PRUEBA DE HABILIDADES PRÁCTICAS

SARAI DANIELA MUÑOZ MARIÑO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
INGENIERA DE SISTEMAS
BOGOTÁ, 2020

PRUEBA DE HABILIDADES PRÁCTICAS

SARAI DANIELA MUÑOZ MARIÑO

PROYECTO DE GRADO
PARA EL TITULO DE
INGENIERA DE SISTEMAS

TUTOR
JOSÉ CARDONA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
INGENIERA DE SISTEMAS
BOGOTÁ, 2020

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

Firma del presidente del Jurado

_____

Firma del jurado

_____

Firma del jurado

Bogotá, 20 de mayo de 2020

DEDICATORIA

A Dios primeramente por darme la oportunidad de vivir para lograr mis objetivos y darme fuerza en los momentos difíciles para continuar en este proceso.

A mi madre, por su amor incondicional, por sus palabras llenas de enseñanza y sabiduría, por ser mi compañía siempre, por cada momento que ha dedicado a guiarme y por sus exhortaciones.

Y a todas las personas que de una u otra manera, estuvieron presentes en este proceso.

AGRADECIMIENTOS

A mi madre por apoyar este sueño incondicional y darme fortaleza, aún cuando lo veía lejos de lograrlo.

A la UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA por darme la oportunidad de estudiar bajo esta modalidad, por ser de las mejores y estar dentro de las mejores en este ámbito.

A los tutores que hicieron parte de este proceso y que fueron fundamentales para lograr esta meta

TABLA DE CONTENIDO

INTRODUCCIÓN

Por medio de este trabajo se pretende dar a conocer la adquisición de conocimientos que se dieron con la realización del curso diplomado. Con el cual desarrollamos habilidades para el desarrollo, configuración y administración de redes.
Está compuesto por unos escenarios propuestos, modelados hacía la vida real, en escenarios que vemos en las empresas donde laboramos, en colegios, universidades, entre otros lugares cotidianos, para la finalización del diplomado de acuerdo con las instrucciones de una guía de aprendizaje.

Se desarrollará el proceso de configuraciones paso a paso, desde el modo privilegiado de dispositivos como routers, switches, para protocolos DHCP y NAT, protocolos de routing como RIPv2 y direccionamiento de IPv4 e IPv6, listas de acceso ACL.

Adicional, hoy en día es súper importante la implementación de la seguridad digital en los dispositivos que a diario se pueden manejar, así que también se soluciona de manera práctica, las configuraciones básicas para la seguridad de acceso a los diferentes elementos que componen una red o varias redes interconectadas.

Todo lo anterior se lleva a cabo con una herramienta de simulación, en este caso se hizo bajo Packet Tracer, con el cual se demuestra la aplicabilidad de lo aquí plasmado, que reúne toda la información de una manera conectada a lo resuelto en los dos escenarios propuestos, con el objetivo de una demostración netamente gráfica y una experimentación con diferentes topologías.

OBJETIVOS

GENERAL

Realizar la construcción de redes, implementando las diferentes tecnologías existentes en Packet Tracer como simulador, para la configuración y administración respectiva de estas.

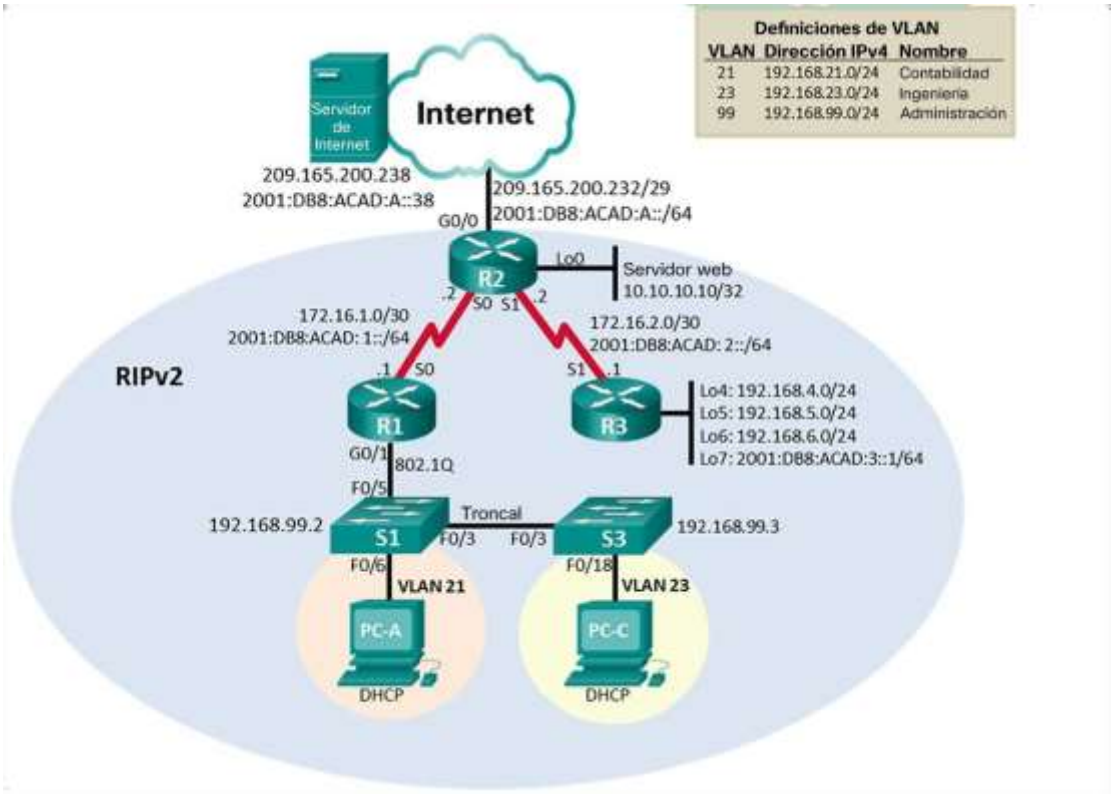
ESPECÍFICOS

- Desarrollar las capacidades obtenidas a través del desarrollo de los escenarios planteados
- Adquirir nuevas competencias por medio del mejoramiento en el proceso de configuración y administración de redes.

