SOLUCIÓN DE DOS ESCENARIOS PRESENTES EN ENTORNOS CORPORATIVOS BAJO USO DE TECNOLOGÍA CISCO

LUIS GABRIEL ALBERTO CONTRERAS VILLAMIZAR

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERIA DE SISTEMAS
GIRARDOT
2021

SOLUCIÓN DE DOS ESCENARIOS PRESENTES EN ENTORNOS CORPORATIVOS BAJO USO DE TECNOLOGÍA CISCO

LUIS GABRIEL ALBERTO CONTRERAS VILLAMIZAR

Diplomado de opción de grado presentado para optar el título de
INGENIERO DE SISTEMAS

DIRECTORA

MG NANCY AMPARO GUACA GIRÓN

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA – ECBTI
INGENIERIA DE SISTEMAS
GIRARDOT
2021

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

_____

_____

_____

Firma del presidente del jurado

Firma del jurado

Firma del jurado

GIRARDOT, 27 de noviembre de 2021

AGRADECIMIENTOS

Agradezco primero a dios y a mi familia por inspirarme a ser mejor persona, por impulsarme a crecer profesional y moralmente, a los ingenieros de la Unad por soportar el karma de ayudarme en mi proceso que sé que no fue fácil y termino dejándoles varias canas, siempre les agradeceré por estar pendiente de que todo me saliera bien, de corazón aspiro que continúen dejando su marca personal y corazón en cada actividad que realiza en esta Universidad.

TABLA DE CONTENIDO

TABLAS DE ILUSTRACIONES

LISTA DE TABLAS

GLOSARIO

ENRUTAMIENTO DINAMICO: El enrutamiento adaptativo, también llamado enrutamiento dinámico, es un proceso para determinar la ruta óptima que debe seguir un paquete de datos a través de una red para llegar a un destino específico.

OSPF: Open Short Path First versión 2, es un protocolo de routing interno basado en el estado del enlace o algoritmo Short Path First, estándar de Internet, que ha sido desarrollado por un grupo de trabajo del Internet Engineering task Force, cuya especificación viene recogida en el RFC 2328, es un protocolo de enrutamiento open source, por lo tanto, puede ser utilizado por equipos que no pertenezcan a la marca Cisco. Ha sido pensado para el entorno de Internet y su pila de protocolos TCP/IP, como un protocolo de routing interno, es decir, que distribuye información entre routers que pertenecen al mismo Sistema Autónomo.

DHCP: El Protocolo de configuración dinámica de host (DHCP) es un protocolo cliente/servidor que proporciona automáticamente un host de protocolo de Internet (IP) con su dirección IP y otra información de configuración relacionada, como la máscara de subred y la puerta de enlace predeterminad

LOOPBACK DNS: El Servicio de nombres de dominio le indica al navegador la dirección IP que se ha registrado oficialmente para un nombre de dominio especificado. El navegador sólo conoce la dirección de un servidor DNS, ya que se introduce en su configuración. Esa configuración puede apuntar a un archivo en una computadora de la misma red, en un archivo disponible en una computadora conectada a Internet o a un archivo en el mismo equipo.

ACL: Una Lista de Control de Accesos (ACL: Access Control List) es una serie de instrucciones que controlan que en un router se permita el paso o se bloqueen los paquetes IP de datos, que maneja el equipo según la información que se encuentra en el encabezado de estos.

NAT: funciona como un redireccionador de puertos del router. Es un intérprete o traductor de peticiones. Cuando tu configuras tu router, que tiene una IP única en cada momento, para que redirecciones puertos de servicios concretos a ciertas máquinas o dispositivos de tu red, estás configurando un NAT el principal objetivo es comunicarse con redes externas sin necesitar consumir direcciones públicas, que utilizan protocolos desconocidos o sin compatibilidad

RESUMEN

El siguiente documento es una registro sobre el cumplimiento de los parámetros requeridos en el diplomado CISCO CCNA, en el cual se adquirieron conocimientos y habilidades que ayudaron a mejorar el dominio de los conceptos básicos e intermedios para la administración y manipulación de las diferentes capas del modelo OSI profundizando en factores como la práctica y ejercicios de campo mediante el programa packet tracert ofrecido por la plataforma netacad, en todas las actividades hubo dependencia del conocimiento teórico, conceptual y de aplicación para implementación de redes LAN WAN en el futuro desempeño profesional

PALABRAS CLAVE: Administración, interconexión, comunicación, multicapa, enrutamiento

ABSTRACT

The following document is a reference guide on the fulfillment of the parameters required in the CISCO CCNA diploma course, in which knowledge and skills were acquired that helped to improve the mastery of the basic and intermediate concepts for the administration and manipulation of the different layers of the OSI model deepening factors such as practice and field exercises using the packet tracert program offered by the netacad platform, in all activities there was dependence of theoretical, conceptual and application knowledge for implementation of LAN WAN networks in future professional performance

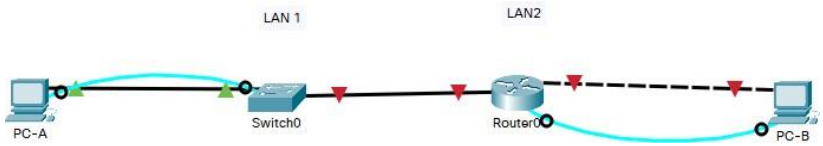
KEYWORDS: Management, interconnection, communication, multilayer, routing

INTRODUCCIÓN

Las herramientas marcan la diferencia, cuando se tienen buenos fundamentos, en redes se facilita entender cómo crece una infraestructura, como mantenerla y solucionar los posibles problemas, esto nos permite aclarar el porqué de cada cosa que aspiramos aplicar o su objetivo, vamos realizar un recorrido por el cumplimiento de los temas de este diplomado, la información que se adquirió y el cómo se aplica cada concepto en la vida real a través de cada actividad, podremos identificar el control de los dispositivos de red desde un computador por medio de un cable de consola o el acceso directo mediante el cli o consola en un router o switch que tenga IOS como sistema principal de los dispositivos, en cisco los comandos son generales y son parecidos, se derivan en una rutina de procedimientos para establecer el orden factores como el cálculo de las subredes y la cantidad de equipos que se requieren conectar, es vital conocer las características de los dispositivos a usar y como se crea la necesidad para poder realizar una planeación precisa mediante el uso de herramientas de simulación de red como packet tracert, el cual promueve un desarrollo avanzado de una red y simular lo que se quiere alcanzar antes de implementarlo puesto así en la explicación de escenarios veremos el desarrollo de temas como vlans enrutamiento estático y dinámico, direccionamiento, lista de control de acceso, protocolos, máscaras de tamaño variable subredes entre otros vamos hacer un recorrido por las capas del modelo OSI pero de una manera aplicada dejando de lado pero en nuestra mente los conceptos generales y una tomando una vista a la aplicación, en cada escenario sobresalen temas específicos como OSPF y el conocimiento de la cantidad de usuarios máximos para una subred los filtros en tiempo real y los mecanismos de control para realizar redes más seguras y más administrables nuestra tecnología avanzar a pasos largos ayer un computador llenaba una habitación hoy con un Smartphone podemos vulnerar cualquier red si no es administrada por personas idóneas de allí se sugiere intrínsecamente basar la atención en la seguridad desde que se empieza a construir un proyecto.

