMARCA(config-if)#ip ospf message-digest-key 1 md5 7 network
CUNDINAMARCA(config-if)#router ospf 1
CUNDINAMARCA(config-router)#area 0 authentication message-digest
```

- Autenticación local con AAA.

```
BUCARAMANGA>en
BUCARAMANGA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
BUCARAMANGA(config)#aaa new-model
BUCARAMANGA(config)#aaa au
BUCARAMANGA(config)#aaa authentication login default local
BUCARAMANGA(config)#aaa authorization exec default local
BUCARAMANGA(config)#aaa authorization network default local
BUCARAMANGA(config)#username carlos privilege 15 password 0 asdf
BUCARAMANGA(config)#username murcia privilege 1 password 0 asdf
BUCARAMANGA(config)#line vty 0 4
BUCARAMANGA(config-line)#privilege level 15
BUCARAMANGA(config-line)#transport input ssh
BUCARAMANGA(config-line)#
```

```
TUNJA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
TUNJA(config)#aaa new-model
TUNJA(config)#aaa authentication login default local
TUNJA(config)#aaa authorization exec default local
TUNJA(config)#aaa authorization network default local
TUNJA(config)#username carlos privilege 15 password 0 asdf
TUNJA(config)#username murcia privilege 1 password 0 asdf
TUNJA(config)#line vty 0 4
TUNJA(config-line)#privilege level 15
TUNJA(config-line)#transport input ssh
TUNJA(config-line)#
```

```
CUNDINAMARCA#conf t
```

Enter configuration commands, one per line. End with CNTL/Z.
CUNDINAMARCA(config)#aaa new-model
CUNDINAMARCA(config)#aaa authentication login default local
CUNDINAMARCA(config)#aaa authorization exec default local
CUNDINAMARCA(config)#aaa authorization network default local
CUNDINAMARCA(config)#username carlos privilege 15 password 0 asdf
CUNDINAMARCA(config)#username murcia privilege 1 password 0 asdf
CUNDINAMARCA(config)#line vty 0 4
CUNDINAMARCA(config-line)#privilege level 15
CUNDINAMARCA(config-line)#transport input ssh
CUNDINAMARCA(config-line)#

- Un máximo de intentos para acceder al router.
- Máximo tiempo de acceso al detectar ataques.
- Enrutamiento autenticado.

BUCARAMANGA(config)#ip domain name UNAD.NET
BUCARAMANGA(config)#username carlos pass asdf
BUCARAMANGA(config)#crypto key generate rsa
The name for the keys will be: BUCARAMANGA.UNAD.NET
Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

BUCARAMANGA(config)#ip ssh authentication-retries 3
*mar. 1 0:3:55.336: %SSH-5-ENABLED: SSH 1.99 has been enabled
BUCARAMANGA(config)#ip ssh time-out 120
BUCARAMANGA(config)#line vty 0 15
BUCARAMANGA(config-line)#transport input ssh
BUCARAMANGA(config-line)#end
BUCARAMANGA#
%SYS-5-CONFIG_I: Configured from console by console

BUCARAMANGA#show ip ssh
SSH Enabled - version 1.99
Authentication timeout: 120 secs; Authentication retries: 3
BUCARAMANGA#

```
TUNJA(config)#ip domain name UNAD.NET
TUNJA(config)#username carlos pass asdf
TUNJA(config)#crypto key generate rsa
The name for the keys will be: TUNJA.UNAD.NET
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

TUNJA(config)#ip ssh authentication-retries 3
*mar. 1 0:8:5.796: %SSH-5-ENABLED: SSH 1.99 has been enabled
TUNJA(config)#ip ssh time-out 120
TUNJA(config)#line vty 0 15
TUNJA(config-line)#transport input ssh
TUNJA(config-line)#end
TUNJA#
%SYS-5-CONFIG_I: Configured from console by console

TUNJA#show ip ssh
SSH Enabled - version 1.99
Authentication timeout: 120 secs; Authentication retries: 3
TUNJA#
```

```
CUNDINAMARCA(config)#ip domain name UNAD.NET
CUNDINAMARCA(config)#username carlos pass asdf
CUNDINAMARCA(config)#crypto key generate rsa
The name for the keys will be: CUNDINAMARCA.UNAD.NET
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

