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

EDWIN AUGUSTO VIRGUEZ VANEGAS

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD.
FACULTAD DE CIENCIAS BASICAS TECNOLOGIA E INGENIERIA
Facatativá
NOVIEMBRE 30 DEL 2020.

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

EDWIN AUGUSTO VIRGUEZ AUGUSTO

DIPLOMADO DE OPCION DE GRADO PRESENTADO PARA OPTAR POR EL TITULO DE INGENIERO DE SISTEMAS

DIEGO EDINSON RAMIREZ CLAROS
TUTOR

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD.
FACULTAD DE CIENCIAS BASICAS TECNOLOGIA E INGENIERIA
Facatativá
NOVIEMBRE 30 DEL 2020

Ciudad: Facatativá (Cundinamarca) noviembre 30 del 2020.

Nota de aceptación.

_____
_____
_____
_____
_____

Firma del Presidente del Jurado.

Firma del Jurado.

Firma del Jurado.

Desde que comencé con este proceso formativo, en primer lugar, debo agradecer a mi madre que me ha dado la fuerza y el apoyo incondicional, otro eje fundamental en este largo y arduo camino son mi esposa e hija que todos los días tengo el respaldo y el motivo de luchar cada día para poder cumplir mis metas.

También quiero agradecer a la UNAD por darnos los espacios y la oportunidad de pertenecer y ser egresado de esta prestigiosa entidad educativa.

EDWIN AUGUSTO VIRGUEZ

AGRADECIMIENTOS

Le agradezco inicialmente a la UNAD por todo ese compromiso que ha adquirido con las personas que tienen algún tipo de dificultad o menos favorecidas por habernos brindado esa posibilidad y oportunidad de podernos superar y formarnos como unas personas íntegras dentro de nuestras ramas del saber.

Les agradezco enormemente a los TUTORES por ser parte íntegra de nuestra formación por estar constantemente acompañándonos en este proceso y siempre contar con el apoyo de cada uno de ellos en el desarrollo de las actividades.

A todo el personal de la universidad que directa o indirectamente nos colaboraron para cumplir con nuestros quehaceres.

A todos mis compañeros por el compartir, aceptar y apoyar cada una de las actividades propuestas.

CONTENIDO

TABLA DE FIGURAS

LISTA DE TABLAS

GLOSARIO

En esta sección se relacionan todos los conceptos dejando claro la teoría que se siguió como modelo de la realidad de los estudios de caso de redes que son el tema de investigación en este trabajo.

Cable coaxial:

Es un cable utilizado para transportar señales eléctricas de alta frecuencia que posee dos conductores concéntricos, uno central, llamado vivo, encargado de llevar la información, y uno exterior, de aspecto tubular, llamado malla o blindaje, que sirve como referencia de tierra y retorno de las corrientes. Entre ambos se encuentra una capa aislante llamada dieléctrico, de cuyas características dependerá principalmente la calidad del cable. Todo el conjunto suele estar protegido por una cubierta aislante.

Cable de fibra óptica:

Es un medio de transmisión empleado habitualmente en redes de datos; un hilo muy fino de material transparente, vidrio o materiales plásticos, por el que se envían pulsos de luz que representan los datos a transmitir. El haz de luz queda completamente confinado y se propaga por el interior de la fibra con un ángulo de reflexión por encima del ángulo límite de reflexión total, en función de la ley de Snell. La fuente de luz puede ser láser o un LED.

Cable de par trenzado:

Es una forma de conexión en la que dos conductores son entrelazados para cancelar las interferencias electromagnéticas (IEM) de fuentes externas y la diafonía de los cables adyacentes.

Direcciones IP:

Es una etiqueta numérica que identifica, de manera lógica y jerárquica, a un interfaz (elemento de comunicación/conexión) de un dispositivo (habitualmente una computadora) dentro de una red que utilice el protocolo IP (Internet Protocol), que corresponde al nivel de red del protocolo TCP/IP. Dicho número no se ha de confundir con la dirección MAC que es un identificador de 48bits para identificar de forma única a la tarjeta de red y no depende del protocolo de conexión utilizado ni de la red

Dirección IP dinámica:

Es una IP asignada mediante un servidor DHCP (Dynamic Host Configuration Protocol) al usuario.

Dirección IP fija:

Es una IP asignada por el usuario de manera manual.

DNS server:

Consiste en un conjunto jerárquico de **servidores DNS**. Cada dominio o subdominio tiene una o más **zonas de autoridad** que publican la información acerca del dominio y los nombres de servicios de cualquier dominio incluido

Ethernet:

El nombre Ethernet viene del concepto físico de *ether*. En su momento el prefijo *fast* se le agregó para diferenciarla de la versión original Ethernet de 10 Mbps.

Fastethernet:

Es el nombre de una serie de estándares de IEEE de redes

Gateway: (puerta de enlace):

Es un dispositivo, con frecuencia un ordenador, que permite

interconectar redes con protocolos y arquitecturas diferentes a todos los niveles de comunicación. Su propósito es traducir la información del protocolo utilizado en una red al protocolo usado en la red de destino.

Host: Un **host o anfitrión:**
Es un ordenador que funciona como el punto de inicio y final de las transferencias de datos. Más comúnmente descrito como el lugar donde reside un sitio web.

IOS:
Son las siglas de Internetwork Operating System, (Sistema Operativo de Interconexión de Redes) sistema operativo creado por Cisco Systems para programar y mantener equipos de interconexión de redes informáticas como switches (conmutadores) y routers (enrutadores).

LAN red de área local (del inglés **Local Área Network**):
Es la interconexión de varios ordenadores y periféricos. Su extensión esta limitada físicamente a un edificio o a un entorno de 200 metros o con repetidores podríamos llegar a la distancia de un campo de 1 kilómetro. Su aplicación más extendida es la interconexión de ordenadores personales y estaciones de trabajo en oficinas, fábricas, etc., para compartir Recursos e intercambiar datos y aplicaciones.

WAN:
Una Red de Área Amplia (Wide Área Network o WAN, del inglés), es un tipo de red de computadoras capaz de cubrir distancias desde unos 100km hasta unos 1000 km, dando el servicio a un país o un continente.

