SOLUCIÓN DE DOS ESCENARIOS PRESENTES EN ENTORNOS CORPORATIVOS BAJO EL USO DE TECNOLOGÍAS CISCO

JENNY PAOLA DIAZ CHÁVEZ

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

SOLUCIÓN DE DOS ESCENARIOS PRESENTES EN ENTORNOS CORPORATIVOS BAJO EL USO DE TECNOLOGÍAS CISCO

JENNY PAOLA DIAZ CHÁVEZ

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

DIRECTOR:
RAUL BAREÑO GUTIERREZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA-UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGÍA E INGENIERÍA-ECBTI
INGENIERÍA DE SISTEMAS
SOGAMOSO
2021

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

_____

_____

_____

Firma del Presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

Sogamoso, 30 de noviembre de 2021

CONTENIDO

Pág.

LISTA DE FIGURAS

LISTA DE TABLAS

GLOSARIO

CCNA: (Cisco Certified Network Associate) es una certificación entregada por la compañía Cisco Systems a las personas que hayan rendido satisfactoriamente el examen correspondiente, sobre infraestructuras de red e Internet. Está orientada a los profesionales que operan equipamiento de networking.

INTERFAZ: Se refiere al componente de hardware que permite que un dispositivo pueda conectarse a una red cualquiera.

VLAN: Una VLAN, acrónimo de virtual LAN, es un método para crear redes lógicas independientes dentro de una misma red física. Varias VLAN pueden coexistir en un único conmutador físico o en una única red física.

IPV4: La dirección IPv4 es un número de 32 bits que identifica de forma exclusiva una interfaz de red en un sistema, tal como se explica en aplicación de las direcciones IP a las interfaces de red. Una dirección IPv4 se escribe en dígitos decimales, y se divide en cuatro campos de 8 bits separados por puntos.

IPV6: El IPv6 es una actualización al protocolo IPv4, diseñado para resolver el problema de agotamiento de direcciones.

RESÚMEN

En el presente informe se muestra paso a paso del desarrollo de dos escenarios planteados denominados, *Solución de dos escenarios presentes en entornos corporativos bajo el uso de tecnologías CISCO*, el anterior conformado por el módulo CCNA1 y CCNA2, busca incentivar el estudio de comandos, protocolos y previo uso de las herramientas necesarias para dar cumplimiento a los objetivos y configuración propuestos en la actividad.

Para el desarrollo de esta actividad se hace uso del simulador de Cisco Systems Packet Tracer, el cual optimiza el proceso de aprendizaje poniendo en práctica uno a uno los conocimientos obtenidos y a la vez arrojando en tiempo real las evidencias de los resultados de dichas configuraciones lo cual complementa y muestra la trazabilidad tanto del proceso como de los conocimientos obtenidos.

Este proyecto es realizado con el fin de otorgar el titulo de la carrera ingeniería de sistemas.

Palabras clave: CISCO, CCNA, conmutación, Packet Tracer, redes, ingeniería.

ABSTRACT

This report shows step by step the development of two scenarios called, Solution of two scenarios present in corporate environments using CISCO technologies, the previous one consisting of the CCNA1 and CCNA2 modules, seeks to encourage the study of commands, protocols and after using the necessary tools to comply with the objectives and configuration proposed in the activity.

For the development of this activity, use is made of the Cisco Systems Packet Tracer simulator, which optimizes the learning process by putting into practice the knowledge obtained one by one and at the same time showing in real time the evidence of the results of said configurations, which complements and shows the traceability of both the process and the knowledge obtained.

This project is carried out in order to grant the degree of systems engineering career.

Keywords: CISCO, CCNA, switching, Packet Tracer, networks, systems.

INTRODUCCIÓN

El presente trabajo se realiza siguiendo las rúbricas propuestas por el diplomado de profundización CISCO CCNA (diseño e implementación de soluciones integradas LAN/WAN), planteado como opción de trabajo de grado, en el cual busca identificar la compresión y habilidades para la solución de problemas relacionados con Networking; con base a lo anterior se plantean dos escenarios con sus respectivas evidencias, donde se observa el desarrollo de cada uno de estos.

En este se realizan prácticas en el software Packet Tracer siguiendo cada uno de los ítems propuestos en las diferentes unidades de los módulos CCNA1 y CCNA2, donde se contemplan temas como configuración de direccionamiento acorde a su topología configuración de protocolos de enrutamiento OSPFv2, configuración de enrutamiento dinámico, configuración de interfaces LAN, configuración de VLANs, implementación de DHCP y NAT para IPv4, configuración de DHCP para VLAN, configuración de NAT en router, configurar listas de acceso estándar y extendido.

Descripción de escenarios propuestos para la prueba de habilidades

1. ESCENARIO 1

Descripción general

Figura 1 - Topología propuesta escenario 1

Escenario 1

Topología

Fuente: propia

En este primer escenario se configurarán los dispositivos de una red pequeña. Debe configurar un router, un switch y equipos, diseñar el esquema de direccionamiento IPv4 para las LAN propuestas. El router y el switch también deben administrarse de forma segura.

Objetivos

Parte 1: Construir en el simulador la Red

Parte 2: Desarrollar el esquema de direccionamiento IP para la LAN1 y la LAN2

Parte 3: Configurar los aspectos básicos de los dispositivos de la Red propuesta.

Parte 4: Configurar los ajustes básicos de seguridad en el R1 y S1

Parte 4: Configurar los hosts y verificar la conectividad entre los equipos

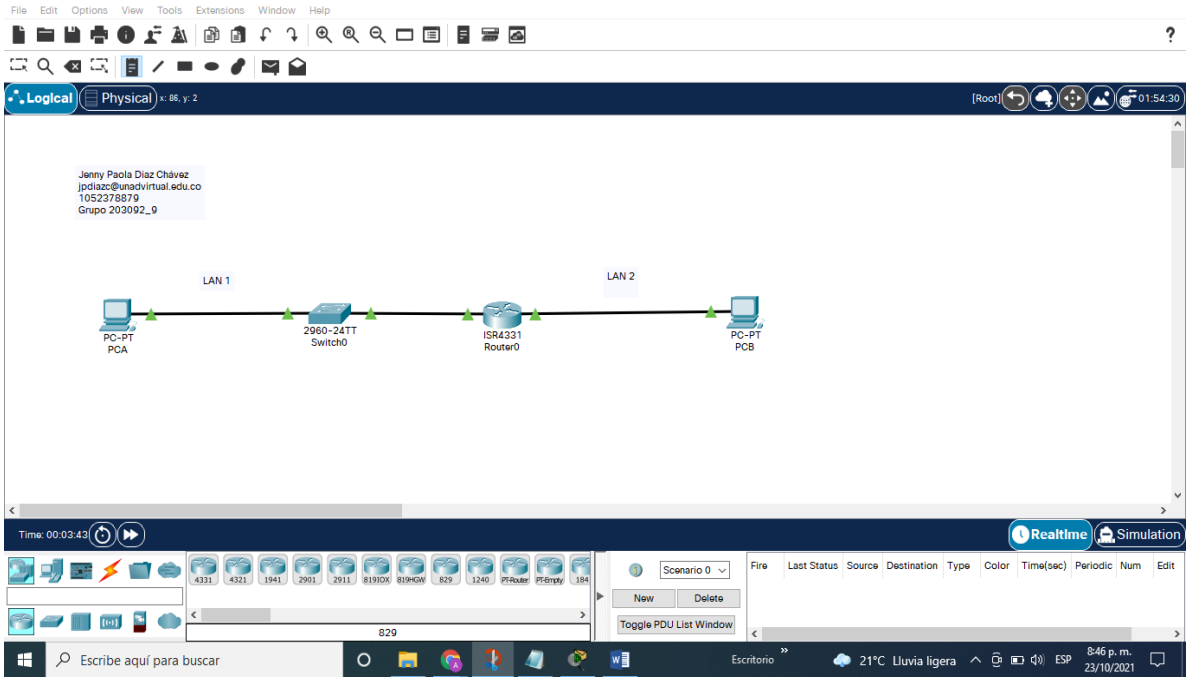
Aspectos básicos/situación

En el desarrollo del caso de estudio usted implementa la topología mostrada en la figura y configura el Router R1 y el swich S1, y los PCs. Con la dirección suministrada realizará el subnetting y cumplirá el requerimiento para la LAN1 (100 host) y la LAN2 (50 hosts).