ESCENARIO 1 Construcción de la red

Ilustración 1 escenario inicial



Fuente: propia

Cálculo de subredes

Tabla 1 direccionamiento

	CANTIDAD	SUBREDES	MASCARA EN NUMERO	MASCARAS	PRIMERA IP	ULTIMA IP	BROADCAST	SIGUIENTE SUBRED
100	1	192.168.72.0	25	255.255.255.128	192.168.72.1	192.168.72.126	192.168.72.127	128
50	2	192.168.72.128	26	255.255.255.192	192.168.72.129	192.168.72.190	192.168.72.191	64

Fuente: propia

Tabla 2 asignación de direcciones

REQUERIMIENTO	ASIGNACION
Dirección de Red	192.168.72.0
Requerimiento de host Subred LAN1	192.168.72.128
Requerimiento de host Subred LAN2	192.168.72.192
R1 G0/0/1	192.168.72.1
R1 G0/0/0	192.168.72.129
S1 SVI	192.168.72.2
PC-A	192.168.72.126
PC-B	192.168.72.190

Fuente: propia

Comandos configuración router R1

Tabla 3 configuración router 1

COMANDO	ACCION
Router(config)#no ip domain-lookup	Desactiva la búsqueda de dominio
Router(config)#hostname R1	Asigna el nombre del router
R1(config)#ip domain name ccna-lab.com	Sirve para Establecer el dominio
R1(config)#enable secret ciscoenpass	Cifra la contraseña para el modo de ejecución
R1(config)#line console 0	Cambia a la línea de consola
R1(config-line)#password ciscoconpass	Establece la contraseña para la consola
R1(config)#security passwords min-length 10	Establecer una longitud mínima
R1(config)#username admin password admin1pass	Crear usuarios administrativos
R1(config)#line vty 0 4	Acceder line vty
R1(config-line)#password ciscocisco	Establecer un password line vty
R1(config-line)#login local	Definir autenticación local
R1(config-line)#transport input ssh	Establecer protocolo de trasporte ssh
R1(config)#service password-encryption	Cifra las contraseña de texto no cifrado
R1(config)#banner motd ## este es un router privado cualquier instruccion tendra efectos penales##	Definir el mensaje banner para información de acceso al router
R1(config)#interface GigabitEthernet0/0/0	Seleccionar interfaz 0
R1(config-if)#ip address 192.168.72.129 255.255.255.192	Asignación de ip y mascara
R1(config-if)#description esta es la interfaz	Agregar una descripción a la interfaz

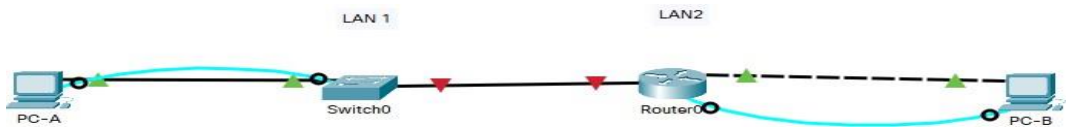
de la LAN 2	
R1(config-if)#no shutdown	Encender la interfaz GigabitEthernet0/0/0
R1(config-if)#interface GigabitEthernet0/0/1 R1(config-if)#no shutdown	Encender la interfaz GigabitEthernet0/0/1
R1(config-if)#description esta es la interfaz de la LAN 1	Descripción de la interfaz LAN 1
R1(config-if)#ip address 192.168.72.1 255.255.255.128	Asignar dirección ip a la interfaz GigabitEthernet0/0/1
R1(config-if)#no shutdown	Encender la interfaz
R1(config)#crypto key generate rsa	Generar acceso domain 1024 bits
R1#copy running-config startup-config	Guardando la configuración del router

Fuente: propia

Current config r1
Current configuration: 1069 bytes
version 16.6.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
security passwords min-length 10
hostname R1
enable secret 5 1mERr$EJnmB234UvJf9yoQMWYJK/
ip cef
no ipv6 cef
username admin password 7 082048430017540713181F
no ip domain-lookup
ip domain-name ccna-lab.com
spanning-tree mode pvst
interface GigabitEthernet0/0/0
description esta es la interfaz de la LAN 2
ip address 192.168.72.129 255.255.255.192
duplex auto
speed auto
interface GigabitEthernet0/0/1
description esta es la interfaz de la LAN 1
ip address 192.168.72.1 255.255.255.128
duplex auto
speed auto
interface GigabitEthernet0/0/2
no ip address
duplex auto
speed auto
shutdown
interface Vlan1
no ip address

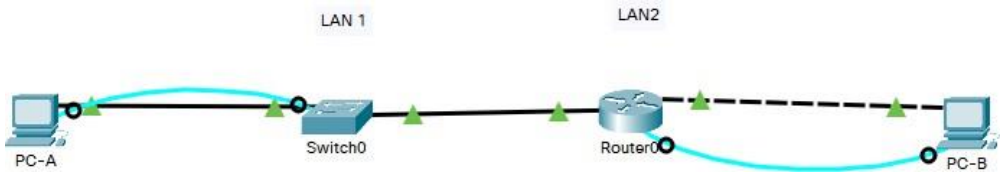
shutdown
ip classless
ip flow-export version 9
banner motd ^C^C
line con 0
password 7 0822455D0A1606181C1B0D1739
login
line aux 0
line vty 0 4
password 7 0822455D0A16061E010803
login local
transport input ssh

Primera interfaz encendida
Ilustración 2 encendido de la interfaz



Fuente: propia

Segunda interfaz encendida
Ilustración 3 configuración segunda interfaz



Fuente: propia

Configuración s1
Tabla 4 configuración S1

COMANDO	ACCION
S1(config)#no ip domain-lookup	Deshabilitar la búsqueda de dominio
Switch(config)#hostname S1	Asignación de nombre
S1(config)#ip domain name ccna-	Asignación de dominio

lab.com	
S1(config)#enable secret ciscoenpass	Habilitar password con seguridad
S1(config-line)#	Acceder línea de consola
S1(config-line)#password ciscoconpass	Asignar password línea de consola
S1(config-line)#username admin password admin1pass	Creación de usuario y password
S1(config)#line vty 0 4	Acceder línea vty
S1(config-line)#password ciscocisco	Asignación de password
S1(config-line)#transport input ssh	Configuración capa de transporte ssh
S1(config-line)#service password-encryption	Cifrar las contraseñas de texto no cifrado
S1(config-line)#banner motd ## este es un router privado cualquier instruccion tendra efectos penales##	Definición del banner de acceso
S1(config)#crypto key generate rsa	Definición clave de cifrado a 1024
S1(config-if)#ip address 192.168.72.2 255.255.255.128	Configuración vlan
S1(config-if)#no shutdown	encendido de interfaz
S1(config)#ip default-gateway 192.168.72.1	Asignación del Gateway
S1#copy running-config startup-config	Guardar la configuración