Loopback:
Es un interfaz de red virtual que siempre representa al propio dispositivo

independientemente de la dirección IP que se le haya asignado. El valor en IPv4 es 127.0.0.1 y :: 1 para el caso de IPv6.

Mascara de subred:

La máscara permite distinguir los bits que identifican la red y los que identifican el host de una dirección IP.

Modelo OSI:

Es un lineamiento funcional para tareas de comunicaciones y, por consiguiente, no especifica un estándar de comunicación para dichas tareas. Sin embargo, muchos estándares y protocolos cumplen con los lineamientos del Modelo OSI.

Modo de router:

Para configurar los parámetros de uno de los protocolos de enrutamiento

OSPF: (Open Shortest Path First)

Frecuentemente abreviado **OSPF** es un protocolo de enrutamiento jerárquico de pasarela interior o IGP (Interior Gateway Protocol), que usa el algoritmo Dijkstra enlace-estado (LSA - *Link State Algorithm*) para calcular la ruta más corta posible. Usa *cost* como su medida de métrica. Además, construye una base de datos enlace-estado (*link-state database*, LSDB) idéntica en todos los enrutadores de la zona.

EIGRP: (Enhanced Interior Gateway Routing Protocol, Protocolo de enrutamiento de gateway interior mejorado):

Es un protocolo de encaminamiento vector distancia y un protocolo de enrutamiento de link-state , propiedad de Cisco Systems, que ofrece lo mejor de los algoritmos de vector de distancias y del estado de enlace. Se considera un protocolo avanzado que se basa en las características normalmente asociadas

con los protocolos del estado de enlace.

RIP:

Son las siglas de Routing Information Protocol (Protocolo de Información de Enrutamiento). Es un protocolo de puerta de enlace interna o IGP (Internal Gateway Protocol) utilizado por los routers (encaminadores), aunque también pueden actuar en equipos, para intercambiar información acerca de redes IP.

Packet Tracer:

Es la herramienta de aprendizaje y simulación de redes interactiva para los instructores y alumnos de Cisco CCNA. Esta herramienta les permite a los usuarios crear topologías de red, configurar dispositivos, insertar paquetes y simular una red con múltiples representaciones visuales. Packet Tracer se enfoca en apoyar mejor los protocolos de redes que se enseñan en el currículum de CCNA.

Ping:

La utilidad **ping** comprueba el estado de la conexión con uno o varios equipos remotos por medio de los paquetes de solicitud de eco y de respuesta de eco (ambos definidos en el protocolo de red ICMP) para determinar si un sistema IP específico es accesible en una red. Es útil para diagnosticar los errores en redes o enrutadores IP.

Protocolos:

Es un conjunto de reglas usadas por computadoras para comunicarse unas con otras a través de una red. Un protocolo es una convención o estándar que controla o permite la conexión, comunicación, y transferencia de datos entre dos puntos finales.

RESUMEN

A lo largo de mi carrera, y en especial en el presente Diplomado logre profundizar mucho en mi conocimiento en especial todo lo relacionado con la REDES, las T.I. y comprendo la importancia que esto radica ya que estas tecnologías están tomando mucha fuerza dentro de nuestras vidas tanto laborales como familiares y personales. Debemos ser conscientes que como profesionales siempre tenemos que ser parte de ese cambio, ese cambio constructivo que ayuda, que forma, que cambia mejorando constantemente.

La actividad es supremamente importante para mí, pues he aplicado cada uno de los temas que a lo largo de mi proceso de estudio miré, las redes que se han configurado son 2 casos muy reales ajustados a problemas que muy seguramente vamos a tratar dentro de la vida profesional que nos espera, nuestra intención es que nos practiquemos en el desarrollo de una serie de ejercicios prácticos, desarrollando nuestra actitud propositiva hacia problemáticas de una empresa que le queremos aportar.

Este trabajo nos ha colaborado para que nos familiaricemos de una manera mucho más amena con todos los dispositivos y elementos que hacen parte de la red ya que podemos distinguir cada una de sus diferencias y posibilidades que se nos presentan.

Todo el montaje de la red la realizamos dentro del simulador, magnífica herramienta desarrollada por CISCO, llamada PACKET TRACER, gracias a este podemos ejecutar gran parte de los comandos que se pueden configurar dentro de los dispositivos reales.

Esperamos este trabajo sea del agrado de todos ustedes.

ABSTRACT

Throughout my career, and especially in this Diploma, I managed to deepen my knowledge, especially everything related to NETWORKS, T.I. and I understand the importance of this, since these technologies are taking a lot of force in our work, family and personal lives. We must be aware that as professionals we always have to be part of that change, that constructive change that helps, that forms, that changes constantly improving.

The activity is supremely important to me, because I have applied each of the topics that I looked at throughout my study process, the networks that have been configured are 2 very real cases adjusted to problems that we are most likely going to deal with within the professional life that awaits us, our intention is that we practice in the development of a series of practical exercises, developing our proactive attitude towards problems of a company that we want to contribute.

This work has helped us to become familiar in a much more pleasant way with all the devices and elements that are part of the network since we can distinguish each of their differences and possibilities that are presented to us.

All the assembly of the network is carried out within the simulator, a magnificent tool developed by CISCO, called PACKET TRACER, thanks to this we can execute a large part of the commands that can be configured within the real devices.

We hope this work is to the liking of all of you

INTRODUCCION

Nuestra época definitivamente es un periodo de cambio, de revolución y de muchos avances tecnológicos donde cómo podemos observar las telecomunicaciones han jugado un papel supremamente importante. Gracias a todo esto el desarrollo es evidente, desde los pequeños hasta las grandes empresas pueden crecer muy rápidamente siempre y cuando empleemos los medios adecuados para llegar a los clientes finales. Si observamos nuestras vidas estas no han sido para nada ajenas a estos cambios tan grandes, la verdad dependemos de las redes, por lo menos siempre y cuando estas sean bien utilizadas la web, las redes sociales, el chat, todos estos elementos bien utilizados nos facilitan muchas de nuestras tareas de márquetin.

Veos entonces que es muy importante el hecho de que dentro de nuestra formación profesional tengamos un amplio conocimiento acerca de las redes de datos, y que mejor manera que podamos afianzar y mejorarlos a través de una práctica de estos 2 ESCENARIOS, escenarios que son muy similares a aspectos reales y que muy posiblemente encontraremos en nuestra vida profesional.