Parte 1: Construya la Red

En el simulador construya la red de acuerdo con la topología lógica que se plantea en la figura 1, cable conforme se indica en la topología, y conecte los equipos de cómputo.

Figura 2 - Topología implementada en Packet Tracer



Fuente: propia

Parte 2: Desarrolle el esquema de direccionamiento IP

Desarrolle el esquema de direccionamiento IP. Para la dirección IPv4 cree las dos subredes con la cantidad requerida de hosts. Asigne las direcciones de acuerdo con los requisitos mencionados en la tabla de direccionamiento.

Cada estudiante tomará el direccionamiento 192.168.X.0 donde X corresponde a los últimos dos dígitos de su cédula.

Tabla de direccionamiento

Tabla 1- Tabla de direccionamiento

Item	**Requerimiento**
Dirección de Red	192.168.79.0
Requerimiento de host Subred LAN1	100
Requerimiento de host Subred LAN2	50
R1 G0/0/1	Primera dirección de host de la subred LAN1
R1 G0/0/0	Primera dirección de host de la subred LAN2
S1 SVI	Segunda dirección de host de la subred LAN1
PC-A	Última dirección de host de la subred LAN1
PC-B	Última dirección de host de la subred LAN2

Fuente: propia

Parte 3: Configure aspectos básicos

Los dispositivos de red (S1 y R1) se configuran mediante conexión de consola.

Paso 1: configurar los ajustes básicos

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 2- Configuración R1

Tarea	**Especificación**
Desactivar la búsqueda DNS	Router#conf t

Tarea	Especificación
	Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R1
Nombre de dominio	R1(config)#ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	R1(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	R1(config)#line con 0 R1(config-line)#password ciscoconpass R1(config-line)#login R1(config-line)#exit
Establecer la longitud mínima para las contraseñas	R1(config)#security passwords minlength 10
Crear un usuario administrativo en la base de datos local	R1(config)#username admin privilege 15 secret admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	R1(config)#line vty 0 4 R1(config-line)#login local R1(config-line)#exit
Configurar VTY solo aceptando SSH	R1(config)#line vty 0 4 R1(config-line)#transport input ssh R1(config-line)#login local R1(config-line)#exit

Tarea	**Especificación**
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption
Configure un MOTD Banner	R1(config)#banner motd #ACCESO NO AUTORIZADO#
Configurar interfaz G0/0/0	R1(config)#description HACIA PCB R1(config)#int GigabitEthernet0/0/0 R1(config-if)#ip add 192.168.97.1 255.255.255.192 R1(config-if)#no shutdown R1(config-if)#exit
Configurar interfaz G0/0/1	R1(config)#description HACIA S1 R1(config)#int GigabitEthernet0/0/1 R1(config)#192.168.79.1 255.255.255.128 R1(config-if)#no shutdown R1(config-if)#exit
Generar una clave de cifrado RSA	R1(config)#crypto key generate rsa general-keys modulus 1024

Fuente: propia

Las tareas de configuración de S1 incluyen lo siguiente:

Tabla 3 - Configuración S1

Tarea	**Especificación**
Desactivar la búsqueda DNS.	Switch#conf t Switch(config)#no ip domain-lookup
Nombre del switch	Switch(config)#hostname S1
Nombre de dominio	S1(config)#ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	S1(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	S1(config)#line con 0 S1(config-line)#password ciscoconpass S1(config-line)#login S1(config-line)#exit
Crear un usuario administrativo en la base de datos local	S1(config)#username admin privilege 15 secret admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	S1(config)#line vty 0 4 S1(config-line)#login local S1(config-line)#exit
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	S1(config)#line vty 0 4 S1(config-line)#transport input ssh S1(config-line)#login local S1(config-line)#exit

Tarea	Especificación
Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption
Configurar un MOTD Banner	S1(config)#banner motd #ACCESO NO AUTORIZADO#
Generar una clave de cifrado RSA	S1(config)#crypto key generate rsa general-keys modulus 1024
Configurar la interfaz de administración (SVI)	S1(config)#interface vlan 99 S1(config-if)#ip address 192.168.79.2 255.255.255.128 S1(config-if)#no shut S1(config-if)#exit
Configuración del gateway predeterminado	S1(config)#ip default-gateway 192.168.79.1

Fuente: propia

Paso 2. Configurar los equipos

Configure los equipos host PC-A y PC-B conforme a la tabla de direccionamiento, registre las configuraciones de red del host con el comando **ipconfig /all**.

Tabla 4 - Configuración PC-A

PC-A Network Configuration	
Descripción	HACIA S1
Dirección física	0001.429B.E573
Dirección IP	192.168.79.126

PC-A Network Configuration	
Máscara de subred	255.255.255.128
Gateway predeterminado	192.168.79.1

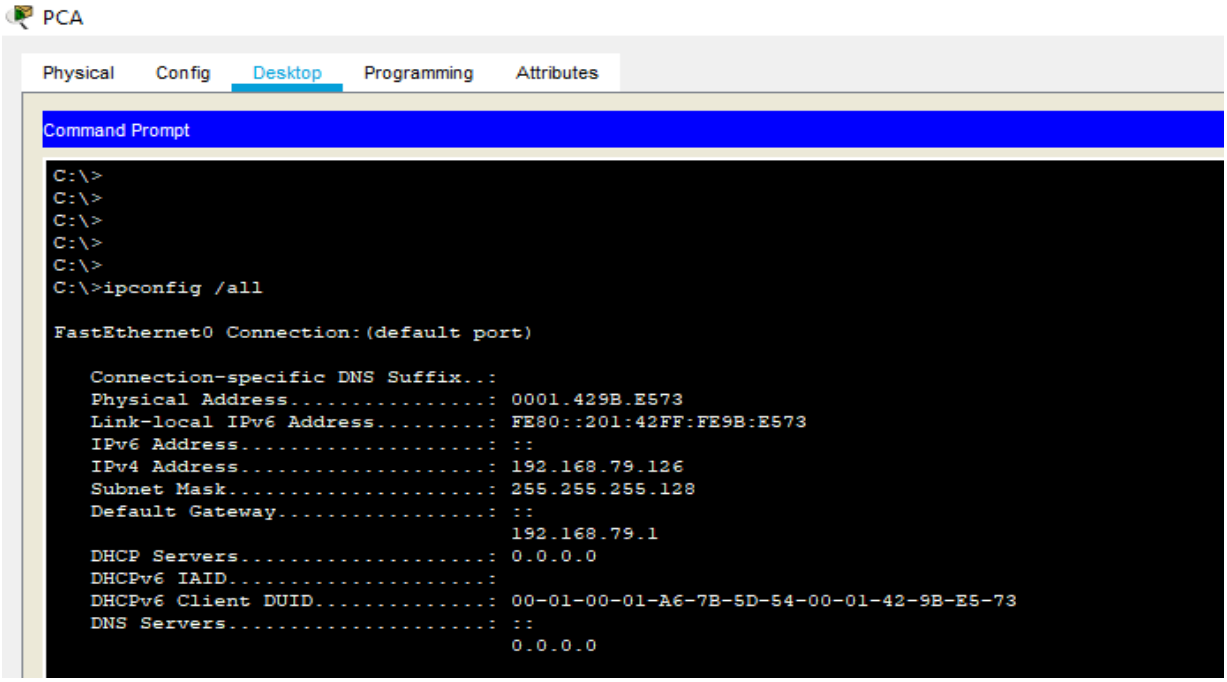
Fuente: propia

Tabla 5 - Configuración PC-B

PC-B Network Configuration	
Descripción	HACIA R1
Dirección física	0000.0CCB.B9A0
Dirección IP	192.168.97.62
Máscara de subred	255.255.255.192