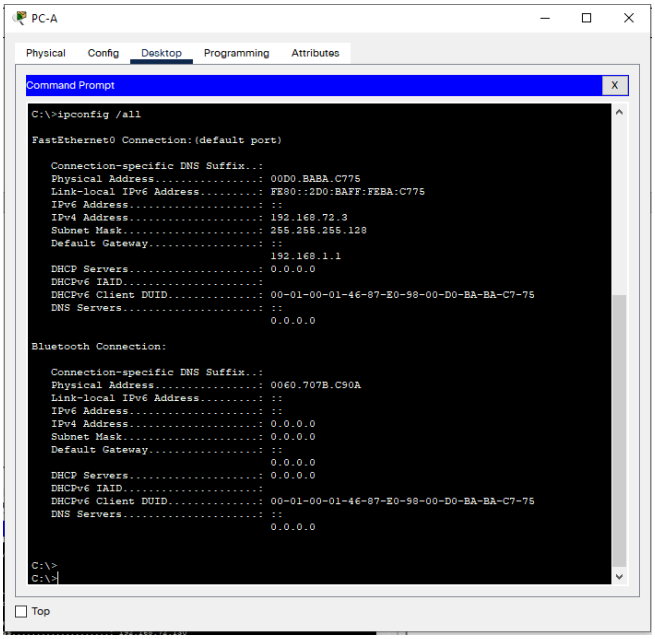
Fuente: propia

Current config s1
Current configuration : 1393 bytes
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
hostname S1
enable secret 5 1mERr$EJnmB234UvJf9yoQMWYJK/
no ip domain-lookup
ip domain-name ccna-lab.com
username admin privilege 1 password 7 082048430017540713181F
spanning-tree mode pvst
spanning-tree extend system-id
interface FastEthernet0/1
interface FastEthernet0/2
interface FastEthernet0/3
interface FastEthernet0/4
interface FastEthernet0/5

interface FastEthernet0/6
interface FastEthernet0/7
interface FastEthernet0/8
interface FastEthernet0/9
interface FastEthernet0/10
interface FastEthernet0/11
interface FastEthernet0/12
interface FastEthernet0/13
interface FastEthernet0/14
interface FastEthernet0/15
interface FastEthernet0/16
interface FastEthernet0/17
interface FastEthernet0/18
interface FastEthernet0/19
interface FastEthernet0/20
interface FastEthernet0/21
interface FastEthernet0/22
interface FastEthernet0/23
interface FastEthernet0/24
interface GigabitEthernet0/1
interface GigabitEthernet0/2
interface Vlan1
ip address 192.168.72.2 255.255.255.128
ip default-gateway 192.168.72.1
banner motd ^C^C
line con 0
password 7 0822455D0A1606181C1B0D1739
line vty 0 4
password 7 0822455D0A16061E010803
login
transport input ssh
line vty 5 15
login

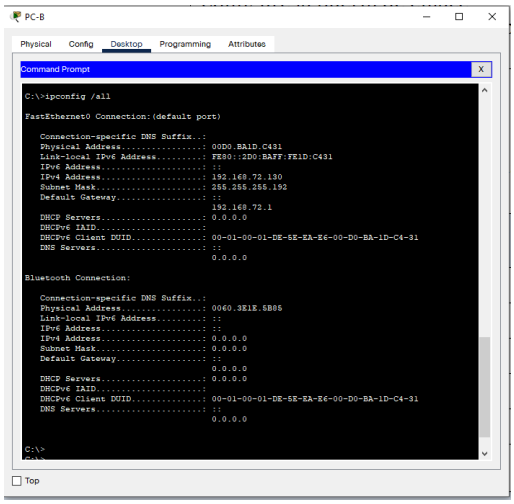
Configuración equipos de computo

Ilustración 4 configuración PC-A



Fuente: propia

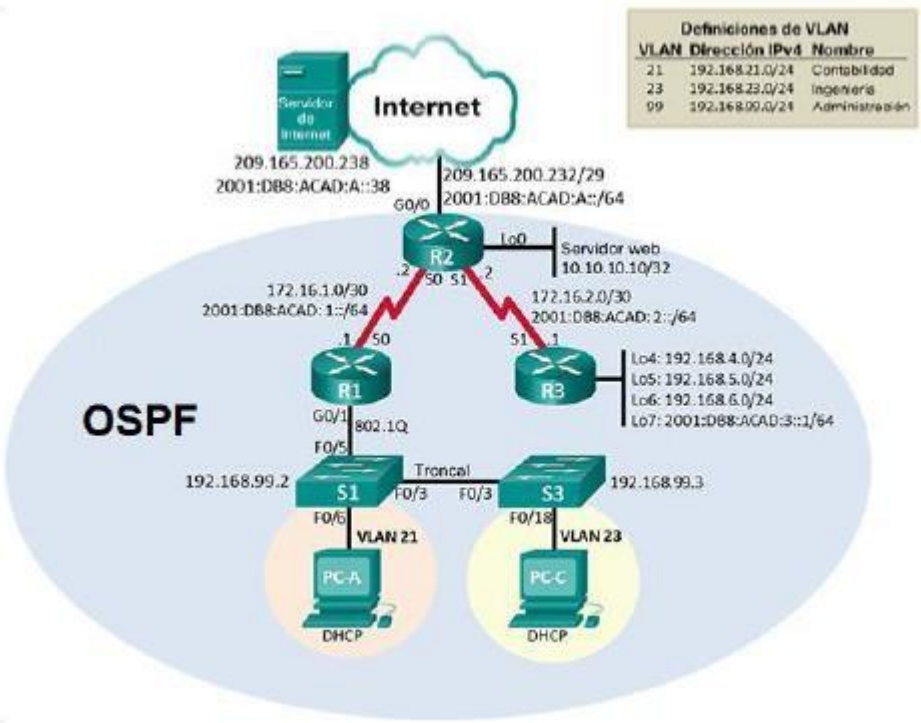
Ilustración 5 Configuración PC-B



Fuente: propia

ESCENARIO 2

Ilustración 6 Escenario 2



(cisco, 2021)

Inicializar dispositivos

- Elimine las configuraciones de inicio y vuelva a cargar los dispositivos.
- Antes de continuar, solicite al instructor que verifique la inicialización de los dispositivos.
- Eliminar el archivo startup-config de todos los routers

Restablecer configuraciones del R1
Ilustración 7 Restablecer R1

```
Router>enable
Router#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Router#
```

Fuente: propia

Restablecer configuraciones del R2
Ilustración 8 Restablecer R2

```
Router>enable
Router#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Router#
```

Fuente: propia

Restablecer configuraciones del R3
Ilustración 9 Restablecer R3

```
Router>enable
Router#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Router#
```

Fuente: propia

Router>enable
Router#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Router#reload
Proceed with reload? [confirm]

NOTA: La anterior imagen demostrara el comportamiento de los comandos en los tres routers en vista de que es el mismo procedimiento o comando para conseguir el resultado esperado

Eliminar el archivo startup-config de todos los switches *y recargarlos*
Switch>enable
Switch#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Switch#reload
Proceed with reload? [confirm]
Ilustración 10 evidencia show flash

```
Switch>enable
Switch#show flash
Directory of flash:/

    1  -rw-     4670455          <no date>  2960-lanbasek9-mz.150-2.SE4.bin

64016384 bytes total (59345929 bytes free)
Switch#
```