En primera instancia comenzaremos desarrollando un pequeño ejercicio en el cual aplicaremos el direccionamiento IPV4 empleando VLSM y además configuraremos el protocolo RIP, con el fin de observar su funcionamiento. Continuaremos en el segundo caso a desarrollar una propuesta con el fin de mejorar considerablemente la red que en la actualidad posee, aplicaremos VLSM lo que no permitirá un menor desperdicio de direcciones IP, además trabajaremos por consiguiente con protocolos como son EIGRP, OSPF y RIP V2. Estos protocolos trabajan de una manera mucho más eficiente, calculan sus rutas empleando algoritmos mucho más especializados dependiendo de cada una de las circunstancias.

JUSTIFICACIÓN

Nuestras vidas dependen más y más de la tecnología, si miramos en frente nuestro muy seguramente contamos con un dispositivo gracias al cual nos podemos conectar a la RED, las telecomunicaciones son parte esencial de nuestras vidas. Las microempresas, empresas, organizaciones emplean mucho estas tecnologías en nuestros días todo con el fin de explotarla de la mejor manera y sacar el mayor provecho posible.

OBJETIVOS

Objetivo general

Se desarrollará cada uno de los ESCENARIO INDICADOS, siguiendo las especificaciones que se nos suministra para la misma.

Objetivos Específico

- Diseñar y documentar un esquema de direccionamiento según los requisitos.
- Aplicar una configuración básica a los dispositivos.
- Verificar la conectividad entre todos los dispositivos de la topología de la red.
- Configurar todos los dispositivos que intervienen dentro de una red de datos.
- Comprender el funcionamiento de cada uno de los dispositivos que intervienen.

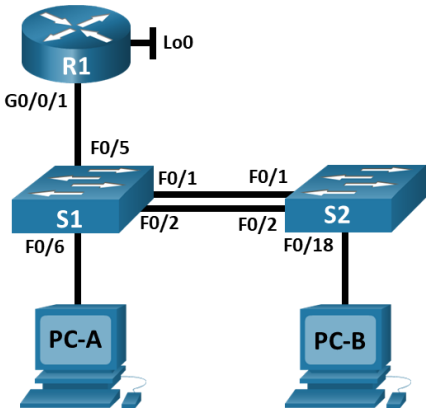
ESCENARIO 1

Descripción de escenarios propuestos para la prueba de habilidades

Escenario 1

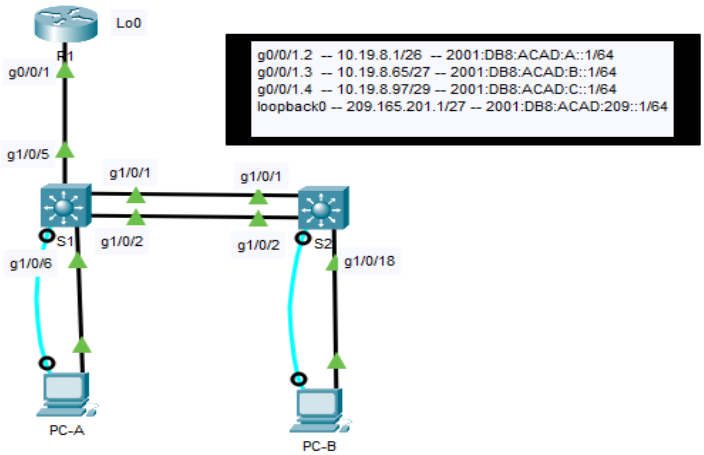
Topología

Figura 1Topología propuesta escenario 1



Fuente: Autor

Figura 2 Topología desarrollada escenario 1



Fuente: Autor

En este primer escenario se configurarán los dispositivos de una red pequeña. Debe configurar un router, un switch y equipos que admitan tanto la conectividad IPv4 como IPv6 para los hosts soportados. El router y el switch también deben administrarse de forma segura. Configurará el enrutamiento entre VLAN, DHCP, Etherchannel y port-security.

Tabla de VLAN

Tabla 1 - Nombre VLAN -Escenario 1

VLAN	Nombre de la VLAN
2	Bikes
3	Trikes
4	Management
5	Parking
6	Native

Tabla de asignación de direcciones

Tabla 2 - Asignación de Direcciones IP - Escenario 1

Dispositivo / interfaz	Dirección IP / Prefijo	Puerta de enlace predeterminada
R1 G0/0/1.2	10.19.8.1 /26	No corresponde
R1 G0/0/1.2	2001:db8:acad:a: :1 /64	No corresponde
R1 G0/0/1.3	10.19.8.65 /27	No corresponde
R1 G0/0/1.3	2001:db8:acad:b: :1 /64	No corresponde
R1 G0/0/1.4	10.19.8.97 /29	No corresponde
R1 G0/0/1.4	2001:db8:acad:c: :1 /64	No corresponde
R1 G0/0/1.6	No corresponde	No corresponde
R1 Loopback0	209.165.201.1 /27	No corresponde
R1 Loopback0	2001:db8:acad:209: :1 /64	No corresponde

Dispositivo / interfaz	Dirección IP / Prefijo	Puerta de enlace predeterminada
S1 VLAN 4	10.19.8.98 /29	10.19.8.97
VLAN S1 4	2001:db8:acad:c: :98 /64	No corresponde
S1 VLAN 4	fe80: :98	No corresponde
S2 VLAN 4	10.19.8.99 /29	10.19.8.97
S2 VLAN 4	2001:db8:acad:c: :99 /64	No corresponde
S2 VLAN 4	fe80: :99	No corresponde
PC-A NIC	Dirección DHCP para IPv4	DHCP para puerta de enlace predeterminada IPv4
PC-A NIC	2001:db8:acad:a: :50 /64	fe80::1
PC-B NIC	DHCP para dirección IPv4	DHCP para puerta de enlace predeterminada IPv4
PC-B NIC	2001:db8:acad:b: :50 /64	fe80::1

Instrucciones

Parte 1: **Inicializar y Recargar y Configurar aspectos basicos de los dispositivos**

Paso 1: Inicializar y volver a cargar el router y el switch

- Borre las configuraciones de inicio y las VLAN del router y del switch y vuelva a cargar los dispositivos.