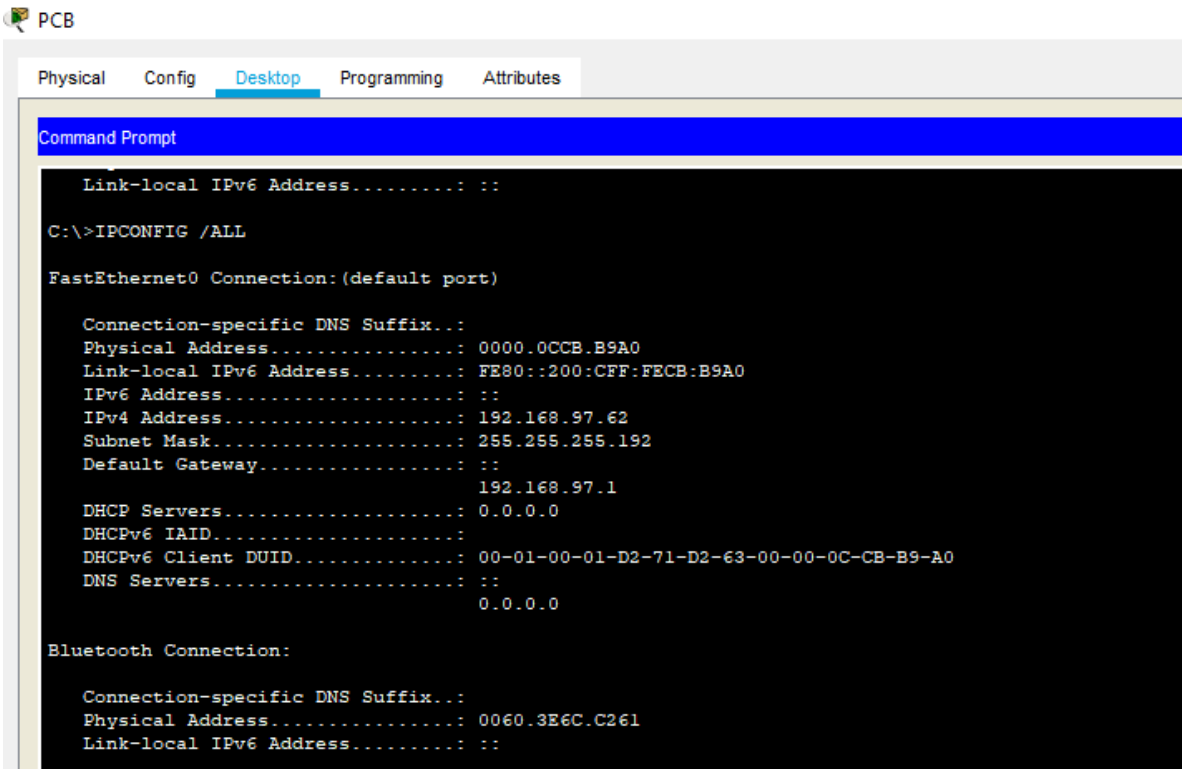
Fuente: propia

Figura 3 - Configuración PC- A en Packet Tracer



Fuente: propia

Figura 4 - Configuración PC- B en Packet Tracer



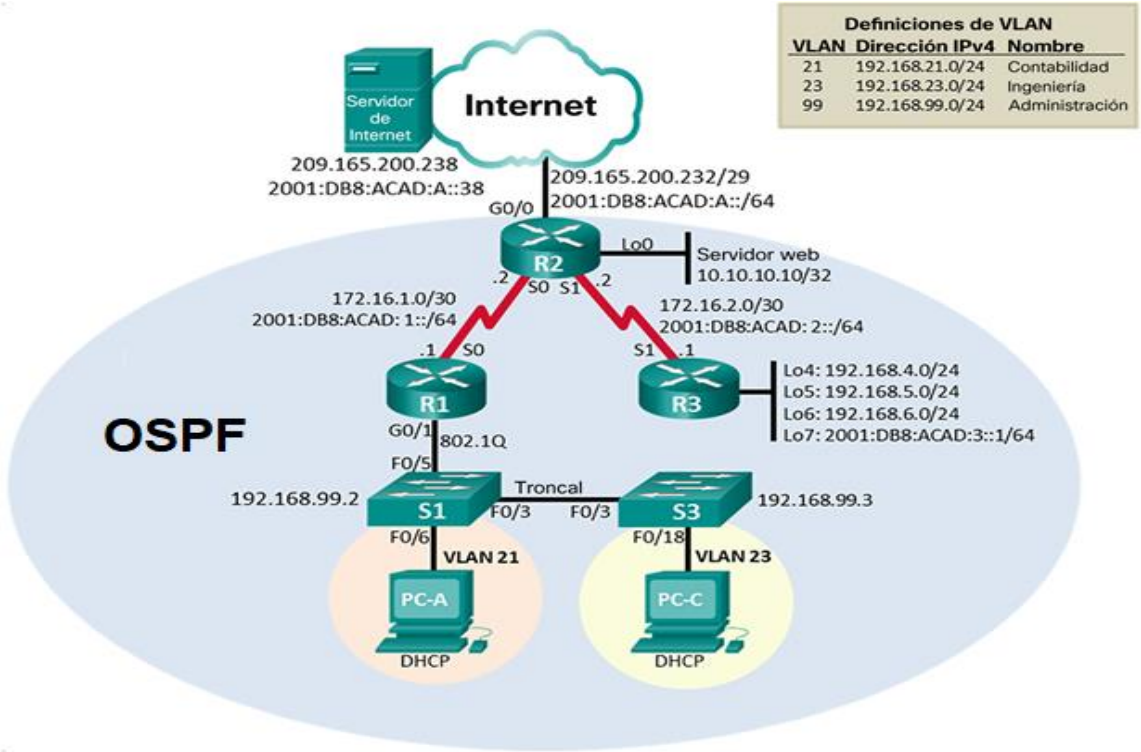
Fuente: Propia

2. Escenario 2

Se debe configurar una red pequeña para que admita conectividad IPv4 e IPv6, seguridad de switches, routing entre VLAN, el protocolo de routing dinámico OSPF, 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

Figura 5 - Topología propuesta escenario 2



Fuente: propia

Parte 1: Inicializar dispositivos

Paso 1: Inicializar y volver a cargar los routers y los switches

Elimine las configuraciones de inicio y vuelva a cargar los dispositivos.

Antes de continuar, solicite al instructor que verifique la inicialización de los dispositivos.

Tabla 6 - Configuración inicialización de dispositivos

Tarea	Comando de IOS
Eliminar el archivo startup-config de todos los routers	#Erase startup-config
Volver a cargar todos los routers	#reload
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	#delete flash:config.text #delete flash:vlan.dat
Volver a cargar ambos switches	#reload
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	#show flash:

Fuente: propia

Parte 2: Configurar los parámetros básicos de los dispositivos

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 7 - Direccionamiento IP

Elemento o tarea de configuración	Especificación
Dirección IPv4	209.165.200.238
Máscara de subred para IPv4	255.255.255.248
Gateway predeterminado	209.165.200.233
Dirección IPv6/subred	2001:DB8:ACAD:A::38/64
Gateway predeterminado IPv6	2001:DB8:ACAD:A::1

Fuente: propia

Nota: Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente en partes posteriores de esta práctica de laboratorio.

Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 8 - Configuración R1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	no ip domain-lookup
Nombre del router	R1
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	service password-encryption
Mensaje MOTD	Se prohíbe el acceso no autorizado.
Interfaz S0/0/0	Establezca la descripción Establecer la dirección IPv4 Consultar el diagrama de topología para conocer la información de direcciones Establecer la dirección IPv6 Consultar el diagrama de topología para conocer la información de direcciones Establecer la frecuencia de reloj en 128000 Activar la interfaz

Elemento o tarea de configuración	Especificación
Rutas predeterminadas	Configurar una ruta IPv4 predeterminada de S0/0/0 Configurar una ruta IPv6 predeterminada de S0/0/0

Fuente: propia

Nota: Todavía no configure G0/1.

Paso 3: Configurar R2

La configuración del R2 incluye las siguientes tareas:

Tabla 9 - Configuración R2

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	no ip domain-lookup
Nombre del router	R2
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	Service password-encryption
Habilitar el servidor HTTP	ip http server (Este commando solo funciona en un router real, en packet tracer no se puede)
Mensaje MOTD	Se prohíbe el acceso no autorizado.

Elemento o tarea de configuración	Especificación
Interfaz S0/0/0	Establezca la descripción Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Activar la interfaz
Interfaz S0/0/1	Establecer la descripción Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Establecer la frecuencia de reloj en 128000. Activar la interfaz
Interfaz G0/0 (simulación de Internet)	Establecer la descripción. Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. Establezca la dirección IPv6. Utilizar la primera dirección disponible en la subred. Activar la interfaz
Interfaz loopback 0 (servidor web simulado)	Establecer la descripción. Establezca la dirección IPv4.
Ruta predeterminada	Configure una ruta IPv4 predeterminada de G0/0. Configure una ruta IPv6 predeterminada de G0/0.

Fuente: propia

Paso 4: Configurar R3

La configuración del R3 incluye las siguientes tareas:

Tabla 10- Configuración R3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	no ip domain-lookup
Nombre del router	R3
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	Service password-encryption
Mensaje MOTD	Se prohíbe el acceso no autorizado.
Interfaz S0/0/1	Establecer la descripción Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Activar la interfaz
Interfaz loopback 4	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.
Interfaz loopback 5	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.
Interfaz loopback 6	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.