CUNDINAMARCA(config)#ip ssh authentication-retries 3
*mar. 1 0:11:53.981: %SSH-5-ENABLED: SSH 1.99 has been enabled
CUNDINAMARCA(config)#ip ssh time-out 120
CUNDINAMARCA(config)#line vty 0 15
CUNDINAMARCA(config-line)#transport input ssh
CUNDINAMARCA(config-line)#end
CUNDINAMARCA#
```

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

CUNDINAMARCA#show ip ssh
SSH Enabled - version 1.99
Authentication timeout: 120 secs; Authentication retries: 3
CUNDINAMARCA#

- Listas de control de acceso

BUCARAMANGA(config)#access-list 101 permit udp host 0.0.0.0 eq bootpc host 255.255.255.255 eq bootps
BUCARAMANGA(config)#access-list 101 permit ip 172.31.0.0 0.0.0.63 172.31.0.128 0.0.0.63
BUCARAMANGA(config)#access-list 101 permit ip 172.31.0.64 0.0.0.63 172.31.0.192 0.0.0.63
BUCARAMANGA(config)#access-list 101 permit ip 172.31.0.0 0.0.0.63 172.31.1.0 0.0.0.63
BUCARAMANGA(config)#access-list 103 permit udp host 0.0.0.0 eq bootpc host 255.255.255.255 eq bootps
BUCARAMANGA(config)#access-list 103 deny ip 172.31.0.64 0.0.0.63 172.31.0.0 0.0.255.255
BUCARAMANGA(config)#access-list 103 permit ip 172.31.0.64 0.0.0.63 any
BUCARAMANGA(config)#

BUCARAMANGA(config)#access-list 102 permit udp host 0.0.0.0 eq bootpc host 255.255.255.255 eq bootps
BUCARAMANGA(config)#access-list 102 permit ip 172.31.1.0 0.0.0.63 172.31.0.128 0.0.0.63
BUCARAMANGA(config)#access-list 102 permit ip 172.31.1.0 0.0.0.63 172.31.0.0 0.0.0.63
BUCARAMANGA(config)#access-list 101 permit udp host 0.0.0.0 eq bootpc host 255.255.255.255 eq bootps
BUCARAMANGA(config)#access-list 101 deny ip 172.31.1.64 0.0.0.63 172.31.0.0 0.0.255.255
BUCARAMANGA(config)#access-list 101 permit ip 172.31.1.64 0.0.0.63 any

TUNJA(config)#access-list 20 permit 172.31.0.0 0.0.31.255
TUNJA(config)#access-list 102 permit ip 172.31.0.128 0.0.0.63 172.31.0.0 0.0.0.63
TUNJA(config)#access-list 102 permit ip 172.31.0.128 0.0.0.63 172.31.1.0 0.0.0.63
TUNJA(config)#access-list 103 permit tcp 172.31.0.192 0.0.0.63 any eq www

TUNJA(config)#access-list 103 permit tcp 172.31.0.192 0.0.0.63 any eq ftp

TUNJA(config)#ip dhcp excluded-address 172.31.1.65 172.31.1.70
TUNJA(config)#ip dhcp excluded-address 172.31.1.1 172.31.1.5
TUNJA(config)#ip dhcp excluded-address 172.31.0.1 172.31.0.5
TUNJA(config)#ip dhcp excluded-address 172.31.0.65 172.31.0.70

- Puntos 2, 3 y 6
- NAT ROUTER TUNJA

TUNJA(config)#ip nat inside source static 172.31.2.26 209.17.220.10
TUNJA(config)#ip nat inside source list 20 interface g0/0 overload
TUNJA(config)#access-list 20 permit 172.31.0.0 0.0.31.255

SWITCH

Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S_CUN
S_CUN(config)#no ip domain-lookup
S_CUN(config)#enable password class
S_CUN(config)#line console 0
S_CUN(config-line)#password cisco
S_CUN(config-line)#login
S_CUN(config-line)#line vty 0 15
S_CUN(config-line)#password cisco
S_CUN(config-line)#login
S_CUN(config-line)#exit
S_CUN(config)#line console 0
S_CUN(config-line)#logging synchronous
S_CUN(config-line)#interface VLAN1
S_CUN(config-if)#ip address 172.31.2.8 255.255.255.248
Bad mask /29 for address 172.31.2.8
S_CUN(config-if)#ip default-gateway 172.31.2.1
S_CUN(config)#int range fa0/1-6
S_CUN(config-if-range)#exit
S_CUN(config)#interface VLAN1

```
S_CUN(config-if)#no shutdown
S_CUN(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up
S_CUN(config-if)#exit
S_CUN(config)#exit
S_CUN#
%SYS-5-CONFIG_I: Configured from console by console


Switch(config)#hostname S_TUNJA
S_TUNJA(config)#no ip domain-lookup
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)#exit
S_TUNJA(config)#line console 0
S_TUNJA(config-line)#logging synchronous
S_TUNJA(config-line)#int vlan1
S_TUNJA(config-if)#ip address 172.31.2.8 255.255.255.248
Bad mask /29 for address 172.31.2.8
S_TUNJA(config-if)#ip default-gateway 172.31.2.1
S_TUNJA(config)#int range fa0/1-6
S_TUNJA(config-if-range)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to down
%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to down
%LINK-5-CHANGED: Interface FastEthernet0/5, changed state to down
%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to down
S_TUNJA(config-if-range)#
%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed
state to up
%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed
state to up
S_TUNJA(config-if-range)#exit
S_TUNJA(config)#exit