Fuente: propia

PARTE 2: Configurar los parámetros básicos de los dispositivos

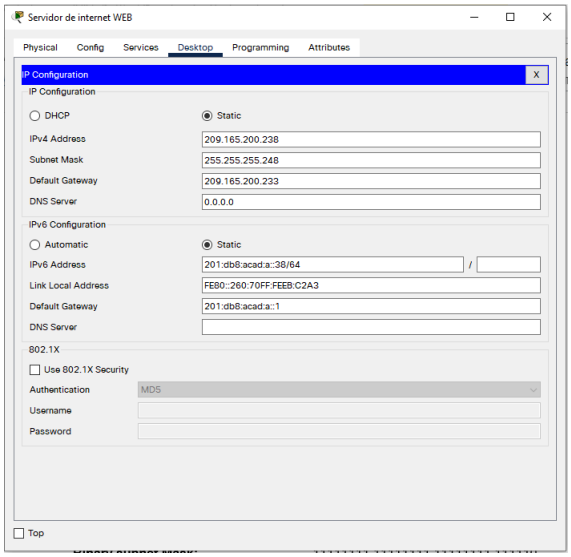
Configuración servidor de internet y direccionamiento Servidor web

Tabla 5 configuración servidor web

Entrada	**Dirección**
Dirección lpv4	209.165.200.238
Máscaras de subred para lpv4:	255.255.255.248
Gateway predeterminado:	209.165.200.233
Dirección lpv6/subred:	201:db8:acad:a::38/64
Gateway predeterminado lpv6:	201:db8:acad:a::1

Fuente: propia

Ilustración 11 Configuración servidor



Fuente: propia

Tabla 6 Configuración principal escenario 2

ID:	209.165.200.232
Dirección de red:	209.165.200.232
rango:	209.165.200.233-209.165.200.238
Broadcast:	209.165.200.239
Numero de host:	8
Numero de host disponible:	6

Mascara de subred:	255.255.255.248
Mascara Wildcard:	0.0.0.7
Mascara Binaria:	11111111.11111111.11111111.111110
Tipo de dirección:	PUBLICIP-CLASS C

Fuente: propia

Tabla 7 Asignación ipv6 y rango de direcciones

Dirección ipv6:	2001.db8:acad:a::38/64
Dirección ipv6 completa:	2001:0db8:acad:000a:0000:0000:0000:0038
Total de direcciones:	Q18.446.744.073.709.551.616
Red:	2001:0db8:acad:000a:: /64 2001:0db8:acad:000a:0000:0000:0000:0000/
Rango de direcciones	2001:db8:acad:a::1 2001:0db8:acad:000a:0000:0000:0000:0001 2001:db8:acad:a:ffff:ffff:ffff:ffff 2001:0db8:acad:000a:ffff:ffff:ffff:ffff
Tipo de direcciones:	GLOBAL UNICAST

Fuente: propia

Configuración R1

Tabla 8 Configuración de R1

COMANDO	ACCION
Router>enable Router#configure terminal Enter configuration commands, one per line. End with CNTL/Z.	Acceso a la configuración del router y terminal
Router(config)#no ip domain-lookup	Deshabilitar búsqueda
Router(config)#hostname R1	Cambio de nombre
R1(config)#enable secret class	Password secreto
R1(config)#line console 0	Línea de consola
R1(config-line)#password cisco	Asignación de password
R1(config-line)#login	Logueo
R1(config-line)#line vty 0 15	Definir vty
R1(config-line)#password cisco	Asignacion de password
R1(config-line)#login	Logueo
R1(config-line)#service password-encryption	Encriptación

R1(config)#banner motd %Se prohibe el acceso no autorizado.% ipv6 unicast-routing	Banner o mensaje Para permitir direccionamiento ipv6(importante para direccionamiento)
R1(config)#interface s0/0/0	Seleccionar interfaz
R1(config-if)#description	Definir descripción
R1(config-if)#ip address 172.16.1.1 255.255.255.252	Definir dirección ip y mascara
R1(config-if)#ipv6 address 2001:db8:acad:1::1/64	Definir ipv6 y mascara
R1(config-if)#clock rate 128000	Definir reloj
R1(config-if)#no shutdown	Encender
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down	Evidencia interfaz encendida
R1(config-if)#exit	Salir
R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0	Definir rutas predeterminadas ipv4
R1(config)#ipv6 route ::/0 s0/0/0	Definir rutas predeterminadas ipv6

Fuente: propia

NOTA el comando ipv6 unicast-routing es parte esencial en el desarrollo de este ejercicio por lo que se debe tener presente siempre que se haga cada configuración, adicional no se configuro G0/1

Configuración R2

Tabla 9 Configuración R2

COMANDO	ACCION
Router>enable Router#configure terminal Enter configuration commands, one per line. End with CNTL/Z.	Acceso a la configuración del router y terminal
Router(config)#no ip domain-lookup	Deshabilita la búsqueda de dominio
Router(config)#hostname R2	Cambia el nombre
R2(config)#enable secret class R2(config)#line console 0 R2(config-line)#password cisco R2(config-line)#login R2(config-line)#line vty 0 15 R2(config-line)#password cisco R2(config-line)#login R2(config-line)#service password-encryption	Habilita password secreto, habilita línea de consola, le define un password, se loguea,selecciona la línea vty de la 0 a la 15,le asigna un password, se loguea, encripta el password

R2(config)#ip http server R2(config)#banner motd %Se prohibe el acceso no autorizado.%	Comando no disponible en packet tracert, asigna un mensaje.
R2(config)#interface s0/0/0	Selecciona la interfaz serial 0/0/0
R2(config-if)#description Conexion 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 shutdown R2(config-if)#interface s0/0/1 R2(config-if)#description conexión a R3 R2(config-if)#ip address 172.16.2.2 255.255.255.252 R2(config-if)#ipv6 address 2001:db8:acad:2::2/64	Define una descripción a la interfaz, asigna una dirección ip y mascara de subred, asigna una dirección ip y mascara de subred al dispositivo, enciende la interfaz. Evidencia cambio de estado del puerto serial 0/0/0, selección interfaz 0/0/1, creación de descripción, asignación de direcciones ipv4 e ipv6
R2(config-if)#interface g0/0 R2(config-if)#description Conexion a internet R2(config-if)#ip address 209.165.200.233 255.255.255.248 R2(config-if)#ipv6 address 2001:db8:acad:a::1/64 R2(config-if)#no shutdown R2(config-if)#interface loopback 0 R2(config-if)# R2(config-if)#ip address 10.10.10.10 255.255.255.255 R2(config-if)#description Servidor web R2(config-if)#exit R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0 %Default route without gateway, if not a point-to-point interface, may impact performance R2(config)#ipv6 route ::/0 g0/0	Selección g/0/0/0 Creación de descripción Asignación de dirección ip4 y mascara Asignación de ipv6 y mascara Se enciende la interfaz Se evidencia cambio de estado Selección interfaz loopback 0 Evidencia del estado Asignación de dirección y mascara Asignación de descripción Asignación de rutas predeterminadas
ip http server // este comando genera un error en vista de que no está disponible en packet tracer	Ilustración 12 Router>enable Router#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Router(config)#no ip domain-lookup Router(config)#hostname R2 R2(config)#enable secret class R2(config)#line console 0 R2(config-line)#password cisco R2(config-line)#login R2(config-line)#line vty 0 15 R2(config-line)#password cisco R2(config-line)#login R2(config-line)#service password-encryption R2(config)#ip http server ^ % Invalid input detected at '^' marker.