Elemento o tarea de configuración	Especificación
Interfaz loopback 7	Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones.
Rutas predeterminadas	

Fuente: propia

Paso 5: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 11 - Configuración S1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	no ip domain-lookup
Nombre del switch	S1
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	Service password-encryption
Mensaje MOTD	Se prohíbe el acceso no autorizado.

Fuente: Propia

Paso 6: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 12 - Configuración S3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	no ip domain-lookup

Elemento o tarea de configuración	Especificación
Nombre del switch	S3
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	Service password-encryption
Mensaje MOTD	Se prohíbe el acceso no autorizado.

Fuente: propia

Paso 7: Verificar la conectividad de la red

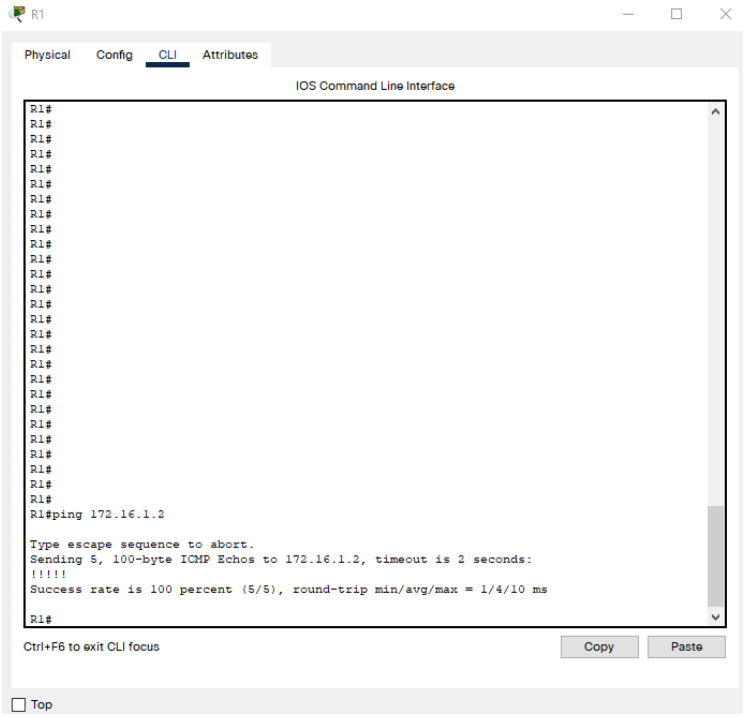
Utilice el comando **ping** para probar la conectividad entre los dispositivos de red.

Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Tabla 13 - Verificación conectividad

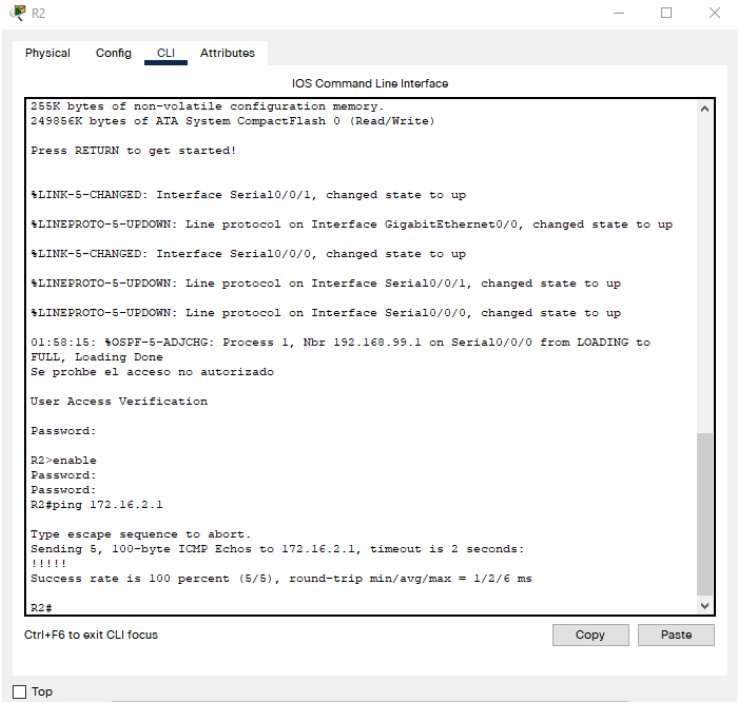
Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.2	Exitoso
R2	R3, S0/0/1	172.16.2.1	Exitoso
PC de Internet	Gateway predeterminado	209.165.200.225	Este ping no es exitoso debido a que no hace parte del segmento y hubo necesidad de modificar la dirección IP por la 209.165.200.238, al anterior indicada en la topología.

Figura 6 - Ping R1 a 172.16.1.2 _Exitoso



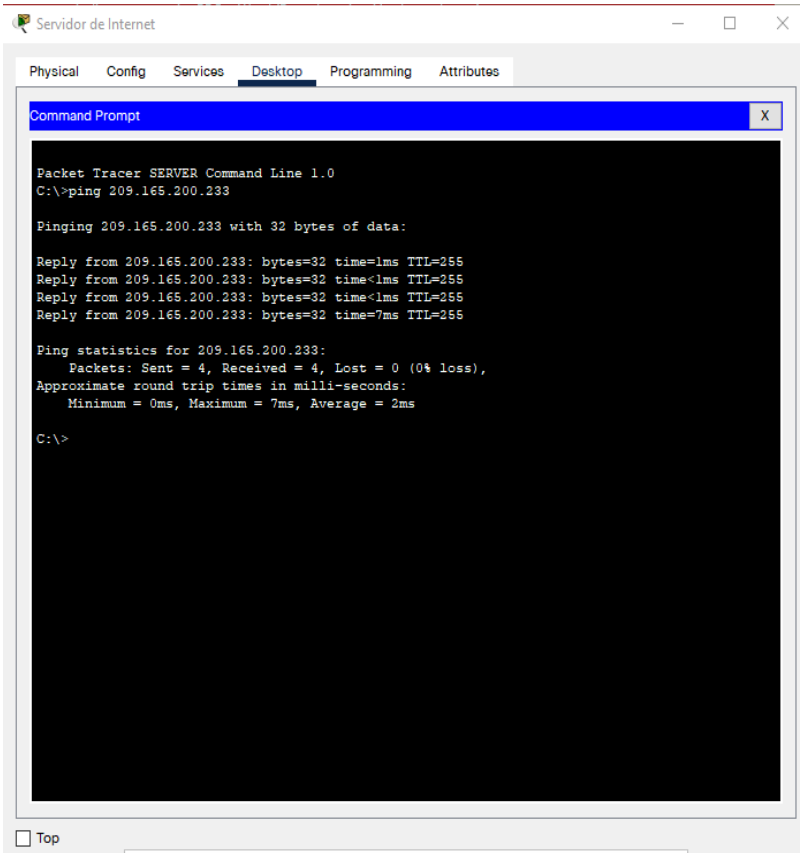
Fuente: propia

Figura 7 - Ping R2 a 172.16.2.1 _Exitoso



Fuente: propia

Figura 8 - Ping a Gateway predeterminado IP 209.165.200.233



Fuente: propia

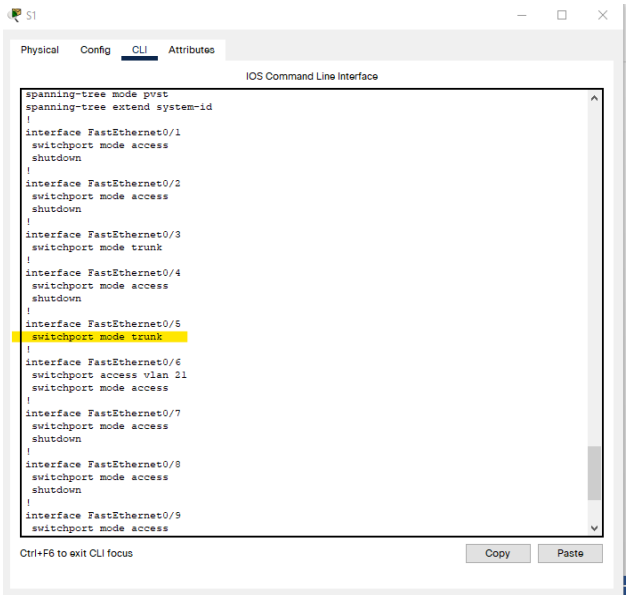
Nota: Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente.