ESCENARIO 1

Se debe configurar una red pequeña para que admita conectividad IPv4 e IPv6, seguridad de switches, routing entre VLAN, el protocolo de routing dinámico RIPv2, el protocolo de configuración de hosts dinámicos (DHCP), la traducción de direcciones de red dinámicas y estáticas (NAT), listas de control de acceso (ACL) y el protocolo de tiempo de red (NTP) servidor/cliente. Durante la evaluación, probará y registrará la red mediante los comandos comunes de CLI.

TOPOLOGÍA



PARTE 1: INICIALIZAR DISPOSITIVOS

PASO 1: Inicializar y volver a cargar los routers y los switches.

- Eliminar el archivo startup-config de todos los routers

Se entra al modo privilegiado (EXEC) del router y se ejecuta el comando #erase startup-config.
Aparecerá el siguiente mensaje:

Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]

Se confirma con tecla “Enter” y se borran todos los datos de la memoria NVRAM

Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram

Esto se realiza para cada router y cada switch. Y por último se vuelven a cargar los routers, sin ninguna configuración anterior con el comando *#reload,* con el cual luego aparecerá toda la información del dispositivo

- Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior.

Se entra al modo privilegiado (EXEC) del switch y se ejecuta el comando *#erase startup-config.*
Aparecerá el siguiente mensaje:

Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]

Se confirma con tecla “Enter” y se borran todos los datos de la memoria NVRAM. Aparece el siguiente mensaje de confirmación:

Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram

Y esto se realiza para cada router y cada switch.

- Se elimina una base de datos VLAN con el comando *#delete vlan.dat*, en éste caso no existe ninguna por lo que el mensaje será el siguiente para ambos dispositivos:

Delete filename [vlan.dat]? Delete flash:/vlan.dat? [confirm]
%Error deleting flash:/vlan.dat (No such file or directory)

- Se vuelven a cargar los switches, sin ninguna configuración anterior con el comando *#reload,* con el cual luego aparecerá toda la información del dispositivo.

- Y, por último, se valida que no haya archivos de VLAN en el directorio de la memoria flash con #dir flash

Directory of flash:/ No files in directory
64016384 bytes total (64016384 bytes free)

PARTE 2: CONFIGURAR LOS PARÁMETROS BÁSICOS

PASO 1: Configurar la computadora de Internet.

Las tareas de configuración del servidor de Internet incluyen lo siguiente (para obtener información de las direcciones IP, consulte la topología)

Tabla 1. Direccionamiento Servidor de Internet

Elemento o tarea de configuración	**Especificación**
Dirección IPv4	209.165.200.238
Máscara de subred para IPv4	255.255.255.248
Gateway predeterminado	209.165.200.234
Dirección IPv6/subred	2001:DB8:ACAD:A::38/64
Gateway predeterminado IPv6	2001:DB8:ACAD:2::1

PASO 2: Configurar R1

- Se desactiva la búsqueda DNS, con los siguientes comandos:

Router>en
Router#conf t
Router(config)#no ip domain-lookup

- Se nombra el router *#hostname R1* y en automático se ve el cambio:

R1(config)

- Los siguientes comandos son para: configurar contraseñas para los diferentes accesos del router, encriptar las contraseñas no cifradas y enviar un mensaje de advertencia

R1(config)#enable secret class
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config- line)#line vty 0 4
R1(config- line)#password cisco
R1(config- line)#login

R1(config-line)#service password-encryption
R1(config)#bann motd "Se prohibe el acceso no autorizado"

- Configuración de interfaz s0/0/0

Se establece descripción, se cambia frecuenta del reloj, se configuran las direcciones del dispositivo y las rutas estáticas predeterminadas.

R1(config)#int s0/0/0
R1(config-if)#description R1-s0/0/0 a R2
R1(config-if)#clock rate 128000
This command applies only to DCE interfaces
R1(config-if)#ip address 172.16.1.1 255.255.255.252
R1(config-if)#ipv6 unicast-routing
R1(config)#int s0/0/0
R1(config-if)#ipv6 address 2001:DB8:ACAD:A:1::1/64
R1(config-if)#no sh
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
R1(config-if)#exit
R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0
R1(config)#ipv6 route ::/0 s0/0/0

Se establecieron estas rutas estáticas ya que no nos están dando un inicio de red para realizar los saltos.

PASO 3: Configurar R2

- Se desactiva la búsqueda DNS, con los siguientes comandos:

Router>en
Router#conf t
Router(config)#no ip domain-lookup

- Se nombra el router *#hostname R2* y en automático se ve el cambio:

R2(config)

- Los siguientes comandos son para: configurar contraseñas para los diferentes accesos del router, encriptar las contraseñas no cifradas y enviar un mensaje de advertencia

R1(config)#enable secret class
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config- line)#line vty 0 4
R1(config- line)#password cisco

R1(config- line)#login
R1(config-line)#service password-encryption
R1(config)#bann motd "Se prohibe el acceso no autorizado"

- Se configura la interfaz s0/0/0

Se establece descripción y se configuran las direcciones del dispositivo

R2(config)#ipv6 unicast-routing
R2(config)#int s0/0/0
R2(config-if)#description R2-s0/0/0 a R1
R2(config-if)#ip address 172.16.1.2 255.255.255.252
R2(config-if)#ipv6 address 2001:DB8:ACAD:1::2/64
R2(config-if)#no sh

- Se configura la interfaz s0/0/1

Se establece descripción, se configuran las direcciones del dispositivo y frecuencia del reloj.