Fuente: propia

Configuración de r3

Tabla 10 Configuración R3

COMANDO	ACCION
Router>enable	Configuración de la terminal
Router#configure terminal	Deshabilitar la búsqueda de dominio
R3(config)#enable secret class	Habilitar password
R3(config)#line console 0	Habilitar línea de consola
R3(config-line)#password cisco	Habilitar password cisco
R3(config-line)#login	Loguearse
R3(config-line)#line vty 0 15	Seleccionar línea vty de la 0 a la 15
R3(config-line)#password cisco	Asignar password cisco
R3(config-line)#login	Loguearse
R3(config-line)#service password-encryption	Habilitar encriptación
R3(config)#banner motd %Se prohíbe el acceso no autorizado. %	Definir un banner
R3(config)#interface s0/0/1	Seleccionar interfaz serial 0/0/0
R3(config-if)#description Conexion a R2	Definir descripción
R3(config-if)#ip address 172.16.2.1	Asignar dirección ipv4 y mascara
255.255.255.252 R3(config-if)#ipv6 address	Asignación ipv6 y mascara
2001:db8:acad:2::1/64	Encender la interfaz
R3(config-if)#no shutdown	Evidencia encendida de interfaz
R3(config-if)#interface loopback 4	Habilitar interfaz loopback
R3(config-if)#ip address 192.168.4.1	Asignar dirección y mascara
255.255.255.0	Comprobar el estado de la interfaz
R3(config-if)#interface loopback 5	Habilitar router para acceder a la terminal
R3(config-if)#ip address 192.168.5.1	Habilitar interfaz loopback
255.255.255.0	Asignar dirección y mascara
R3(config-if)#int loopback 6 R3(config-if)#	Comprobar el estado de la interfaz
R3(config-if)#ip address 192.168.6.1	Habilitar interfaz loopback
255.255.255.0	Asignar dirección y mascara
R3(config-if)#interface loopback 7	Comprobar el estado de la interfaz
R3(config-if)#ipv6 address	Asignar dirección ipv6
2001:DB8:ACAD:3::1/64 R3(config-if)#exit	Enrutar por puerto serial 0/0/1 en ipv4
R3(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1	Enrutar por puerto serial ipv6
%Default route without gateway, if not a point-to-point interface, may impact performance performance	
R3(config)#ipv6 route ::/0 s0/0/1	

Fuente: propia

Configuración S1

Tabla 11 Configuración S1

COMANDO	ACCION
Switch>enable	Habilitar switch
Switch#configure terminal	Acceso a la terminal
Switch(config)#no ip domain-lookup	Deshabilitar la busqueda de dominio

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 15 S1(config-line)#password cisco S1(config-line)#login S1(config-line)#service password-encryption S1(config)#banner motd %Se prohíbe el acceso no autorizado.%	Asignar nombre del host Habilitar password encriptado Habilitar línea de consola Habilitar el password cisco Loguearse Habilitar line vty de la línea 0 a la 15 Asignar password cisco Loguearse Habilitar encriptado asignación mensaje de banner

Fuente: propia

Configuración S3

Tabla 12 Configuración S3

COMANDO	ACCION
Switch>enable Switch#configure terminal 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	Habilitar switch Acceso a la terminal Deshabilitar la búsqueda de dominio Asignar nombre del host Habilitar password encriptado Habilitar línea de consola Habilitar el password cisco Loguearse
S3(config-line)#line vty 0 15 S3(config-line)#password cisco S3(config-line)#login S3(config-line)#service password-encryption S3(config)#banner motd %Se prohíbe el acceso no autorizado.%	Habilitar line vty de la línea 0 a la 15 Asignar password cisco Loguearse Habilitar encriptado asignación mensaje de banner

Fuente: propia

Resultado ping R1 R2 Servidor de internet

Tabla 13 revisión ping R1, R2, servidor

Desde	**A**	**Dirección IP**	**Resultados de Ping**
R1	R2, S0/0/0	172.16.1.2	Exitoso
R2	R3, S0/0/1	172.16.2.1	Exitoso
Servidor web de internet	Gateway predeterminado	209.165.200.233	Exitoso

Fuente: propia

Ilustración 13 ping R1 a R2

```
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 = 1/2/10 ms
```

Fuente: propia

Ilustración 14 ping R2 a R3

```
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 = 2/5/16 ms
```

Fuente: propia

Ilustración 15 ping servidor

```
Packet Tracer SERVER Command Line 1.0
C:\>ping 209.165.200.233

Pinging 209.165.200.233 with 32 bytes of data:

Reply from 209.165.200.233: bytes=32 time<1ms TTL=255
Reply from 209.165.200.233: bytes=32 time<1ms TTL=255
Reply from 209.165.200.233: bytes=32 time<1ms TTL=255
Reply from 209.165.200.233: bytes=32 time<1ms TTL=255

Ping statistics for 209.165.200.233:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Fuente: propia

Configuración S1

Tabla 14 Configuración S1 vlan 21,23,99

COMANDO	ACCION
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 Administracion S1(config-vlan)#exit S1(config)#interface vlan 99 S1(config-if)#ip address 192.168.99.2 255.255.255.0 S1(config-if)#no shutdown S1(config-if)#exit S1(config)#ip default-gateway 192.168.99.1 S1(config)#interface f0/3 S1(config-if)#switchport mode trunk	Acceso al s1 Terminal Creación vlans y asignación de nombre Seleccionar la interfaz vlan 99 para cambiar el estado Definir dirección ipv4 Encenderla Salir Definir una puerta de enlace predeterminada Convertirla en trocal

S1(config-if)#switchport trunk native vlan 1 S1(config-if)#interface f0/5 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1 S1(config-if)#interface range f0/1-2, f0/4, f0/6-24, g0/1-2 S1(config-if-range)#switchport mode access S1(config-if-range)#interface f0/6 S1(config-if)#switchport access vlan 21 S1(config-if)#interface range f0/1-2, f0/4, f0/7-24, g0/1-2 S1(config-if-range)#shutdown	Configuración general de las vlan de acceso por rango de interfaces nativas troncales y de acceso

Fuente: propia

Configuración S3

Tabla 15 Configuración S3 vlan 21,23,99

COMANDO	ACCION
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)#exit S3(config)#interface vlan 99 S3(config-if)#ip address 192.168.99.2 255.255.255.0 S3(config-if)#no shutdown S3(config-if)#exit S3(config)#ip default-gateway 192.168.99.1 S3(config)#interface f0/3 S3(config-if)#switchport mode trunk S3(config-if)#switchport trunk native vlan 1 S3(config-if)#interface f0/5 S3(config-if)#switchport mode trunk S3(config-if)#switchport trunk native vlan 1 S3(config-if)#interface range f0/1-2, f0/4, f0/6-24, g0/1-2 S3(config-if-range)#switchport mode access S3(config-if-range)#interface f0/6 S3(config-if)#switchport access vlan 21 S3(config-if)#interface range f0/1-2, f0/4, f0/7-24, g0/1-2 S3(config-if-range)#shutdown	Creación vlans y asignación de nombre Seleccionar la interfaz vlan 99 para cambiar el estado Definir dirección ipv4 Encenderla interfaz Salir Definir una puerta de enlace predeterminada Convertirla en trocal Configuración general de las vlan de acceso por rango de interfaces nativas troncales y de acceso

Fuente: propia

Segunda configuración r1

Tabla 16 configuración R1 vlan 21,23,99

COMANDO	ACCION
R1(config)#interface 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)#interface 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)#interface g0/1.99 R1(config-subif)#description LAN de Administracion R1(config-subif)#encapsulation dot1q 99 R1(config-subif)#ip address 192.168.99.1 255.255.255.0 R1(config-subif)#interface g0/1 R1(config-if)#no shutdown R1(config-if)#	Seleccionar subinterfaz g/0/1.21 Crear la descripción Encapsular Definir dirección ip Seleccionar subinterfaz g0/1.23 Crear descripción Encapsular Definir dirección ip Seleccionar subinterfaz g0/1.99 Crear descripción Encapsular Definir dirección ip Seleccionar interfaz g0/1 Encender la interfaz

Fuente: propia

Resultados ping S1, S3

Tabla 17 ping s1 a r1 y s3 a r1 vlan

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

Fuente: propia

Ilustración 16 ping S1 a R1