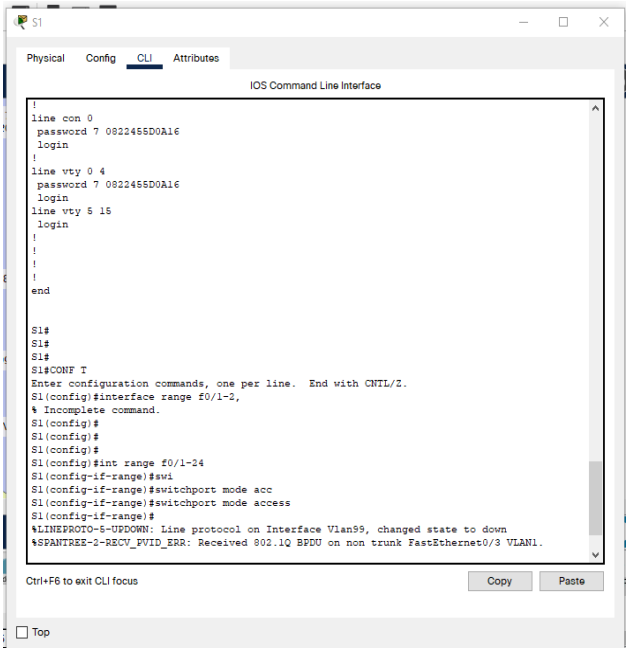
Parte 3: Configurar la seguridad del switch, las VLAN y el routing entre VLAN

Paso 1: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 14 -Configuración S1

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	Utilizar la tabla de equivalencias de VLAN para topología para crear y nombrar cada una de las VLAN que se indican
Asignar la dirección IP de administración.	Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S1 en el diagrama de topología
Asignar el gateway predeterminado	Asigne la primera dirección IPv4 de la subred como el gateway predeterminado.
Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN native
Forzar el enlace troncal en la interfaz F0/5	Utilizar la red VLAN 1 como VLAN native S1(config)#int ran S1(config)#int range f0/3,f0/5 S1(config-if-range)#switch S1(config-if-range)#switchport mode trunk 

Elemento o tarea de configuración	Especificación
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range S1(config)#int range f0/1-24 S1(config-if-range)#swi S1(config-if-range)#switchport mode acc S1(config-if-range)#switchport mode access 
Asignar F0/6 a la VLAN 21	Switchport access vlan 21 interface FastEthernet0/6 switchport access vlan 21 switchport mode access
Apagar todos los puertos sin usar	shutdown

Plantilla de configuración S1	S1#sh run Building configuration... Current configuration : 2153 bytes version 12.2 no service timestamps log datetime msec no service timestamps debug datetime msec service password-encryption hostname S1 enable secret 5 1mERr$9cTjUIEqNGurQiFU.ZeCi1 no ip domain-lookup spanning-tree mode pvst spanning-tree extend system-id interface FastEthernet0/1 switchport mode access shutdown interface FastEthernet0/2 switchport mode access shutdown interface FastEthernet0/3 switchport mode trunk interface FastEthernet0/4 switchport mode access shutdown interface FastEthernet0/5 switchport mode trunk interface FastEthernet0/6 switchport access vlan 21 switchport mode access interface FastEthernet0/7 switchport mode access shutdown interface FastEthernet0/8 switchport mode access shutdown interface FastEthernet0/9 switchport mode access shutdown interface FastEthernet0/10 switchport mode access shutdown interface FastEthernet0/11 switchport mode access shutdown

	interface FastEthernet0/12 switchport mode access shutdown interface FastEthernet0/13 switchport mode access shutdown interface FastEthernet0/14 switchport mode access shutdown interface FastEthernet0/15 switchport mode access shutdown interface FastEthernet0/16 switchport mode access shutdown interface FastEthernet0/17 switchport mode access shutdown interface FastEthernet0/18 switchport mode access shutdown interface FastEthernet0/19 switchport mode access shutdown interface FastEthernet0/20 switchport mode access shutdown interface FastEthernet0/21 switchport mode access shutdown interface FastEthernet0/22 switchport mode access shutdown interface FastEthernet0/23 switchport mode access shutdown interface FastEthernet0/24 switchport mode access shutdown interface GigabitEthernet0/1 interface GigabitEthernet0/2 interface Vlan1 no ip address shutdown

Elemento o tarea de configuración	Especificación
	interface Vlan99 ip address 192.168.99.2 255.255.255.0 ip default-gateway 192.168.99.1 banner motd ^C Se prohbe el acceso no autorizado. ^C line con 0 password 7 0822455D0A16 login line vty 0 4 password 7 0822455D0A16 login line vty 5 15 login end

Fuente: propia

Paso 2: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 15 - Configuración S3

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	Utilizar la tabla de equivalencias de VLAN para topología para crear cada una de las VLAN que se indican Dé nombre a cada VLAN.
Asignar la dirección IP de administración	Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S3 en el diagrama de topología
Asignar el gateway predeterminado.	Asignar la primera dirección IP en la subred como gateway predeterminado.
Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN nativa

Plantilla de configuración S3	R3#show run Building configuration... Current configuration : 1675 bytes! version 15.1 no service timestamps log datetime msec no service timestamps debug datetime msec service password-encryption !hostname R3 enable secret 5 1mERr$9cTjUIEqNGurQiFU.ZeCi1 no ip cef ipv6 unicast-routing no ipv6 cef license udi pid CISCO2911/K9 sn FTX1524TTRW- spanning-tree mode pvst interface Loopback4 ip address 192.168.4.1 255.255.255.0 ip nat inside interface Loopback5 ip address 192.168.5.1 255.255.255.0 ip nat inside interface Loopback6 ip address 192.168.6.1 255.255.255.0 ip nat inside interface Loopback7 no ip address

	ipv6 address 2001:DB8:ACAD:3::1/64 ipv6 enable interface GigabitEthernet0/0 no ip address duplex auto speed auto shutdown interface GigabitEthernet0/1 no ip address duplex auto speed auto shutdown interface GigabitEthernet0/2 no ip address duplex auto speed auto shutdown interface Serial0/0/0 no ip address clock rate 2000000 shutdown interface Serial0/0/1 description CONEXION_CON_R2 ip address 172.16.2.1 255.255.255.252 ip nat outside ipv6 address 2001:DB8:ACAD:2::1/64 ipv6 enable

Elemento o tarea de configuración	Especificación
	interface Vlan1 no ip address shutdown ip nat pool INTERNET 209.165.200.227 209.165.200.228 netmask 255.255.255.248 ip classless ip route 0.0.0.0 0.0.0.0 Serial0/0/1 ip flow-export version 9 ipv6 route ::/0 Serial0/0/1 access-list 1 permit 192.168.4.0 0.0.0.255 access-list 1 permit 192.168.5.0 0.0.0.255 access-list 1 permit 192.168.6.0 0.0.0.255 banner motd ^C Se prohbe el acceso no autorizado ^C line con 0 password 7 0822455D0A16 login line aux 0 line vty 0 4 password 7 0822455D0A16 login end

Fuente: propia

Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 16 - Configuración R1

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1	Descripción: LAN de Contabilidad Asignar la VLAN 21 Asignar la primera dirección disponible a esta interfaz
Configurar la subinterfaz 802.1Q .23 en G0/1	Descripción: LAN de Ingeniería Asignar la VLAN 23 Asignar la primera dirección disponible a esta interfaz
Configurar la subinterfaz 802.1Q .99 en G0/1	Descripción: LAN de Administración Asignar la VLAN 99 Asignar la primera dirección disponible a esta interfaz
Activar la interfaz G0/1	No shutdown
Plantilla de configuración R1	R1#show run Building configuration... Current configuration : 2541 bytes version 15.1 no service timestamps log datetime msec no service timestamps debug datetime msec service password-encryption hostname R1 enable secret 5 1mERr$9cTjUIEqNGurQiFU.ZeCi1 ip dhcp excluded-address 192.168.21.1 192.168.21.20 ip dhcp excluded-address 192.168.23.1 192.168.23.20 ip dhcp pool ACCT network 192.168.21.0 255.255.255.0 default-router 192.168.21.1 dns-server 10.10.10.10 domain-name ccna-sa.com ip dhcp pool ENGNR network 192.168.23.0 255.255.255.0 default-router 192.168.23.1 dns-server 10.10.10.10 domain-name WR ip cef ipv6 unicast-routing