R2(config)#int s0/0/1
R2(config-if)#description R2-s0/0/1 a R3
R2(config-if)#clock rate 128000
R2(config-if)#ip address 172.16.2.2 255.255.255.252
R2(config-if)#ipv6 address 2001:DB8:ACAD:2::2/64
R2(config-if)#no sh

- Se configura la interfaz g0/0

Se establece descripción y se configuran las direcciones del dispositivo.

R2(config)#int g0/0
R2(config-if)#description R2-g0/0 a Server
R2(config-if)#ip address 209.165.200.234 255.255.255.248
R2(config-if)#ipv6 address 2001:DB8:ACAD:A::45/64
R2(config-if)#no sh

- Se configuran las rutas estáticas

R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0
R2(config)#ipv6 route ::/0 g0/0

Se establecieron estas rutas estáticas ya que no nos están dando un inicio de red para realizar los saltos.

PASO 4: Configurar R3

- Se desactiva la búsqueda DNS, con los siguientes comandos:

Router>en
Router#conf t
Router(config)#no ip domain-lookup

- Los siguientes comandos son para: configurar contraseñas para los diferentes accesos del router, encriptar las contraseñas no cifradas y enviar un mensaje de advertencia.

R3(config)#enable secret class
R3(config)#line console 0
R3(config-line)#password cisco
R3(config-line)#login
R3(config- line)#line vty 0 4
R3(config- line)#password cisco
R3(config- line)#login
R3(config-line)#service password-encryption
R3(config)#bann motd "Se prohibe el acceso no autorizado"

- Se configura la interfaz s0/0/1

Se establece descripción, se configuran las direcciones del dispositivo y frecuencia del reloj.

R3(config)#ipv6 unicast-routing
R3(config)#int s0/0/1
R3(config-if)#description R3-s0/0/1 a R2
R3(config-if)#ip address 172.16.2.1 255.255.255.252
R3(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64
R3(config-if)#no sh

- Se configuran las interfaces loopback 4-7

R3(config-if)#int loopback 4
%LINK-5-CHANGED: Interface Loopback4, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback4, changed state to up
R3(config-if)#ip address 192.168.4.1 255.255.255.0
R3(config-if)#int loopback 5
%LINK-5-CHANGED: Interface Loopback5, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback5, changed state to up
R3(config-if)#ip address 192.168.5.1 255.255.255.0
R3(config-if)#int loopback 6
%LINK-5-CHANGED: Interface Loopback6, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback6, changed state to up
R3(config-if)#ip address 192.168.6.1 255.255.255.0
R3(config-if)#int loopback 7
%LINK-5-CHANGED: Interface Loopback7, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback7, changed state to up
R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64

- Se configuran las rutas estáticas

R3(config)# ip route 0.0.0.0 0.0.0.0 s0/0/1
R3(config)#ipv6 route ::/0 s0/0/1

PASO 5: Configurar S1

- Se configuran contraseñas para los diferentes accesos del router, encriptar las contraseñas no cifradas y enviar un mensaje de advertencia en el modo privilegiado del switch

Switch(config)#no ip domain-lookup
Switch(config)#hostname S1
S1(config)#enable secret class
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#line vty 0 4
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#service password-encryption
S1(config)#bann motd "Se prohibe el acceso no autorizado"

PASO 6: Configurar S3

- Se configuran contraseñas para los diferentes accesos del router, encriptar las contraseñas no cifradas y enviar un mensaje de advertencia en el modo privilegiado del switch.

Switch(config)#no ip domain-lookup
Switch(config)#hostname S3
S3(config)#enable secret class
S3(config)#line console 0
S3(config-line)#password cisco
S3(config-line)#login

S3(config-line)#line vty 0 4
S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#service password-encryption
S3(config)#bann motd "Se prohibe el acceso no autorizado"

PASO 7: Verificar la conectividad de la red

Utilice el comando **ping** para probar la conectividad entre los dispositivos de la red

Desde	**A**	**Dirección IP**	**Resultados de ping**
R1	R2, S0/0/0	172.16.1.2	Sucess
R2	R3, S0/0/1	172.16.2.1	Sucess
PC de Internet	Gateway predeterminado	209.165.200.234	Sucess

```
R1>ping 172.16.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/7 ms
```

Figura 2. Ping R1 – R2, s0/0/0

```
R2>ping 172.16.2.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/14 ms
```