```
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 = 0/0/0 ms
```

Fuente: propia

Ilustración 17 ping S3 a R1

```
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 = 0/0/0 ms
```

Fuente: propia

Ilustración 18 S1 a 21

```
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 = 0/0/0 ms
```

Fuente: propia

Ilustración 19 ping S3 a 23

```
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 = 0/0/3 ms
```

Fuente: propia

Configuración adicional router 1
Tabla 18 Anunciar redes

COMANDO	ACCION
R1>enable Password: Password: Password: R1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. R1(config)#router ospf 72 R1(config-router)#network 172.16.1.0 0.0.0.3 area 0 R1(config-router)#network 192.168.21.0 0.0.0.255 area 0 R1(config-router)#network 192.168.23.0 0.0.0.255 area 0 R1(config-router)#network 192.168.99.0 0.0.0.255 area 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	Acceso a la terminar con privilegios Habilitar ospf Anunciar la red con wildcard y área 0 Anunciar la red con wildcard y área 0 orientado a vlans Anunciar la red con wildcard y área 0 orientado a vlans Anunciar la red con wildcard y área 0 orientado a vlans Habilitar interfaces pasivas para cada subinterface en g0/0/0

Fuente: propia

La configuración del r2 ospf

Tabla 19 Configuración OSPF

COMANDO	ACCION
R2>enable Password: R2#configure terminal Enter configuration commands, one per line. End with CNTL/Z. R2(config)#router ospf 72 R2(config-router)#network 10.10.10.10 0.0.0.0 area 0 R2(config-router)#network 172.16.1.0 0.0.0.3 area 0 R2(config-router)# 00:15:45: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.99.1 on Serial0/0/0 from LOADING to FULL, Loading Done R2(config-router)#network 172.16.2.0 0.0.0.3 area 0 R2(config-router)#passive-interface loopback 0	Configurar OSPF área 0 Anunciar las redes conectadas directamente Establecer la interfaz LAN (loopback) como pasiva Desactive la sumarización automática.

Fuente: propia

Configuracion OSPF R3

Tabla 20 Configuración OSPF R3

COMANDO	ACCION
R3(config)#router ospf 73 R3(config-router)#network 172.16.2.0 0.0.0.3 area 0 R3(config-router)#network 192.168.4.0 0.0.0.255 area 0 R3(config-router)#network 192.168.5.0 0.0.0.255 area 0 R3(config-router)#network 192.168.6.0 0.0.0.255 area 0 R3(config-router)#passive-interface loopback 4 R3(config-router)#passive-interface loopback 5 R3(config-router)#passive-interface loopback 6	Configurar OSPF área 0 Anunciar las redes conectadas directamente Establecer la interfaz LAN (loopback) como pasiva Desactive la sumarización automática
Evidencia commando sh ip protocols	*Ilustración 20 show ip protocols*

	R2#Sh ip protocols Routing Protocol is "ospf 1" Outgoing update filter list for all interfaces is not set Incoming update filter list for all interfaces is not set Router ID 10.10.10.10 Number of areas in this router is 1. 1 normal 0 stub 0 nssa Maximum path: 4 Routing for Networks: 172.16.2.0 0.0.0.3 area 0 192.168.4.0 0.0.0.255 area 0 192.168.5.0 0.0.0.255 area 0 192.168.6.0 0.0.0.255 area 0 Routing Information Sources: Gateway Distance Last Update 10.10.10.10 110 00:12:56 Distance: (default is 110) Fuente: propia
Evidencia commando sh ip route	*Ilustración 21 show ip route* R2#Sh 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 10.0.0.0/32 is subnetted, 1 subnets C 10.10.10.10/32 is directly connected, Loopback0 172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks C 172.16.1.0/30 is directly connected, Serial0/0/0 L 172.16.1.2/32 is directly connected, Serial0/0/0 R2# Fuente: propia

Fuente: propia

Configurar el R1 como servidor de DHCP para las VLAN 21 y 23

Tabla 21 Configuración R1 dhcp vlan 21,23

COMANDO	ACCION
R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20	Exclusión direccion dhcp desde la 1 a la 20 en el segmento 21
R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20	Exclusión direccion dhcp desde la 1 a la 20 en el segmento 23
R1(config)#ip dhcp pool ACCT	Ejecucion dhcp
R1(dhcp-config)#network 192.168.21.0 255.255.255.0	Seleccionar asignar red y mascara para distribuir dhcp segmento 21