Elemento o tarea de configuración	Especificación
	no ipv6 cef license udi pid CISCO2911/K9 sn FTX1524I2YB- no ip domain-lookup spanning-tree mode pvst interface GigabitEthernet0/0 no ip address duplex auto speed auto shutdown interface GigabitEthernet0/1 no ip address ip nat inside duplex auto speed auto interface GigabitEthernet0/1.21 description CONTABILIDAD encapsulation dot1Q 21 ip address 192.168.21.1 255.255.255.0 ip nat inside interface GigabitEthernet0/1.23 description INGENIERIA encapsulation dot1Q 23 ip address 192.168.23.1 255.255.255.0 ip nat inside interface GigabitEthernet0/1.99 description ADMINISTRACION encapsulation dot1Q 99 ip address 192.168.99.1 255.255.255.0 interface GigabitEthernet0/2 no ip address duplex auto speed auto shutdown interface Serial0/0/0 description CONEXION_CON_R2 ip address 172.16.1.1 255.255.255.252 ip nat outside ipv6 address 2001:DB8:ACAD:1::1/64

Elemento o tarea de configuración	Especificación
	ipv6 enable clock rate 128000 interface Serial0/0/1 no ip address clock rate 2000000 shutdown interface Vlan1 no ip address shutdown router ospf 1 log-adjacency-changes passive-interface GigabitEthernet0/1 passive-interface GigabitEthernet0/1.21 passive-interface GigabitEthernet0/1.23 passive-interface GigabitEthernet0/1.99 network 192.168.21.0 0.0.0.255 area 0 network 192.168.23.0 0.0.0.255 area 0 network 192.168.99.0 0.0.0.255 area 0 network 172.16.1.0 0.0.0.3 area 0 ip nat pool INTERNET 209.165.200.225 209.165.200.226 netmask 255.255.255.252 ip classless ip route 0.0.0.0 0.0.0.0 Serial0/0/0 ip flow-export version 9 ipv6 route ::/0 Serial0/0/0 access-list 1 permit 192.168.21.0 0.0.0.255 access-list 1 permit 192.168.23.0 0.0.0.255 banner motd ^C Se prohbe el acceso no autorizado ^C line con 0 password 7 0822455D0A16 login line aux 0 line vty 0 4 password 7 0822455D0A16 login transport input telnet

Elemento o tarea de configuración	Especificación
	ntp server 172.16.1.2 ntp update-calendar end

Fuente: propia

Paso 4: Verificar la conectividad de la red

Utilice el comando **ping** para probar la conectividad entre los switches y el R1.

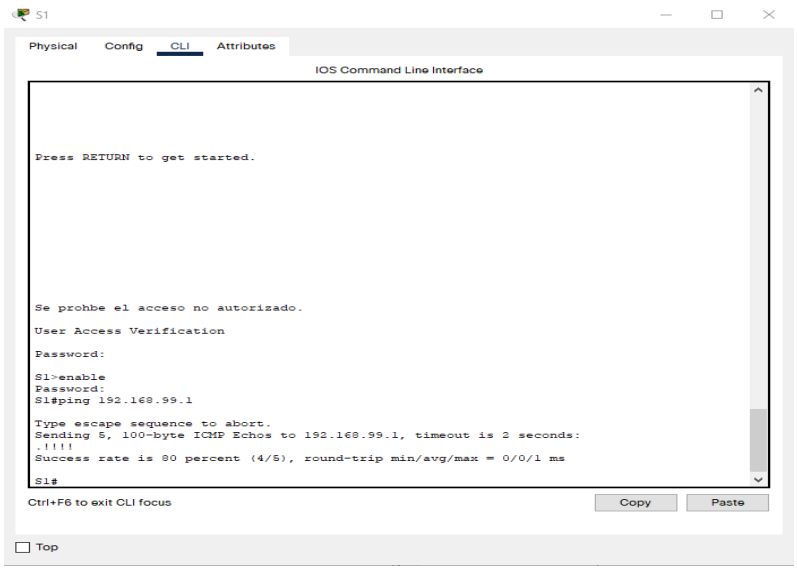
Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Tabla 17 - Verificación conectividad