S1

Erase-startup-config

Delete vlan.dat

Reload

S2

Erase-startup-config

Delete vlan.dat

Reload

Figura 3 reinicio de dispositivos

```
R1#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
R1#
R1#delete vlan.dat
Delete filename [vlan.dat]?
Delete flash:/vlan.dat? [confirm]
%Error deleting flash:/vlan.dat (No such file or directory)

R1#reload
System configuration has been modified. Save? [yes/no]:
% Please answer 'yes' or 'no'.
System configuration has been modified. Save? [yes/no]:y
```

Fuente: autor.

Con el desarrollo de los comandos anteriores se verifico que el dispositivo de reinicio, por lo cual podemos proceder a configurar las plantillas SDM

- Después de recargar el switch, configure la plantilla SDM para que admita IPv6 según sea necesario. Por ultimo no olvidemos que debemos volver a cargar el switch.

Show sdm prefer

Vemos que soporta IPV6

Figura 4 – activación de SDM en los switches.

```
Switch#configure t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#sdm prefer dual-ipv4-and-ipv6 default
Changes to the running SDM preferences have been stored, but cannot take effect until the
next reload.
Use 'show sdm prefer' to see what SDM preference is currently active.
Switch(config)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#reload
System configuration has been modified. Save? [yes/no]:yes
Building configuration...
[OK]
```

Fuente: autor.

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

Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Como objetivo principal de este paso es ajustar a los dispositivos para que sean accesibles y además poderles brindar seguridad. incluyendo un password, si no se conoce la contraseña de acceso aparecerá el mensaje de acceso no permitido, sirviendo esto como método disuasivo para usuarios no autorizados. Se asigna tanto direccionamiento ipv4 e ipv6 y se configura las respectivas troncales, y para finalizar nuestro proceso lo que hacemos es generar una clave segura y además la encriptamos.

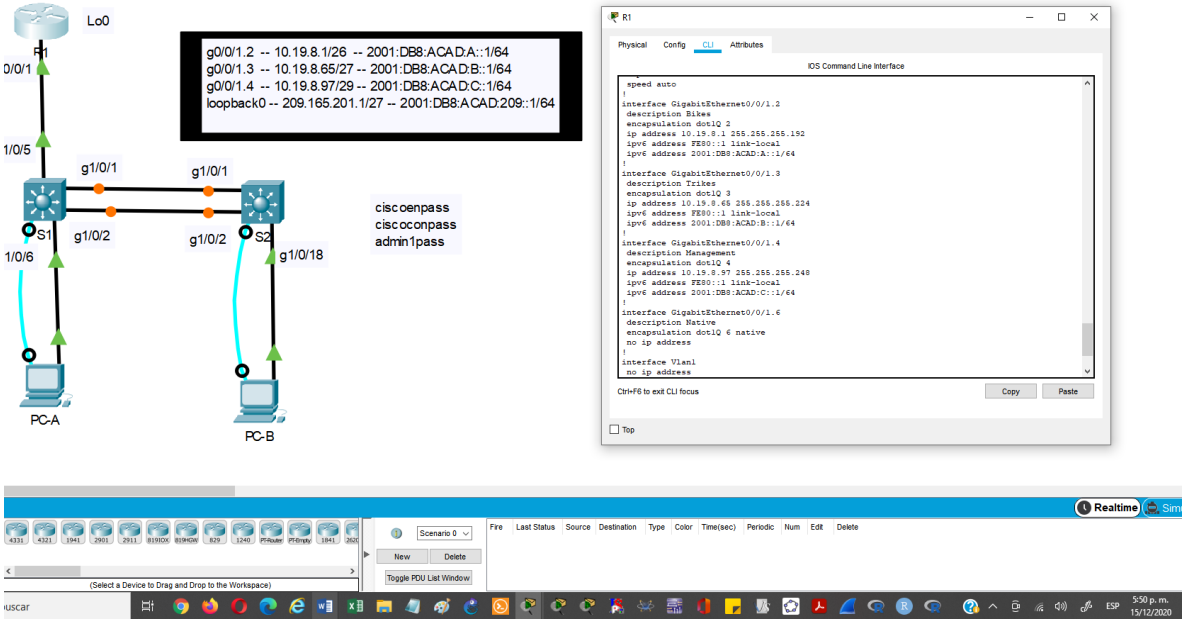
Tabla 3 - Configuración R1- Escenario 1

Tarea	Especificación
Desactivar la búsqueda DNS	No ip domain-lookup
Nombre del router	Hostname R1
Nombre de dominio	ccna-lab.com ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	Ciscoenpass Enable secret ciscoenpass
Contraseña de acceso a la consola	Ciscoconpass Line console 0 Password ciscoconpass login
Establecer la longitud mínima para las contraseñas	10 caracteres Security passwords min-leng 10
Crear un usuario administrativo en la base de datos local	Nombre de usuario: **admin** Password: **admin1pass** Username admin secret admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	Line vt 0 15 login local
Configurar VTY solo aceptando SSH	Transport input ssh
Cifrar las contraseñas de texto no cifrado	Service password-encryption

Tarea	Especificación
Configure un MOTD Banner	Banner motd % Prohibido el acceso no autorizado %
Habilitar el routing IPv6	Ipv6 unicast-routing
Configurar interfaz G0/0/1 y subinterfaces	Establezca la descripción Establece la dirección IPv4. Establezca la dirección local de enlace IPv6 como **fe80: :1** Establece la dirección IPv6. Activar la interfaz. **Int g0/0/1.2** Encapsulation dot1q 2 Description BIKES Ip addres 10.19.8.1 255.255.255.192 Ipv6 addres 2001:db8:acad:a:1/64 Ipv6 addres fe80::1 link local Int g0/0/1 No shutdown **Int g0/0/1.3** Encapsulation dot1q 3 Description TRIKES Ip addres 10.19.8.65 255.255.255.224 Ipv6 addres 2001:db8:acad:b:1/64 Ipv6 addres fe80::1 link local **Int g0/0/1.4** Encapsulation dot1q 4 Description MANAGEMENT Ip addres 10.19.8.97 255.255.255.224 Ipv6 addres 2001:db8:acad:c:1/64 Ipv6 addres fe80::1 link local **Int g0/0/1.6** Encapsulation dot1q 6 NARIVE Description NATIVE Ip addres 10.19.8.97 255.255.255.224 Ipv6 addres 2001:db8:acad:c:1/64 Ipv6 addres fe80::1 link local **Int g0/0/1** No shutdown