Figura 3. Ping R2 – R3, s0/0/1

```
Pinging 209.165.200.234 with 32 bytes of data:

Reply from 209.165.200.234: bytes=32 time=1ms TTL=255
Reply from 209.165.200.234: bytes=32 time<1ms TTL=255
Reply from 209.165.200.234: bytes=32 time<1ms TTL=255
Reply from 209.165.200.234: bytes=32 time<1ms TTL=255

Ping statistics for 209.165.200.234:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Figura 4. Ping Server – Gateway

PARTE 3: CONFIGURAR LA SEGURIDAD DEL SWITCH, VLAN Y EL ROUTING ENTRE VLAN

PASO 1: Configurar S1

- Se crea la base de datos VLAN de acuerdo con la topología.

S1(config)#vlan 21
S1(config-vlan)#name Contabilidad
S1(config-vlan)#vlan 23
S1(config-vlan)#name Ingenieria
S1(config-vlan)#vlan 99
S1(config-vlan)#name Administración

- Se asigna la dirección IP a la VLAN de administración y gateway por default.

S1(config-if)#ip address 192.168.99.2 255.255.255.0
S1(config-if)#ex
S1(config)#ip default-gateway 192.168.99.1

- Se fuerzan los troncales en interfaz f0/3-5

S1(config)#int f0/3
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 1
S1(config-if)#ex
S1(config)#int f0/5
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 1
S1(config-if)#ex

- Se configuran los demás puertos como acceso.

S1(config)#int range fa0/1-2, fa0/4, fa0/6-24, g0/1-2
S1(config-if-range)#switchport mode access

- Se asigna VLAN 21 a interfaz f0/6.

S1(config-if-range)#int f0/6
S1(config-if)#switchport access vlan 21

- Por último, se apagan las interfaces sin funcionamiento administrativamente.

S1(config-if)#int range fa0/1-2, fa0/4, fa0/7-24, g0/1-2

S1(config-if-range)#sh

PASO 2: Configurar S3

- Se crea la base de datos VLAN de acuerdo con la topología.

S3(config)#vlan 21
S3(config-vlan)#name Contabilidad
S3(config-vlan)#vlan 23
S3(config-vlan)#name Ingenieria
S3(config-vlan)#vlan 99
S3(config-vlan)#name Administracion
S3(config-vlan)#ex
S3(config)#int vlan 99

- Se asigna dirección IP a la VLAN de administración y gateway por default.

S3(config)#int vlan 99
S3(config-if)#ip address 192.168.99.3 255.255.255.0
S3(config-if)#ex
S1(config)#ip default-gateway 192.168.99.1

- Se fuerzan los troncales en interfaz f0/3-5.

S3(config)#int f0/3
S3(config-if)#switchport mode trunk
S3(config-if)#switchport trunk native vlan 1

- Se configuran los demás puertos como acceso.

S3(config-if)#int range fa0/1-2, fa0/4-24, g0/1-2
S3(config-if-range)#switchport mode access

- Se asigna VLAN 21 a interfaz f0/18.

S3(config-if-range)#int fa0/18
S3(config-if)#switchport access vlan 21

- Por último, se apagan las interfaces sin funcionamiento administrativamente.

S3(config-if)#int range fa0/1-2, fa0/4-17, fa0/19-24, g0/1-2
S3(config-if-range)#sh

PASO 3: Configurar R1

- Se configuran subinterfaces g0/1.21, 23, 99 y se activa la interfaz g0/0.

R1(config)#int g0/1.21
R1(config-subif)#description LAN de Contabilidad
R1(config-subif)#encapsulation dot1q 21
R1(config-subif)#ip address 192.168.21.1 255.255.255.0
R1(config-subif)#int g0/1.23
R1(config-subif)#description LAN de Ingenieria
R1(config-subif)#encapsulation dot1q 23
R1(config-subif)#ip address 192.168.23.1 255.255.255.0
R1(config-subif)#int g0/1.99
R1(config-subif)#description LAN de Administracion
R1(config-subif)#encapsulation dot1q 99
R1(config-subif)#ip address 192.168.99.4 255.255.255.0
R1(config-subif)#int g0/1
R1(config-if)#no sh

PASO 4: Verificar la conectividad de la red.

Desde	**A**	**Dirección IP**	**Resultados de ping**
S1	R1, dirección VLAN 99	192.168.99.1	Success
S3	R1, dirección VLAN 99	192.168.99.1	Success
S1	R1, dirección VLAN 21	192.168.21.1	Success
S3	R1, dirección VLAN 23	192.168.23.1	Success

Figura 5. Ping S1 – R1, VLAN99

```
S1>ping 192.168.99.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
```

Figura 6. Ping S3 – R1, VLAN99

```
S3>ping 192.168.99.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/4/17 ms
```

```
S1>ping 192.168.21.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.21.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
```

Figura 7. Ping S1 – R1, VLAN21

```
S3>ping 192.168.23.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.23.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/2/3 ms
```

Figura 8. Ping S3 – R1, VLAN21

PARTE 4: CONFIGURAR EL PROTOCOLO DE ROUTING DINÁMICO RIPV2

PASO 1: Configurar RIPv2 en el R1

- Se configura RIP versión 2, se añaden todas las direcciones directamente conectadas, se establecen como pasivas las subinterfaces de VLAN y se desactiva la sumarización automática.

```
R1(config)#router rip
R1(config-router)#version 2
R1(config-router)#network 172.16.1.0
R1(config-router)#network 192.168.21.0
R1(config-router)#network 192.168.23.0
R1(config-router)#network 192.168.99.0
R1(config-router)#passive-interface g0/1.21
R1(config-router)#passive-interface g0/1.23
R1(config-router)#passive-interface g0/1.99
R1(config-router)#no auto-summary
```

PASO 2: Configurar RIPv2 en el R2