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

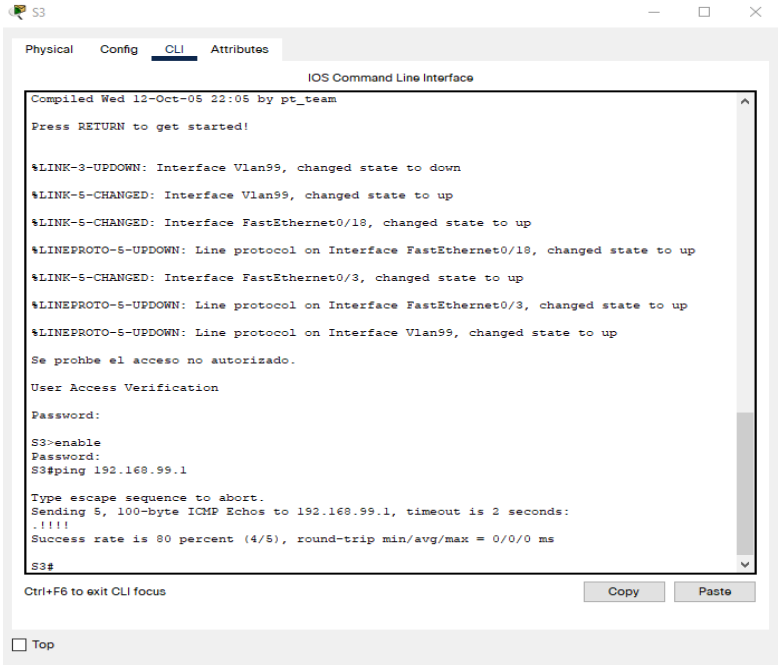
Fuente: propia

Figura 9 - Ping exitoso de S1 a VLAN 99



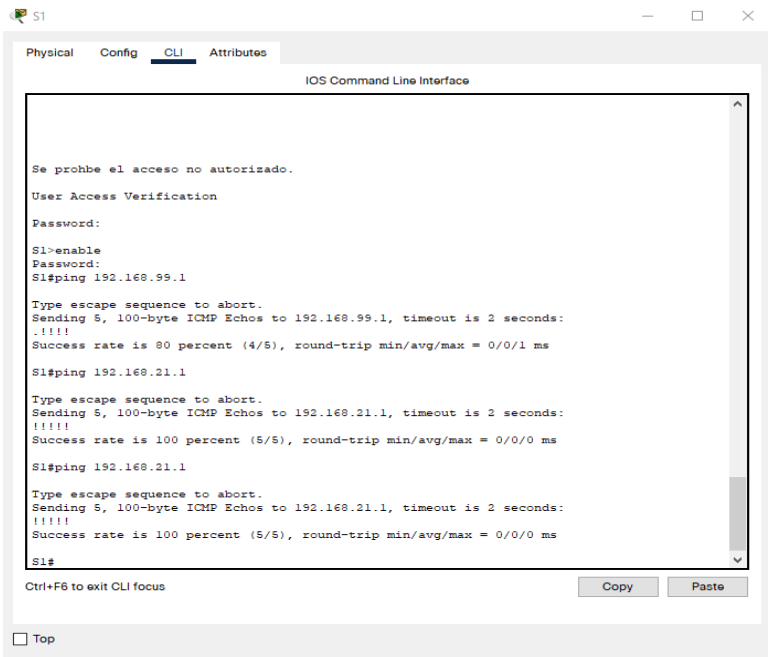
Fuente: propia

Figura 10 - Ping exitoso de S3 a VLAN 99



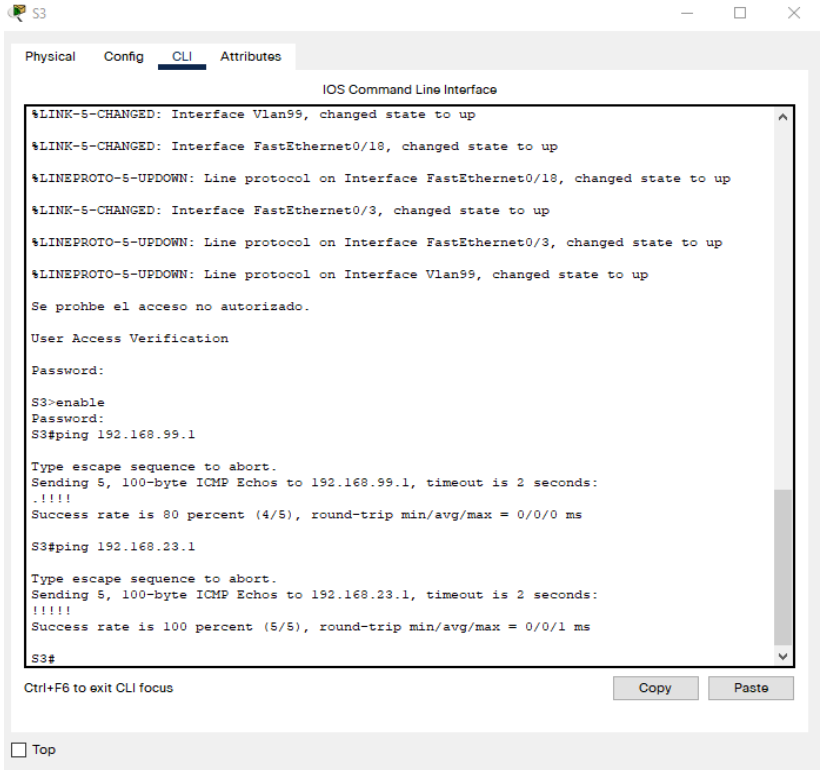
Fuente: propia

Figura 11 - Ping exitoso de S1 a VLAN 21



Fuente: propia

Figura 12 - Ping exitoso de S3



Fuente: propia

Parte 4: Configurar el protocolo de routing dinámico OSPF

Paso 1: Configurar OSPF en el R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 18 - Configuración OSPF en R1

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	router ospf 1 network 192.168.21.0 0.0.0.255 area 0 network 192.168.23.0 0.0.0.255 area 0 network 192.168.99.0 0.0.0.255 area 0 network 172.16.1.0 0.0.0.3 area 0
Anunciar las redes conectadas directamente	Asigne todas las redes conectadas directamente.
Establecer todas las interfaces LAN como pasivas	passive-interface GigabitEthernet0/1 passive-interface GigabitEthernet0/1.21 passive-interface GigabitEthernet0/1.23 passive-interface GigabitEthernet0/1.99
Desactive la sumarización automática	R1(config-router)#no auto-summary

Fuente: propia

Paso 2: Configurar OSPF en el R2

La configuración del R2 incluye las siguientes tareas:

Tabla 19 - Configuración OSPF en R2

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	router ospf 1 network 172.16.1.0 0.0.0.3 area 0 network 172.16.2.0 0.0.0.3 area 0
Anunciar las redes conectadas directamente	**Nota:** Omitir la red G0/0.
Establecer la interfaz LAN (loopback) como pasiva	passive-interface Loopback0
Desactive la sumarización automática.	R2(config-router)#no auto-summary.

Fuente: propia

Paso 3: Configurar OSPFv3 en el R2

La configuración del R3 incluye las siguientes tareas:

Tabla 20 - Configuración OSPFv3 en R2

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	ipv6 router ospf 1 router-id 1.1.1.1
Anunciar redes IPv4 conectadas directamente	interface Serial0/0/0 ipv6 ospf 1 area 0 interface Serial0/0/1 ipv6 ospf 1 area 0
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	passive-interface Loopback0

Elemento o tarea de configuración	Especificación
Desactive la sumarización automática.	R3(config-router)#no auto-summary

Fuente: propia

Paso 4: Verificar la información de OSPF

Verifique que OSPF esté funcionando como se espera. Introduzca el comando de CLI adecuado para obtener la siguiente información:

Tabla 21 - Verificación de OSPF

Pregunta	Respuesta
¿Con qué comando se muestran la ID del proceso OSPF, la ID del router, las redes de routing y las interfaces pasivas configuradas en un router?	Show ip ospf database show ip route show run
¿Qué comando muestra solo las rutas OSPF?	Show ip ospf neighbor
¿Qué comando muestra la sección de OSPF de la configuración en ejecución?	show run | section router ospf

Fuente: propia

Parte 5: Implementar DHCP y NAT para IPv4

Paso 1: Configurar el R1 como servidor de DHCP para las VLAN 21 y 23

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 22 - Configuración R1 como servidor de DHCP

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	ip dhcp excluded-address 192.168.23.1 192.168.23.20
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	ip dhcp excluded-address 192.168.23.1 192.168.23.20

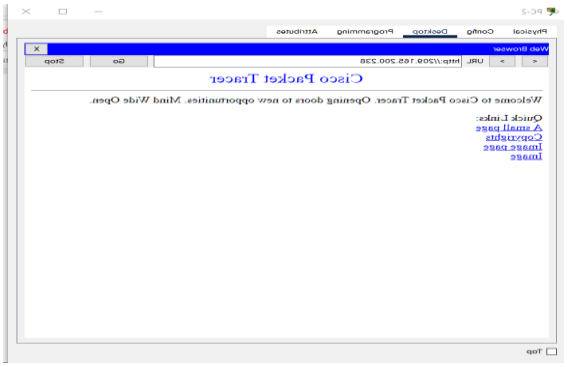
Elemento o tarea de configuración	Especificación
Crear un pool de DHCP para la VLAN 21.	Nombre: ACCT Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el gateway predeterminado
Crear un pool de DHCP para la VLAN 23	Nombre: ENGNR Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el gateway predeterminado

Fuente: propia

Paso 2: Configurar la NAT estática y dinámica en el R2

La configuración del R2 incluye las siguientes tareas:

Tabla 23 - Configuración de la NAT estática y dinámica en el R2

Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario	Nombre de usuario: **webuser** Contraseña: **cisco12345** Nivel de privilegio: **15**
Habilitar el servicio del servidor HTTP	R2(config)#ip http server 

Elemento o tarea de configuración	Especificación
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	R2#ip http authentication local
Crear una NAT estática al servidor web.	Dirección global interna: **209.165.200.229**
Asignar la interfaz interna y externa para la NAT estática	interface GigabitEthernet0/0 ip nat inside interface Serial0/0/0 ip nat outside interface Serial0/0/1 ip nat outside
Configurar la NAT dinámica dentro de una ACL privada	Lista de acceso: 1 Permitir la traducción de las redes de Contabilidad y de Ingeniería en el R1 Permitir la traducción de un resumen de las redes LAN (loopback) **en** el R3
Defina el pool de direcciones IP públicas utilizables.	Nombre del conjunto: **INTERNET** El conjunto de direcciones incluye: **209.165.200.225** – **209.165.200.228**
Definir la traducción de NAT dinámica	**R1:** ip nat pool INTERNET 209.165.200.225 209.165.200.226 netmask 255.255.255.252 **R2**: ip nat pool INTERNET 209.165.200.227 209.165.200.228 netmask 255.255.255.248

Fuente: propia

Paso 3: Verificar el protocolo DHCP y la NAT estática

Utilice las siguientes tareas para verificar que las configuraciones de DHCP y NAT estática funcionen de forma correcta. Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente.

Tabla 24 - Verificación del protocolo DHCP

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	Ping exitoso
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	Ping exitoso
Verificar que la PC-A pueda hacer ping a la PC-C **Nota:** Quizá sea necesario deshabilitar el firewall de la PC.	Ping exitoso
Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.229) Iniciar sesión con el nombre de usuario **webuser** y la contraseña **cisco12345**	Podemos observar el servidor pero el anterior no solicita credencial de acceso esto se debe a que la solicitud de configuración es para un caso real y no una simulación en Packet Tracer.