Switch>en
```

```
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SWITCH_BUCARAMANGA
SWITCH_BUCARAMANGA(config)#no ip domain-lookup
SWITCH_BUCARAMANGA(config)#enable password class
SWITCH_BUCARAMANGA(config)#line console 0
SWITCH_BUCARAMANGA(config-line)#password cisco
SWITCH_BUCARAMANGA(config-line)#login
SWITCH_BUCARAMANGA(config-line)#line vty 0 15
SWITCH_BUCARAMANGA(config-line)#password cisco
SWITCH_BUCARAMANGA(config-line)#login
SWITCH_BUCARAMANGA(config-line)#exit
SWITCH_BUCARAMANGA(config)#vlan 1
SWITCH_BUCARAMANGA(config-vlan)#name REDVLAN1
SWITCH_BUCARAMANGA(config-vlan)#vlan 10
SWITCH_BUCARAMANGA(config-vlan)#name REDVLAN10
SWITCH_BUCARAMANGA(config-vlan)#vlan 30
SWITCH_BUCARAMANGA(config-vlan)#name REDVLAN30
SWITCH_BUCARAMANGA(config-vlan)#exit
SWITCH_BUCARAMANGA(config)#int fa0/2
SWITCH_BUCARAMANGA(config-if)#switchport acces vlan 10
SWITCH_BUCARAMANGA(config-if)#int fa0/3
SWITCH_BUCARAMANGA(config-if)#switchport acces vlan 30
SWITCH_BUCARAMANGA(config-if)#int fa0/1
SWITCH_BUCARAMANGA(config-if)#switchport mode trunk
SWITCH_BUCARAMANGA(config-if)#

SWITCH_BUCARAMANGA(config-line)#interface VLAN1
SWITCH_BUCARAMANGA(config-if)#ip address 172.31.2.0 255.255.255.248
Bad mask /29 for address 172.31.2.0
SWITCH_BUCARAMANGA(config-if)#ip default-gateway 172.31.2.1
SWITCH_BUCARAMANGA(config)#int range fa0/1-6
SWITCH_BUCARAMANGA(config-if-range)#shutdown

%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to administratively
down
%LINK-5-CHANGED: Interface FastEthernet0/5, changed state to administratively
down
%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to administratively
down
SWITCH_BUCARAMANGA(config-if-range)#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively
down
```

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to administratively down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to down
%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to administratively down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to down

SWITCH_BUCARAMANGA(config-if-range)#exit
SWITCH_BUCARAMANGA(config)#int VLAN1
SWITCH_BUCARAMANGA(config-if)#no shutdown
SWITCH_BUCARAMANGA(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up
SWITCH_BUCARAMANGA(config-if)#exit
SWITCH_BUCARAMANGA(config)#exit
SWITCH_BUCARAMANGA#

PUERTO TRONCAL

S_TUNJA(config)#int fa0/1
S_TUNJA(config-if)#switchport mode trunk

SWITCH_BUCARAMANGA(config)#int fa0/1
SWITCH_BUCARAMANGA(config-if)#switchport mode trunk

S_CUN(config)#int fa0/1
S_CUN(config-if)#switchport mode trunk

ACCESO AL PUERTO PARA LA PC

S_TUNJA(config-if)#switchport mode access
S_TUNJA(config-if)#switchport access VLAN 1

CONCLUSIONES

Ingeniar sistemas de comunicación y alternativas de solución a las problemáticas que se presentan en el desarrollo de las actividades económicas de las empresas y de forma global a la necesidad de comunicarnos, hace que exploremos e investiguemos tecnologías que local o remotamente mejoren la dinámica del mundo cambiante, en escenarios de establecer comunicación y transmisión de la información; protocolos, direccionamientos, estrategias aseguran la conexión pero sobre todo genera nuevos conocimientos que obliga a facilitar procesos en entornos prácticos, dinámicos pero seguros.

BIBLIOGRAFÍA

CISCO. (2017). 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. (2017). Configurar las Listas de Acceso IP. Recuperado de https://www.cisco.com/c/es_mx/support/docs/security/ios-firewall/23602-confaccesslists.html

CISCO. (2006). Uso de los comandos Ping Extendido y Traceroute Extendido. Recuperado de https://www.cisco.com/c/es_mx/support/docs/ip/routing-information-protocol-rip/13730-ext-ping-trace.html

CISCO. (2006). Configurar ACL de IP de uso general. Recuperado de https://www.cisco.com/c/es_mx/support/docs/ip/access-lists/26448-ACLsamples.html.

OBSERVATORIO TECNOLOGICO. (2012). Utilización de ACL en routers. Recuperado de http://recursostic.educacion.es/observatorio/web/es/component/content/article/1065-listas-de-control-de-acceso-acl?start=3