R1(dhcp-config)#default-router 192.168.21.1	Router por defecto para dhcp segmento 21
R1(dhcp-config)#dns-server 10.10.10.10	Asignación ip para servidor dns
R1(dhcp-config)#ip domain-name ccna-sa.com	Asignación de dominio para dhcp
R1(config)#ip dhcp pool ENGNR	
R1(dhcp-config)#network 192.168.23.0 255.255.255.0	Seleccionar asignar red y mascara para distribuir dhcp segmento 23

R1(dhcp-config)#default-router 192.168.23.1	Router por defecto para dhcp segmento 23
R1(dhcp-config)#dns-server 10.10.10.10	Asignación ip para servidor dns
R1(dhcp-config)#ip domain-name ccna-sa.com	Asignación de nombre de dominio

Fuente: propia

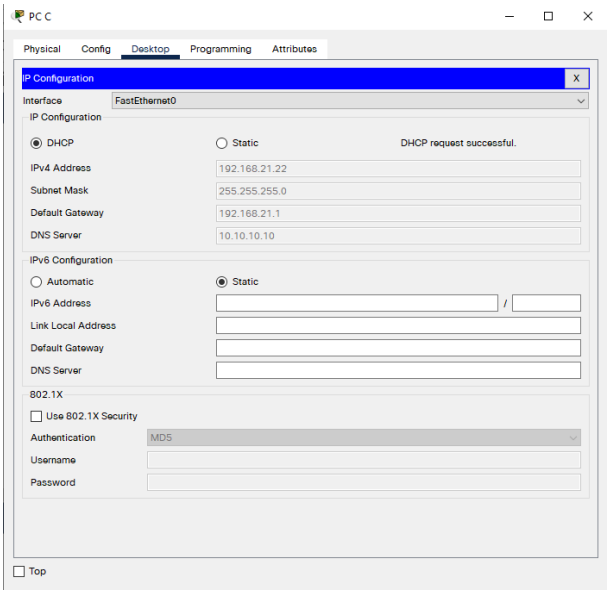
Configuración de usuarios R2

Tabla 22 Configuración R2 acceso y NATS

COMANDO	ACCION
R2(config)#username webuser privilege 15 secret cisco12345	Creación del usuario con privilegios asignando un password encriptado bajo
R2(config)#ip http server	Commando no disponible en packet tracert
^% Invalid input detected at '^' marker.	Erro generado
R2(config)#ip http authentication local	No se permite este comando
% Invalid input detected at '^' marker.	Error generado
R2(config)#ip http secure- server	No se permite este comando
^% Invalid input detected at '^' marker.	Error generado
R2(config)#ip nat inside source static 10.10.10.10 209.165.200.237	Definicion nat estatica
R2(config)#interface g0/0	Seleccion de interfaz
R2(config-if)#ip nat outside	Definicion de nat de salida
R2(config- if)#interface 0/0/0	Seleccion de interfaz 0/0/0
R2(config-if)#ip nat inside	Definicion nat de entrada
R2(config- if)#interface s0/0/1	Seleccion de Interfax 0/0/1
R2(config-if)#ip nat inside	Definicion nat de entrada
R2(configif)#exit	Salir
R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255	Definicion de listas de acceso permitidos
R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255	Permiso a todos los de la subred o segmento 23
R2(config)#access-list 1 permit 192.168.4.0 0.0.3.255	Permitir a todos los de la subred y el segmento 4
R2(config)#ip nat	pool INTERNET 209.165.200.233 209.165.200.236
netmask 255.255.255.28	
R2(config)#ip nat inside source list 1 pool INTERNET	Definicion nat de entrada desde las list creada

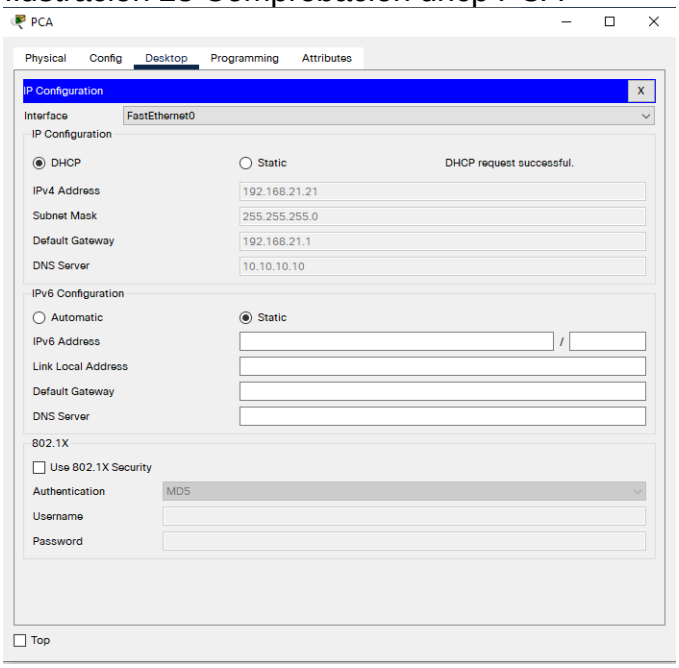
Fuente: propia

Ilustración 22 Comprobación dhcp PC-C



Fuente: propia

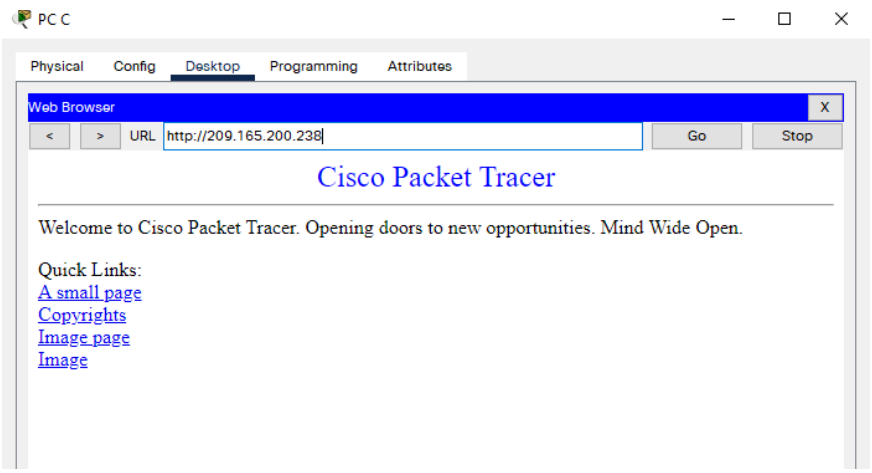
Ilustración 23 Comprobación dhcp PCA



Fuente: propia

Acceso al servidor: *Utilizar un navegador web en la computadora de Internet para acceder alservidor web (209.165.200.229) Iniciar sesión con el nombre de usuario webuser y la contraseña cisco12345*

Ilustración 24 Acceso servicio mediante navegador



Fuente: propia

Configuraciones de hora y ntp

Tabla 23 Asignación de hora, actualización y ACL

R2#clock set 00:40:00 30 April 2020.	Establece la hora del reloj
R2(config)#ntp master 5	Define como master 5
R1(config)#ntp server 172.16.1.2	Define el servidor ntp en la ip
R1(config)#ntp update-calendar	Actualiza el calendario
R1#show ntp associations	Muestra las asociaciones ntp
Nota: Este comando no es soportado con Packet Tracer.	
R1#telnet 172.16.1.2	Accede por telnet
Trying 172.16.1.2 …OpenSe prohibe el acceso no Elaboración propiaizado. User Access Verification	Mensaje de banner visto desde telnet
R2(config)#ip access-list standard ADMIN-MGT	Crea una lista de acceso estándar
R2(config-std-nacl)#permit host 172.16.1.1	Agrega como permitida la dirección ip
R2(config-std-nacl)#exit	Salir
R2(config)#line vty 0 15	Acceder a linea de consola
R2(config-line)#access-class ADMIN-MGT in	limita las conexiones de entrada entre las direcciones en la lista de acceso
R2(config-line)#transport input telnet	Define telnet como protocol de transporte
R2>exit	salir
[Connection to 172.16.1.2 closed by foreign host]	
R3#telnet 172.16.1.2	Petición de Acceso desde telnet
Trying 172.16.1.2 …	
% Connection refused by remote host R3#	Respuesta de la peticion

Fuente: propia

Ilustración 25 verificación acceso telnet R2