Fuente: propia

Parte 6: Configurar NTP

Tabla 25 - Configuración NTP

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	**5 de marzo de 2016, 9 a. m.**
Configure R2 como un maestro NTP.	Nivel de estrato: **5**
Configurar R1 como un cliente NTP.	Servidor: **R2**

Elemento o tarea de configuración	Especificación
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	Ntp update-calendar
Verifique la configuración de NTP en R1.	Show running-config

Fuente: propia

Parte 7: Configurar y verificar las listas de control de acceso (ACL)

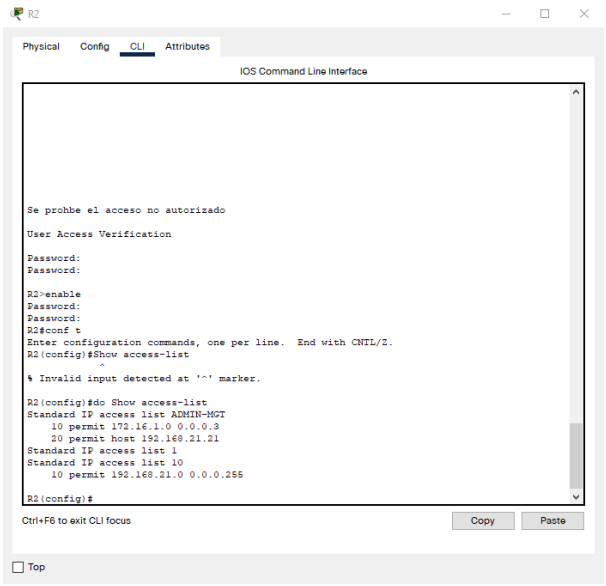
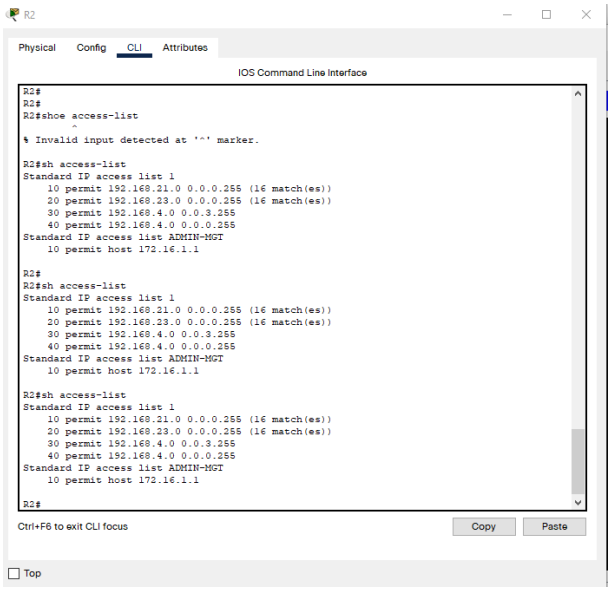
Paso 1: Restringir el acceso a las líneas VTY en el R2

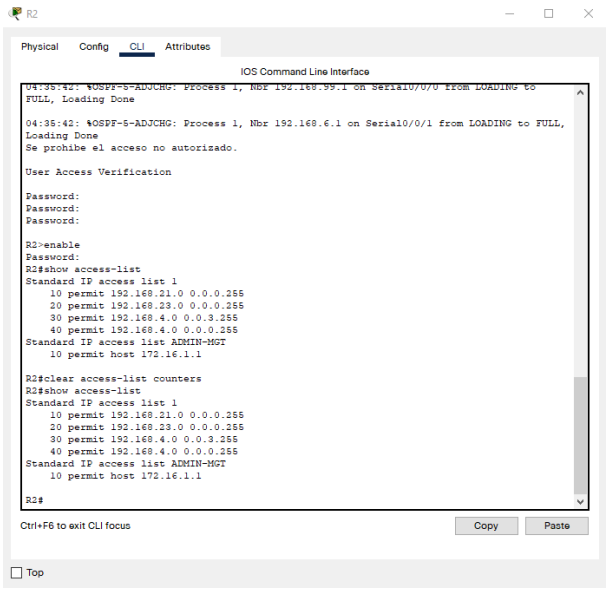
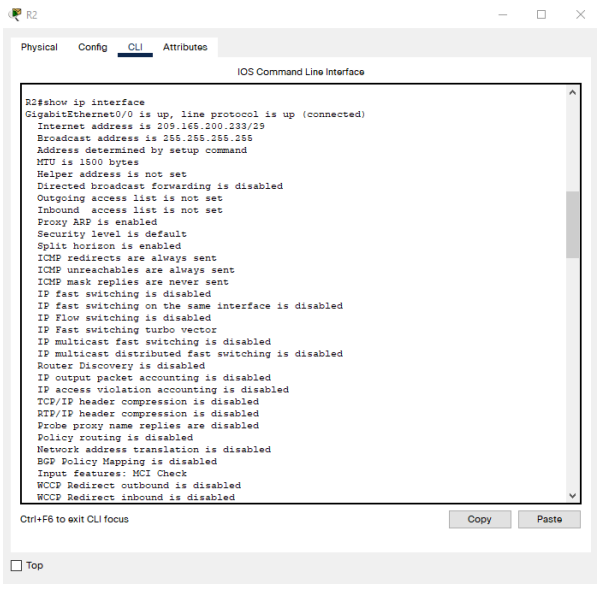
Tabla 26 - Restrincción de acceso a las líneas VTY en R2

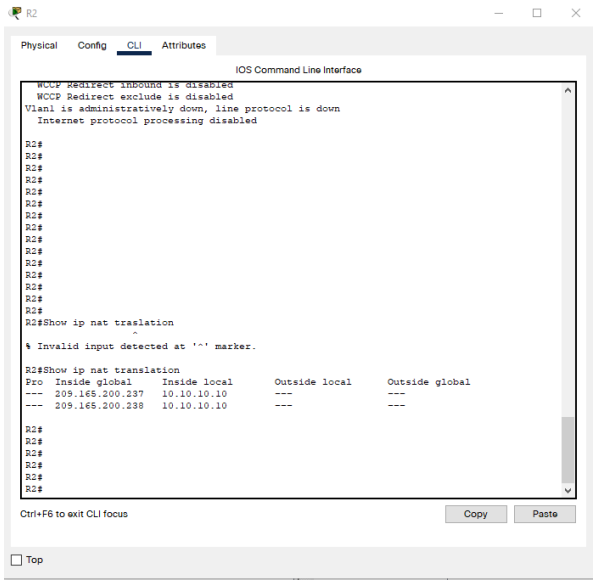
Elemento o tarea de configuración	Especificación
Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2	Nombre de la ACL: **ADMIN-MGT**
Aplicar la ACL con nombre a las líneas VTY	Line vty 0 4 Access-class ADMIN-MGT in
Permitir acceso por Telnet a las líneas de VTY	Line vty 0 4 transport input telnet
Verificar que la ACL funcione como se espera	Funciona correctamente.

Fuente: propia

Paso 2: Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente

Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	Show access-list  

Descripción del comando	Entrada del estudiante (comando)
Restablecer los contadores de una lista de acceso	clear access-list counters 
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	show ip interface 

Descripción del comando	Entrada del estudiante (comando)
¿Con qué comando se muestran las traducciones NAT?	Show ip nat translation 
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	clear ip nat translation *

Fuente: propia

CONCLUSIONES

Después de desarrollar y aprender los contenidos propuestos en el diplomado de profundización de CISCO CCNA, se puede comprender de una manera mas apropiada el termino de conmutación de redes, la cual es una interconexión de equipos en cojunto, conectados por medio de los distintos protocolos que exiten y se adapten a la necesidad del caso.

Mediante el uso de la herramienta Packet Tracer, podemos simular las distintas configuraciones según los casos propuestos por el cliente, con el fin de documentar cada uno de lo casos planteados para la implementación, obteniendo un la trazabilidad de su funcionalidad por medio de pruebas de de conectividad entre los dispositivos.

Este diplomado nos permitió afianzar nuestras competencias para realizar implementaciones de soluciones básicas en el campo de la configuración de redes de datos. Estas actividades se asemejan a la realidad, las cuales nos proyectan a elegir este campo profesional.

BIBLIOGRAFÍA

BAREÑO, Gutiérrez, R., Sevillano, A. M. L., Díaz-Piraquive, F. N., & González-Crespo, R. (2021, July). Analysis of WEB Browsers of HSTS Security Under the MITM 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 dinámico como RIPNG, EIGRP y OSPF basado sobre la plataforma de equipos cisco.
BAREÑO Raúl, G., & Sevillano, A. M. L. (2017, October). Services cloud under HSTS, 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.

CISCO. (2019). Ethernet. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#5

CISCO. (2019). Acceso a la red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#4

CISCO. (2019). Exploración de la red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#1

CISCO. (2019). Configuración de un sistema operativo de red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#2

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 in Electronic Payment Cards on Integrated Public Transport System Applying the ISO

27005 Standard. Case Study Sitp DC Colombia. In 2019 Congreso Internacional de Innovación y Tendencias en Ingenieria (CONIITI) (pp. 1-6). IEEE.

Vesga, J. (2014). Diseño y configuración de redes con Packet Tracer [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgCT9VCtl_pLtPD9

CISCO. (2019). Protocolos y comunicaciones de red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#3

Vesga, J. (2017). Ping y Tracer como estrategia en los procesos de Networking [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgTCtKY-7F5KIRC3