```
R2(config)#router rip
R2(config-router)#version 2
R2(config-router)#network 10.10.10.10
R2(config-router)#network 172.16.1.0
R2(config-router)#network 172.16.2.0
R2(config-router)#passive-interface loopback 0
R2(config-router)#no auto-summary
```

PASO 3: Configurar RIPv2 en el R3

R3(config)#router rip
R3(config-router)#version 2
R3(config-router)#network 172.16.2.0
R3(config-router)#network 192.168.4.0
R3(config-router)#network 192.168.5.0
R3(config-router)#network 192.168.6.0
R3(config-router)#passive-interface loopback 4
R3(config-router)#passive-interface loopback 5
R3(config-router)#passive-interface loopback 6
R3(config-router)#no auto-summary

PASO 4: Verificar la información de RIP

Pregunta	**Respuesta**
¿Con qué comando se muestran la ID del proceso RIP, la ID del router, las redes de routing y las interfaces pasivas configuradas en un router?	*#show ip protocols*
¿Qué comando muestra solo las rutas RIP?	*#show ip route rip*
¿Qué comando muestra la sección de RIP de la configuración en ejecución?	*#show run*

PARTE 5: IMPLEMENTAR DHCP Y NAT IPV4

PASO 1: Configurar R1 como servidor DHCP para las VLAN 21-23

- Se reservan los primeros 20 hosts para VLAN 21/23 respectivamente y se crean los pool para cada VLAN.

R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20
R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20
R1(config)#ip dhcp pool ACCT
R1(dhcp-config)#network 192.168.21.0 255.255.255.0
R1(dhcp-config)#default-router 192.168.21.1
R1(dhcp-config)#dns-server 10.10.10.10
R1(dhcp-config)#ip domain-name ccna-sa.com
R1(config)#ip dhcp pool ENGNR
R1(dhcp-config)#network 192.168.23.0 255.255.255.0
R1(dhcp-config)#default-router 192.168.23.1
R1(dhcp-config)#dns-server 10.10.10.10

R1(dhcp-config)#ip domain-name ccna-sa.com

PASO 2: Configurar la NAT estática y dinámica para R2

- Se ejecutan los comandos para crear una base de datos local y las configuraciones de la NAT estática.

R2(config)#username webuser privilege 15 secret cisco12345
R2(config)#ip nat inside source static 10.10.10.10 209.165.200.237
R2(config)#int g0/0
R2(config-if)#ip nat outside
R2(config-if)#int s0/0/0
R2(config-if)#ip nat inside
R2(config-if)#int s0/0/1
R2(config-if)#ip nat inside
R2(config-if)#ex
R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255
R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255
R2(config)#access-list 1 permit 192.168.4.0 0.0.3.255
R2(config)#no ip nat pool INTERNET 209.165.200.233 209.165.200.236 netmask 255.255.255.252
R2(config)#ip nat inside source list 1 pool INTERNET

PASO 3: Verificar el protocolo DHCP y la NAT estática

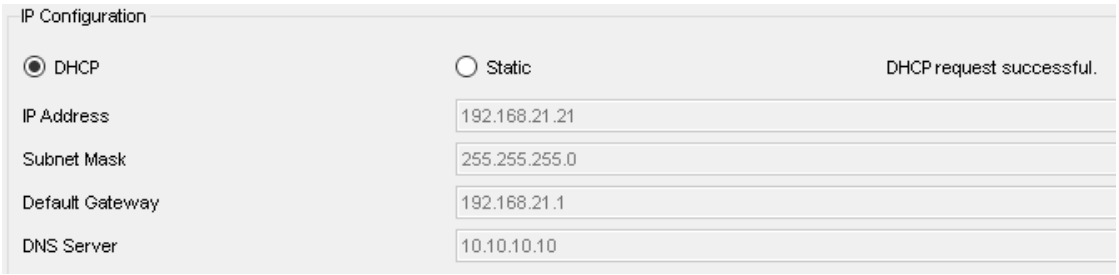


Figura 9. DHCP PC-A

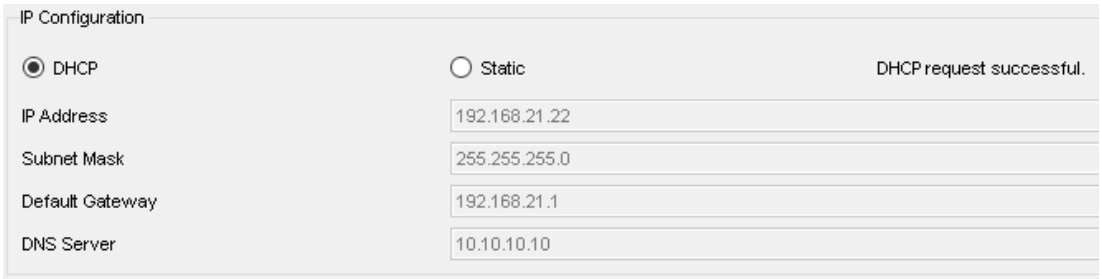


Figura 9. DHCP PC-C

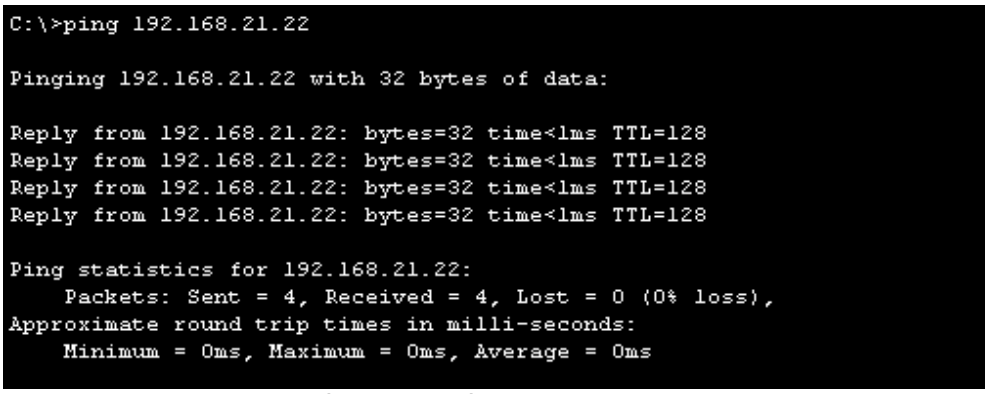


Figura 10. Ping PC-A a PC-C

No es possible conectar el web browser al servidor, puesto packet tracer no soporta comandos para http en routers.

PARTE 6: CONFIGURAR NTP

- Se ajusta reloj, se configuran maestros NTP, se verifica la conexión.

R2#clock set 09:00:00 22 May 2020
R2#ntp master 5
R1(config)#ntp server 172.16.1.2
R1(config)#ntp update-calendar
R1#show ntp associations
address ref clock st when poll reach delay offset disp
~172.16.1.2 .INIT. 16 - 64 0 0.00 0.00 0.12
** sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured*

PARTE 7: CONFIGURAR Y VERIFICAR LAS LISTAS DE CONTROL (ACL)

PASO 1: Restringir el acceso a las líneas vty en R2

- Se configura lista de acceso, se aplica a las línea vty y se permite acceso único.

R2(config)#ip access-list standard ADMIN-MGT
R2(config-std-nacl)#permit host 172.16.1.1
R2(config-std-nacl)#ex
R2(config)#line vty 0 4
R2(config-line)#access-class ADMIN-MGT in
R2(config-line)#transport input telnet

- Se verifica su funcionalidad

R1#telnet 172.16.1.2

Trying 172.16.1.2 ...OpenSe prohibe el acceso no autorizado

PASO 2: Introducir comando de CLI adecuado que se necesita para mostrar lo siguiente.

- Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció.

R2#show access-list Standard IP access list 1
10 permit 192.168.21.0 0.0.0.255
20 permit 192.168.23.0 0.0.0.255