```
R2>enable
Password:
R2#telnet 172.16.1.2
Trying 172.16.1.2 ...
% Connection timed out; remote host not responding
R2#
```

Fuente: propia

Ilustración 26 acceso Telnet R1

```
R1#telnet 172.16.1.2
Trying 172.16.1.2 ...OpenSe prohibe el acceso no autorizado.
```

Fuente: propia

Ilustración 27 Telnet R1 a R2

```
R2>enable
Password:
R2#telnet 172.16.1.2
Trying 172.16.1.2 ...
% Connection timed out; remote host not responding
R2#
```

Fuente: propia

Show access list 1

Ilustración 28 mostrar ACL

```
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))
```

Fuente: propia

Restablecer los contadores de una lista de acceso

Tabla 24 restablecer contadores

R2#clear ip access-list counters	Limpia los contadores
R2#clear ip	Limpia las direcciones ip
bgp Clear BGP connections	Borrar las conexiones bgp
dhcp Delete items from the DHCP database nat Clear NAT	Elimina los elementos de la base de datos nat
ospf clear commands	Limpia los comando ospf
route Delete route table entries	Elimina las entradas o tablas enrutamiento

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

El comando show ip interface se utiliza para verificar la ACL en la interfaz donde sea invocado, el resultado de este comando incluye el número o el nombre de la lista de acceso y el sentido en el que se aplicó la ACL, debido a que lista se puede utilizar para verificar el estado de las interfaces del switch.
se aplica a una interfaz VLAN, la interfaz la cual recibe la dirección verifica si la IP está habilitada y en funcionamiento, por lo general, aunque hay diversos métodos es el método más sencillo

¿Con qué comando se muestran las traducciones NAT?

Para mostrar todas las traducciones NAT se utiliza el siguiente comando **show ip nat translations** y el resultado que nos arroja para este caso es mostrado a continuación

Ilustración 29 verificación NAT pcs y server

```
R2#
10:06:11: %OSPF-5-ADJCHG: Process 13, Nbr 192.168.23.1 on Serial0/0/0 from LOADING to
FULL, Loading Done
show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 209.165.200.226:10192.168.21.21:10   209.165.200.238:10 209.165.200.238:10
icmp 209.165.200.226:11192.168.21.21:11   209.165.200.238:11 209.165.200.238:11
icmp 209.165.200.226:12192.168.21.21:12   209.165.200.238:12 209.165.200.238:12
icmp 209.165.200.226:9 192.168.21.21:9    209.165.200.238:9  209.165.200.238:9
icmp 209.165.200.227:5 192.168.21.22:5    209.165.200.238:5  209.165.200.238:5
icmp 209.165.200.227:6 192.168.21.22:6    209.165.200.238:6  209.165.200.238:6
icmp 209.165.200.227:7 192.168.21.22:7    209.165.200.238:7  209.165.200.238:7
icmp 209.165.200.227:8 192.168.21.22:8    209.165.200.238:8  209.165.200.238:8
---  209.165.200.233   10.10.10.10        ---                ---
```

Fuente: propia

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

El comando que se usa para eliminar las nat antes de que se agote el tiempo de espera clear ip nat translation acompañado del * significa todos los elementos

CONCLUSIONES

Teniendo en cuenta el resultado de este trabajo, se puede concluir que la aplicación de la teoría proporcionada por el Instituto CISCO Networks y lo aprendido tanto en la primera como en la segunda parte de este módulo de Unadista es de gran importancia. para explorar el mundo del diseño de redes, pero también sirve para afirmar que es importante conocer herramientas que permitan estructurar y modelar arquitecturas sin adquirir directamente los dispositivos a implementar y poder verificar su comportamiento por medio de la simulación, las operaciones dinámicas de la red igual a las especificaciones para cada elemento. Son lo mismo. En los casos de estudio CCNA1 y CCNA2, no solo simulamos el para interactuar con las diversas herramientas disponibles para la red real, sino también el para probar cada una de las conexiones y el estado de Los estudios de caso detallados en estos trabajos se presentan con el objetivo de buscar alternativas al enfoque sistemas-entorno en a partir de una especificación orientada a problemas de la red y en los elementos contenidos en la misma red tomados en cada uno de los puntos. Puntos de referencia para iniciar un nuevo diseño de red con las Condiciones requeridas las herramientas proporcionadas en el desarrollo de este diplomado nos permiten ser mejores profesionales

BIBLIOGRAFIA

CORDOBA, N. (10 de 12 de 2020). www.unad.edu.co. Obtenido de https://repository.unad.edu.co/handle/10596/37989

BAREÑO, Gutiérrez, R., Sevillano, A. M. L., Díaz-Piraquive, F. N., & González- Crespo, R. (2021, July). Analysis of WEB Browsers of HSTS Security Under theMITM Management Environment. In International Conference on Knowledge Management in Organizations (pp. 331-344). Springer, Cham.

BAREÑO, Gutiérrez, R., Cardenas-Urrea, S. E., Navarro-Nuñez, W., Sarmiento-Osorio, H., & Forero-Paez, N. (2017). Sistema de votación electrónico con características de seguridad SSL/TLS e IPsec en Colombia. Revista UIS Ingenierías, 16(1), 75-84.

BAREÑO Gutiérrez, R. (2013). Elaboración de un estado de arte sobre el protocolo IPV6; y su implementación sobre protocolos de enrutamiento dinámicocomo RIPNG, EIGRP y OSPF basado sobre la plataforma de equipos cisco.

BAREÑO Raúl, G., & Sevillano, A. M. L. (2017, October). Services cloud underHSTS, Strengths and weakness before an attack of man in the middle MITM.

In 2017 Congreso Internacional de Innovacion y Tendencias en Ingenieria (CONIITI) (pp. 1-5). IEEE.

GUTIERREZ, R. B., Núñez, W. N., Urrea, S. C., Osorio, H. S., & Acosta, N. D.(2016). Revisión de la seguridad en la implementación de servicios sobre IPv6. Inge Cuc, 12(1), 86-93.

GUTIERREZ, R. B., Urrea, S. C., Núñez, W. N., Sarmiento, H., Acosta, N. D., & Sánchez, G. G. V. (2015). Análisis de la seguridad en la implementación de servicios corporativos sobre el protocolo IPV. Revista de Tecnología, 14(1), 127-138.

MOJICA S. Felipe, Andrés, L. V. S., & Raúl, B. G. (2019, October). Risks Found inElectronic Payment Cards on Integrated Public Transport System Applying the ISO27005 Standard. Case Study Sitp DC Colombia. In 2019 Congreso Internacional de Innovación y Tendencias en Ingenieria (CONIITI) (pp. 1-6). IEEE.

Switching, D. e. (14 de 08 de 2018). https://www.unad.edu.co/. Obtenido de https://repository.unad.edu.co/handle/10596/19462

UNAD, u. n. (08 de 2021). https://www.unad.edu.co/. Obtenido de https://campus107.unad.edu.co/ecbti93/pluginfile.php/2917/mod_folder/content/0/Syllabus%20de%20curso%20Diplomado%20de%20Profundizaci%C3%B3n%20CISCO%20CCNA.pdf?forcedownload=1