30 permit 192.168.4.0 0.0.3.255
Standard IP access list ADMIN-MGT
10 permit host 172.16.1.1 (2 match(es))

- Restablecer los contadores de una lista de acceso.

R2#clear ip access-list counters

- ¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?

R2#show ip interface buscar sh run

- ¿Con qué comando se muestran las traducciones NAT?

R2# show ip nat translations

- ¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?

R2#clear ip nat translation
R2#show ip nat translations

ESCENARIO 2

Una empresa posee sucursales distribuidas en las ciudades de Bogotá y Medellín, 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

DESARROLLO – CONFIGURACIONES BÁSICAS

- Se configuran todos los routers con la siguiente información, cambiando nombres según corresponda en la topología.

Router>enable Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname ISP
ISP(config)#enable secret class
ISP(config)#line console 0
ISP(config-line)#password cisco
ISP(config-line)#login
ISP(config-line)#line vty 0 4
ISP(config-line)#password cisco
ISP(config-line)#login
ISP(config-line)#service password-encryption
ISP(config)#banner motd "Se prohibe el acceso no autorizado"

- Se realiza conexión física de acuerdo con la topología (se anexa evidencia)

PARTE 1: CONFIGURACIÓN DE ENRUTAMIENTO

PASO 1: Configurar el enrutamiento en la red usando el protocolo OSPF versión 2, declare la red principal, desactive la sumarización automática.

Medellin-1(config)#router ospf 1
Medellin-1(config-router)#router-id 1.1.1.1
Medellin-1(config-router)#network 172.29.6.0 0.0.0.3 area 0
Medellin-1(config-router)#network 209.17.220.0 0.0.0.3 area 0
Medellin-1(config-router)#no auto-summary
Medellin-1(config-router)#exit

Esta configuración es la misma para cada uno de los dispositivos cambiando las redes principales e interfaces, según corresponda.

PASO 2: Los routers Bogota1 y Medellín1 deberán añadir a su configuración de enrutamiento una ruta por defecto hacia el ISP y, a su vez, redistribuirla dentro de las publicaciones de OSPF.

- Configuración Bogota-1.

Bogota-1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.5
Bogota-1(config)#router ospf 1
Bogota-1(config-router)#default-information originate
Bogota-1(config-router)#exit

- Configuración Medellín-1.

Medellin-1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.2
Medellin-1(config)#router ospf 1
Medellin-1(config-router)#default-information originate
Medellin-1(config-router)#exit

PASO 3: El router ISP deberá tener una ruta estática dirigida hacia cada red interna de Bogotá y Medellín para el caso se sumarizan las subredes de cada uno a 22.

ISP(config)#ip route 172.29.4.0 255.255.252.0 209.17.220.1
ISP(config)#ip route 172.29.0.0 255.255.252.0 209.17.220.6

PARTE 2: TABLA DE ENRUTAMIENTO.

PASO 1: Verificar la tabla de enrutamiento en cada uno de los routers para comprobar las redes y sus rutas.

Medellin-1#show ip route

Gateway of last resort is 209.17.220.2 to network 0.0.0.0 172.29.0.0/16 is variably subnetted, 9 subnets, 3 masks
O 172.29.4.0/25 [110/65] via 172.29.6.2, 00:04:44, Serial0/0/1
O 172.29.4.128/25 [110/65] via 172.29.6.10, 00:08:14, Serial0/0/0
C 172.29.6.0/30 is directly connected, Serial0/0/1 L 172.29.6.1/32 is directly connected, Serial0/0/1
O 172.29.6.4/30 [110/128] via 172.29.6.10, 00:04:44, Serial0/0/0 [110/128] via 172.29.6.2, 00:04:44, Serial0/0/1
C 172.29.6.8/30 is directly connected, Serial0/0/0 L 172.29.6.9/32 is directly connected, Serial0/0/0 C 172.29.6.12/30 is directly connected, Serial0/1/0 L 172.29.6.13/32 is directly connected, Serial0/1/0
209.17.220.0/24 is variably subnetted, 3 subnets, 2 masks C 209.17.220.0/30 is directly connected, Serial0/1/1
L 209.17.220.1/32 is directly connected, Serial0/1/1 C 209.17.220.2/32 is directly connected, Serial0/1/1 S 0.0.0.0/0 [1/0] via 209.17.220.2*

Este comando se ejecuta en cada uno de los dispositivos y la vista es la misma, detallando cada una de las redes y su fomar de conexión.

PARTE 3: DESHABILITAR LA PROPAGACIÓN DEL PROTOCOLO OSPF.

PASO 1: Para no propagar las publicaciones por interfaces que no lo requieran se debe deshabilitar la propagación del protocolo OSPF.

- Configuración Medellin-1.

Medellin-1(config)#router ospf 1
Medellin-1(config-router)#passive-interface s0/1/0
00:01:20: %OSPF-5-ADJCHG: Process 1, Nbr 3.3.3.3 on Serial0/0/0 from LOADING to FULL, Loading Done
Medellin-1(config-router)#

- Configuración Medellin-2.

Medellin-2(config)#router ospf 1
Medellin-2(config-router)#passive-interface g0/0
Medellin-2(config-router)#exit

- Configuración Medellin-3.

Medellin-3(config)#router ospf 1
Medellin-3(config-router)#passive-interface g0/0
Medellin-3(config-router)#exit

- Configuración Bogota-1

Bogota-1(config)#router ospf
Bogota-1(config-router)#passive-interface s0/1/1
Bogota-1(config-router)#exit

- Configuración Bogota-2

Bogota-2(config)#router ospf 1
Bogota-2(config-router)#passive-interface s0/1/0
Bogota-2(config-router)#passive-interface g0/0
Bogota-2(config-router)#exit

- Configuración Bogota-3

Bogota-3(config)#router ospf 1
Bogota-3(config-router)#passive-interface g0/0
Bogota-3(config-router)#exit

PARTE 4: VERIFICACIÓN DEL PROTOCOLO OSPF

Medellin-1#show ip protocols
Maximum path: 4
Routing for Networks:
172.29.6.0 0.0.0.3 area 0
172.29.6.8 0.0.0.3 area 0
172.29.6.12 0.0.0.3 area 0
209.17.220.0 0.0.0.3 area 0 Passive Interface(s): Serial0/1/0
Routing Information Sources: Gateway Distance Last Update
110 00:20:21
110 00:23:44
3.3.3.3 110 00:20:21
7.7.7.7 110 00:23:47
Distance: (default is 110)

PARTE 5: CONFIGURAR EL ENCAPSULAMIENTO Y AUTENTICACIÓN PPP.

PASO 1: Según la topología se requiere que el enlace Medellín1 con ISP sea configurado con autenticación PAP.

Medellin-1(config)#interface Serial0/1/1
Medellin-1(config-if)#encapsulation ppp
Medellin-1(config-if)#no shutdown
Medellin-1(config-if)#exit

Medellin-1(config)#username ISP secret cisco
Medellin-1(config)#int s0/1/1
Medellin-1(config-if)#ppp authentication pap
Medellin-1(config-if)#ppp pap sent-username MEDELLIN password cisco
Medellin-1(config-if)#exit

PASO 2: El enlace Bogotá1 con ISP se debe configurar con autenticación CHAP.

Bogota-1(config)#interface Serial0/0/0
Bogota-1(config-if)#encapsulation ppp
Bogota-1(config-if)#no shutdown
Bogota-1(config-if)#exit
Bogota-1(config)#
Bogota-1(config)#username ISP secret cisco
Bogota-1(config)#int s0/0/0
Bogota-1(config-if)#ppp authentication chap
Bogota-1(config-if)#exit

PARTE 6: CONFIGURAR TRADUCCIÓN DE DIRECCIONES

PASO 1: Compruebe que la traducción de direcciones indique las interfaces de entrada y de salida. Al realizar una prueba de ping, la dirección debe ser traducida automáticamente a la dirección de la interfaz serial 0/1/0 (s0/1/1) del router Medellín1, cómo diferente puerto.

Medellin-1(config)#ip access-list standard HOST
Medellin-1(config-std-nacl)#permit 172.29.4.0 0.0.0.127
Medellin-1(config-std-nacl)#exit
Medellin-1(config)#ip nat inside source list HOST interface s0/1/1 overload
Medellin-1(config)#int s0/0/0
Medellin-1(config-if)#ip nat inside
Medellin-1(config-if)#exit
Medellin-1(config)#int s0/0/1
Medellin-1(config-if)#ip nat inside
Medellin-1(config-if)#exit
Medellin-1(config)#int s0/1/0
Medellin-1(config-if)#ip nat inside
Medellin-1(config-if)#exit
Medellin-1(config)#int s0/1/1
Medellin-1(config-if)#ip nat outside
Medellin-1(config-if)#exit
Medellin-1(config)#exit

PASO 2: Proceda a configurar el NAT en el router Bogotá1. Compruebe que la traducción de direcciones indique las interfaces de entrada y de salida. Al realizar

una prueba de ping, la dirección debe ser traducida automáticamente a la dirección de la interfaz serial 0/1/0 del router Bogotá1, cómo diferente puerto.

Bogota-1(config)#ip access-list standard HOST
Bogota-1(config-std-nacl)#permit 172.29.0.0 0.0.0.255
Bogota-1(config-std-nacl)#exit
Bogota-1(config)#ip nat inside source list HOST interface s0/0/0 overload
Bogota-1(config)#int s0/0/0
Bogota-1(config-if)#ip nat outside
Bogota-1(config-if)#exit
Bogota-1(config)#int s0/0/1
Bogota-1(config-if)#ip nat inside
Bogota-1(config-if)#exit
Bogota-1(config)#int s0/1/0
Bogota-1(config-if)#ip nat inside
Bogota-1(config-if)#exit
Bogota-1(config)#int s0/1/1
Bogota-1(config-if)#ip nat inside
Bogota-1(config-if)#exit

PARTE 7: CONFIGURACIÓN DEL SERVICIO DHCP

PASO 1: Configurar la red Medellín2 y Medellín3 donde el router Medellín2 debe ser el servidor DHCP para ambas redes LAN.

Medellin-2(config)#ip dhcp excluded-address 172.29.4.1
Medellin-2(config)#ip dhcp pool MEDELLIN-2
Medellin-2(dhcp-config)#network 172.29.4.0 255.255.255.128
Medellin-2(dhcp-config)#default-router 172.29.4.1
Medellin-2(dhcp-config)#dns-server 8.8.8.8
Medellin-2(dhcp-config)#exit
Medellin-2(config)#ip dhcp excluded-address 172.29.4.29
Medellin-2(config)#ip dhcp pool MEDELLIN-3
Medellin-2(dhcp-config)#network 172.29.4.128 255.255.255.128
Medellin-2(dhcp-config)#default-router 172.29.4.129
Medellin-2(dhcp-config)#dns-server 8.8.8.8 Medellin-2(dhcp-config)#exit
Medellin-3(config)#int g0/0
Medellin-3(config-if)#ip helper-address 172.29.6.5 Medellin-3(config-if)#exit
Medellin-3(config)#

PASO 2: Configurar la red Bogotá2 y Bogotá3 donde el router Bogota2 debe ser el servidor DHCP para ambas redes LAN.

Bogota-2(dhcp-config)#ip dhcp excluded-address 172.29.0.1
Bogota-2(config)#ip dhcp pool BOGOTA2

Bogota-2(dhcp-config)#network 172.29.0.0 255.255.255.0
Bogota-2(dhcp-config)#default-router 172.29.0.1
Bogota-2(dhcp-config)#dns-server 8.8.8.8
Bogota-2(dhcp-config)#exit
Bogota-2(config)#ip dhcp excluded-address 172.29.1.1
Bogota-2(config)#ip dhcp pool BOGOTA3
Bogota-2(dhcp-config)#network 172.29.1.0 255.255.255.0
Bogota-2(dhcp-config)#default-router 172.29.1.1
Bogota-2(dhcp-config)#dns-server 8.8.8.8
Bogota-2(dhcp-config)#exit
Bogota-2(config)#

PASO 3: Configure el router Bogotá3 para que habilite el paso de los mensajes Broadcast hacia la IP del router Bogotá2.

Bogota-3(config)#int g0/0
Bogota-3(config-if)#ip helper-address 172.29.3.13
Bogota-3(config-if)#exit

CONCLUSIONES

ESCENARIO 1

En este escenario se plasmaba una red LAN, así que primeramente se realizo un calculo de subredes con lo dado en la topología.
Se eliminan correctamente todas las configuraciones que pudiesen tener los dispositivos, se habilitan contraseñas de acceso en modo de privilegio, se configuran de acuerdo con el cálculo de redes cada una de las interfaces, se crean bases de datos VLAN y sus diferentes modos de accesos respecto a las interfaces. Se demuestra con los pings que la conectividad y configuración de la red se hizo efectiva, aunque el simulador no soportaba algunos comandos

ESCENARIO 2

Se realizaron las configuraciones básicas en los diferentes dispositivos propuestos, como seguridad de contraseñas para ingreso y encriptación de estas.
Se configura el protocolo OSPF para el routing dinámico añadiendo las redes respectivas, y a su vez se deshabilita la propagación para evitar tener activas varias IP's públicas dentro de la red. Por último, se habilitan protocolos PAP/CHAP/NAT y DHCP.

GENERALES

- Se logra adquirir habilidades para la configuración básica de accesos, cálculo de subredes a través de alguna herramienta, seguridad en dispositivos y en enrutamiento a las diferentes interfaces que hacen parte de la red, aplicando los distintos protocolos que pueden ser utilizados.

- Se estudio más detalladamente el routing dinámico por protocolo OSPF, RIPv2 y DHCP (respecto a la obtención de las IP's) con el direccionamiento de las identificaciones y descripciones en los dispositivos.

- Se configuran diferentes rutas de acceso por medio de ACL, como una mitigación para evitar ataques de forma remota que se pudiesen dar en la seguridad de la red. Se adquieren nuevos conocimientos sobre éste tipo de protocolo o herramienta.

BIBLIOGRAFÍA

Castillo, A. (n.d) Calculadora IP - Subneteo Online - Redes. Recuperado de: https://www.calculadora-redes.com/

CISCO. (2017). Traducción de direcciones IP para IPv4. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module11/index.html#11.0.1.1

CISCO. (2017). VLANs. Principios de Enrutamiento y Conmutación. Recuperado de https://static-courseassets.s3.amazonaws.com/RSE50ES/module3/index.html#3.0.1.1

Varios (n.d) Blog Cisco Latinoamérica. CISCO. Recuperado de: https://gblogs.cisco.com/la/