Tarea	Especificación
Configure el Loopback0 interface	Establezca la descripción Establece la dirección IPv4. Establece la dirección IPv6. Establezca la dirección local de enlace IPv6 como **fe80::1** Interface loopback 0 Ip address 209.165.201.1 255.255.255.224 Ipv6 address 2001:db8:acad:209::1/64 Ipv6 address fe80::1 link-local Description INTERNET
Generar una clave de cifrado RSA	Módulo de 1024 bits Crypto key generate rsa modulus 1024

Figura 5 show running-config: verificación subinterfaces.



Fuente: autor.

Paso 3: Configure S1 y S2.

Las tareas de configuración incluyen lo siguiente:

Comenzamos realizando la configuración de los 2 switches, los comandos que vamos a aplicar son los más básicos, comenzaremos configurando los respectivos nombres de cada uno de los dispositivos, desactivamos la búsqueda DNS aplicando el comando “NO IP DOMAIN LOOKUP” con lo cual evitamos la traducción de nombres a direcciones IP, configuramos todo lo relacionado a las VLAN, junto con sus enlaces TRONCALES, y por último debemos proceder a agregar contraseñas tanto a la línea de consola líneas VTY, y los mensajes BANNER MOTD, mensaje que aparecen cada vez que ingresamos a los dispositivos.

Tabla 4 - Configuración S1-S2 - Escenario 1

Tarea	Especificación
Desactivar la búsqueda DNS.	No ip domain lookup
Nombre del switch	**S1 o S2, según proceda** Hostname S1 Hostname S2
Nombre de dominio	**ccna-lab.com** ip domain name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	**Ciscoenpass** Enable secret ciscoenpass
Contraseña de acceso a la consola	**Ciscoconpass** Line console 0 Password ciscoconpass Login
Crear un usuario administrativo en la base de datos local	Nombre de usuario: **admin** Password: **admin1pass** Username admin secret admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	Line vty 0 15 Login local

Tarea	Especificación
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	Transport input ssh
Cifrar las contraseñas de texto no cifrado	Service password-encryption
Configurar un MOTD Banner	Banner motd % Prohibido el acceso no autorizado %
Generar una clave de cifrado RSA	**Módulo de 1024 bits** Crypto key generate rsa mosulus 10242
Configurar la interfaz de administración (SVI)	Establecer la dirección IPv4 de capa 3 Establezca la dirección local de enlace IPv6 como **FE80: :98 para S1 y FE80: :99 para S2** Establecer la dirección IPv6 de capa 3 Int vlan 4 Ip address 10.19.8.98 255.255.255.248 Ipv6 address 2001:db8:acad:c::98/64 Ipv6 address fe80::98 link-local Description MANAGEMENT No shutdown
Configuración del gateway predeterminado	Configure la puerta de enlace predeterminada como 10.19.8.97 para IPv4 Ip Default-gateway 10.19.8.97

Paso 4: Configure S1 y <u>S2</u>

Las tareas de configuración incluyen lo siguiente:

Tabla 5 - Configuración S1-S2 - Escenario 1

Tarea	Especificación
Desactivar la búsqueda DNS.	No ip domain lookup
Nombre del switch	**S1 o S2, según proceda** Hostname S2
Nombre de dominio	**ccna-lab.com** ip domain name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	**Ciscoenpass** Enable secret ciscoenpass
Contraseña de acceso a la consola	**Ciscoconpass** Line console 0 Password ciscoconpass Login
Crear un usuario administrativo en la base de datos local	Nombre de usuario: **admin** Password: **admin1pass** Username admin secret admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	Line vty 0 15 Login local
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	Transport input ssh
Cifrar las contraseñas de texto no cifrado	Service password-encryption
Configurar un MOTD Banner	Banner motd % Prohibido el acceso no autorizado %
Generar una clave de cifrado RSA	**Módulo de 1024 bits** Crypto key generate rsa modulus 1024 -- no soportado Crypto key generate rsa 1024

Tarea	Especificación
Configurar la interfaz de administración (SVI)	Establecer la dirección IPv4 de capa 3 Establezca la dirección local de enlace IPv6 como **FE80: :98 para S1 y FE80: :99 para S2** Establecer la dirección IPv6 de capa 3 Int vlan 4 Ip address 10.19.8.99 255.255.255.248 Ipv6 address 2001:db8:acad:c::99/64 Ipv6 address fe80::99 link-local Description MANAGEMENT No shutdown
Configuración del gateway predeterminado	Configure la puerta de enlace predeterminada como 10.19.8.97 para IPv4 Ip Default-gateway 10.19.8.97

Parte 2: Configuración de la infraestructura de red (VLAN, Trunking, EtherChannel)

Paso 5: Configurar <u>S1</u>

La configuración del S1 incluye las siguientes tareas:

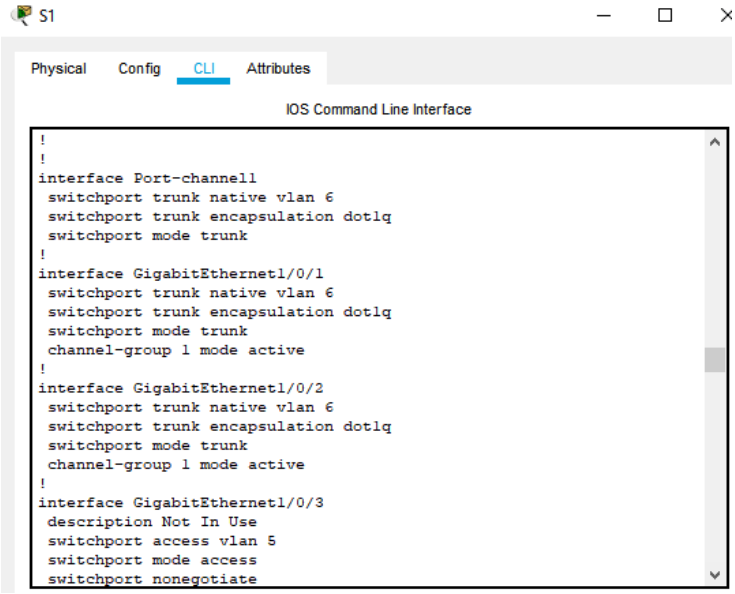
En esta sección lo que haremos es conectar de una menara lógica los diferentes dispositivos, a este le conocemos como VLAN, esto es muy eficiente a la hora de mejorar el rendimiento de nuestra red, segmentando la misma gracias a lo cual se logra que la misma sea más eficiente. Para ellos debemos configurar muchos enlaces como troncales, los cuales serán los encargados de llevar una serie de mensajes o señales a la ubicación deseada, es como tener una autopista que comunica muchos puntos, y estos enlaces son los encargados de llevar las mismas al punto específico, Para esta tarea se emplea un protocolo muy conocido IEEE 802.1Q, el cual lleva los paquetes a la VLAN especifica.

Tabla 6 - Configuración S1-S2 - Escenario 1

Tarea	Especificación
Crear VLAN	Procedemos a crar las VLAN, primero las creamos y luego les agregamos un nombre. Vlan 2 Name bikes Vlan 3 Name trikes Vlan 4 Name management Vlan 5 Name parking Vlan 6 Name native
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	Interfaces F0/1, F0/2 y F0/5 Interfaces G1/0/1, G1/0/2 y G1/0/5 **Interface G1/0/5** Switchport trunk encapsulation dot1q Switchport mode trunk Switchport trunk native vlan 6 **Inteface range G1/0/1-2** Shutdown Switchport trunk encapsulation dot1q Switchport mode trunk Switchport trunk native vlan 6

Tarea	Especificación
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	**Usar el protocolo LACP para la negociación** Channel-group 1 mode active Int port channel 1 Switchport trunk encapsulation dot1q Switchport mode trunk Switchport trunk native vlan 6
Configurar el puerto de acceso de host para VLAN 2	Interface F0/6 Interface g1/0/6 Switchport mode access Switchport access vlan 2
Configurar la seguridad del puerto en los puertos de acceso	Permitir 3 direcciones MAC Switchport port-security máximum 3
Proteja todas las interfaces no utilizadas	Asignar a VLAN 5, Establecer en modo de acceso, agregar una descripción y apagar **Int range g1/0/3-4** Switchport mode Access Switchport Access vlan 5 Description no esta en uso Shutdown **Int range g1/0/7-24** Switchport mode Access Switchport Access vlan 5 Description no esta en uso Shutdown **Int range g1/1/1-4** Switchport mode Access Switchport Access vlan 5 Description no esta en uso Shutdown

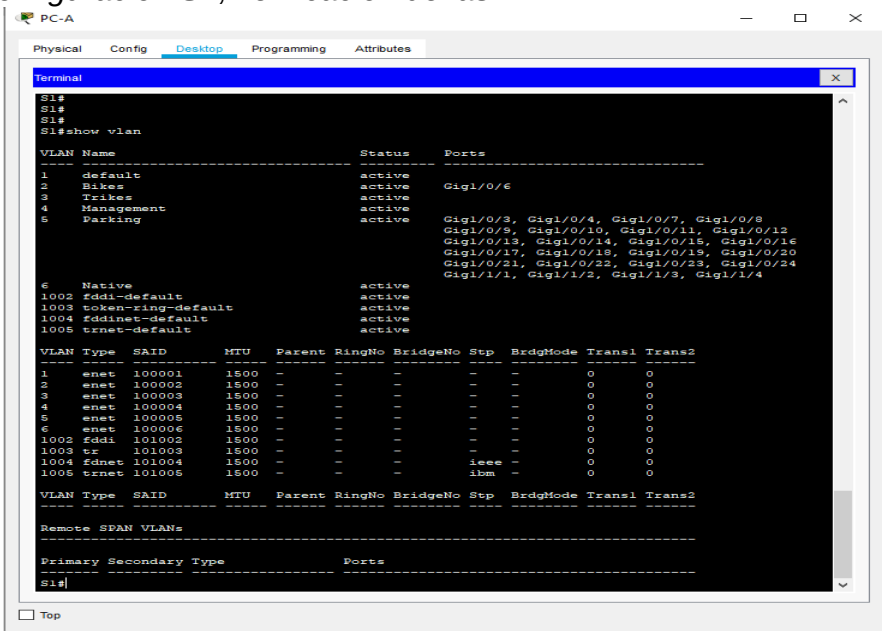
Figura 6 show running-configS1, verificación config. Sub interfaces y asignación de VLAN.



Fuente: autor.

Vemos en esta parte que los comandos que ejecutamos en los pasos anteriores son correctos, podemos observar que el S1 tiene configuradas cada una de las sub-interfaces, estas configuradas como troncales y además cada una fue asignada a la correspondiente VLAN.

Figura 7 configuración S1, verificación de las VLAN.



Fuente: Autor

Paso 6: Configure el S2.

Entre las tareas de configuración de S2 se incluyen las siguientes:

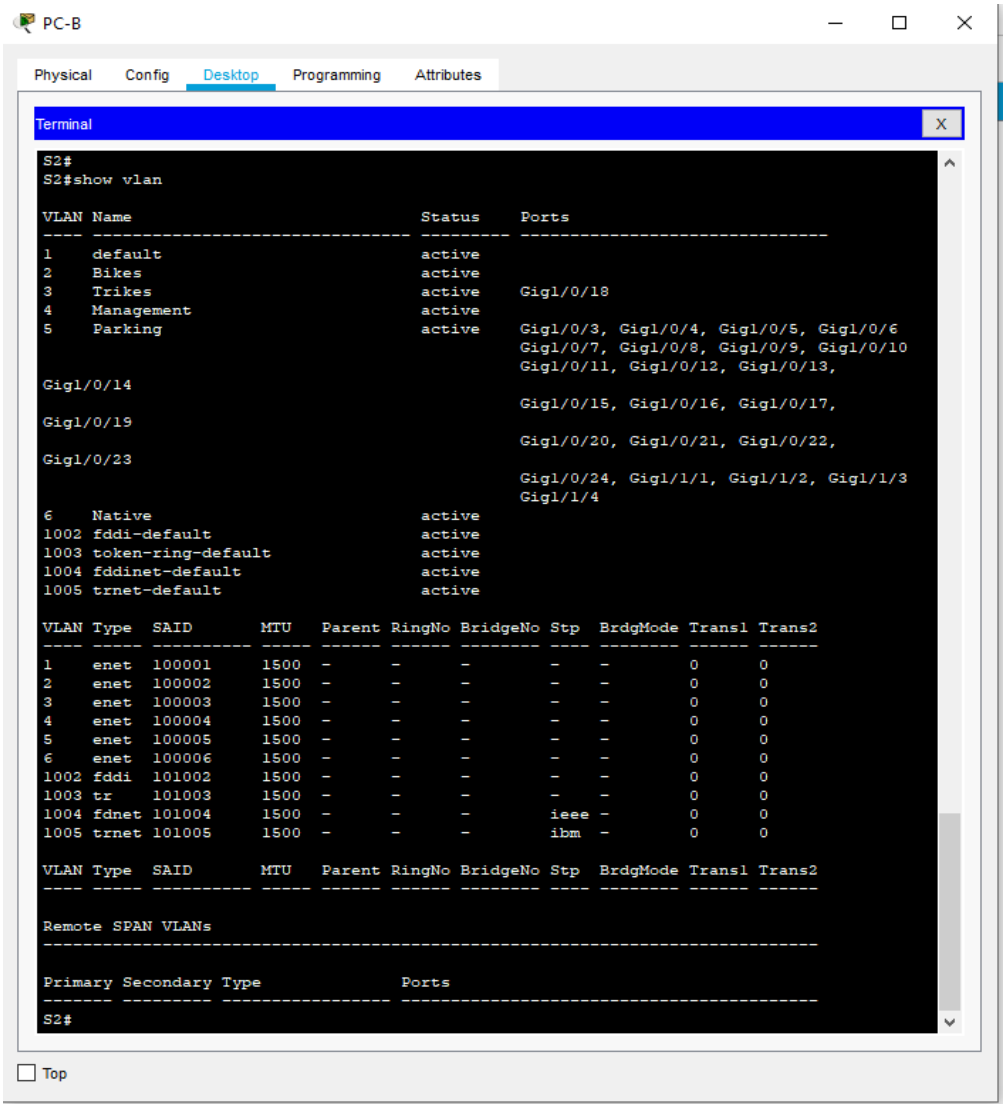
Tabla 7 - Configuración S2 - Escenario 1

Tarea	Especificación
Crear VLAN	Procedemos a crear cada una de las VLAN y luego le asignamos un nombre. Vlan 2 Name bikes Vlan 3 Name trikes Vlan 4 Name management Vlan 5 Name parking Vlan 6 Name native
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	Configuramos las interfaces como troncales y además asignamos la respectiva VLAN a cada una de ellas. Interfaces range G1/0/1-2 shutdown switchport trunk encapsulation dot1q switchport mode trunk switchport trunk native vlan 6

Tarea	Especificación
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	Usar el protocolo LACP para la negociación Channel-group 1 mode active Int port channel 1 switchport trunk encapsulation dot1q switchport mode trunk switchport trunk native vlan 6
Configurar el puerto de acceso del host para la VLAN 3	Interfaz F0/18 Int g0/1/18 Switchport mode Access Switchport Access vlan 3
Configure port-security en los access ports	permite 3 MAC addresses switchport port-security switchport port-security maximum 3

Tarea	Especificación
Asegure todas las interfaces no utilizadas.	Asignar a VLAN 5, Establecer en modo de acceso, agregar una descripción y apagar **Int range g1/0/3-17** Switchport mode Access Switchport Access vlan 5 Description no esta en uso Shutdown **Int range g1/0/19-24** Switchport mode Access Switchport Access vlan 5 Description no esta en uso Shutdown **Int range g1/1/1-4** Switchport mode Access Switchport Access vlan 5 Description no está en uso Shutdown
Debemos activar las interfaces del etherchannel de cada uno de los 2 switches.	S1: G1/0/1-2 NO SHUTDOWN S2: G1/0/1-2 NO SHUTDOWN

Figura 8 Activar EtherChannel S1-S2 escenario 1



Fuente: Autor

Parte 2: Configurar soporte de host

Paso 1: Configure R1

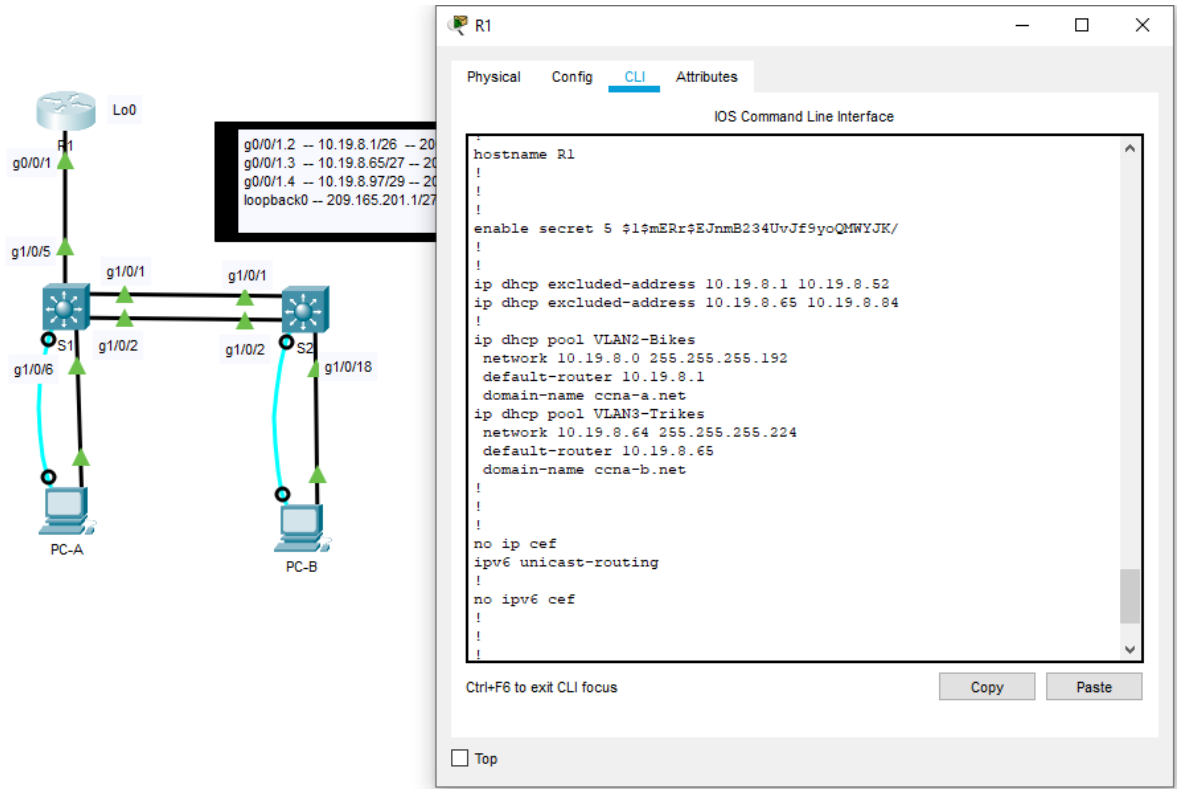
Las tareas de configuración para R1 incluyen las siguientes:

Tabla 8 - Configuración R1 - Escenario 1

Tarea	Especificación
Configure Default Routing	Crear rutas predeterminadas para IPv4 e IPv6 que dirijan el tráfico a la interfaz Loopback 0 Ip route 0.0.0.0 0.0.0.0 loopback 0 **Ipv6 route ::/0 loopback 0**
ofigurar IPv4 DHCP para VLAN 2	Cree un grupo DHCP para VLAN 2, compuesto por las **últimas 10 direcciones** de la subred solamente. Asigne el nombre de dominio ccna-a.net y especifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada 10.19.8.0 /26 10.19.8.1 10.19.8.62 Debemos entonces restringir las primeras direcciones de este rango, ya que solo debemos trabajar con las 10 últimas del mismo. 10.19.8.1 - 10.19.8.52 estas son las que debemos restringir y solo trabajamos con las 10 que sobran. Debemos entonces crear el POOL desde: 10.19.8.52 - 10.19.8.62 Ip dhcp excluded-address 10.19.8.1 10.19.8.52 Ip dhcp POOL VLAN2-BIKES Network 10.19.8.0 255.255.255.192 Default-route 10.19.8.1 Domain-name ccna-b.net

Tarea	Especificación
Configure Default Routing	Crear rutas predeterminadas para IPv4 e IPv6 que dirijan el tráfico a la interfaz Loopback 0 Ip route 0.0.0.0 0.0.0.0 loopback 0 **Ipv6 route ::/0 loopback 0**
Configurar DHCP IPv4 para VLAN 3	Cree un grupo DHCP para VLAN 3, compuesto por las últimas 10 direcciones de la subred solamente. Asigne el nombre de dominio ccna-b.net y especifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada TRIKES 10.19.8.64 /27 10.19.8.65 10.19.8.94 Debemos entonces restringir las primeras direcciones de este rango, ya que solo debemos trabajar con las 10 últimas del mismo. 10.19.8.65 - 10.19.8.84 estas son las que debemos restringir y solo trabajamos con las 10 que sobran. Debemos entonces crear el POOL desde: 10.19.8.85 - 10.19.8.94 Ip dhcp excluded-address 10.19.8.65 10.19.8.84 Ip dhcp POOL VLAN3-TRIKES Network 10.19.8.64 255.255.255.224 Default-route 10.19.8.65 Domain-name ccna-b.net

Figura 9 Configuración R1 escenario 1



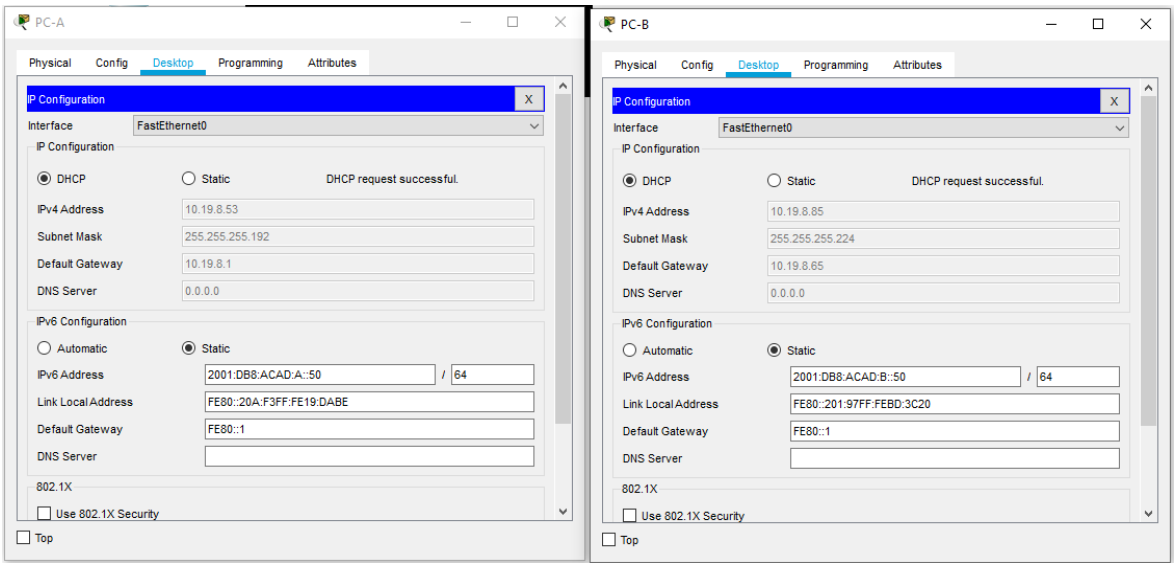
Fuente: Autor

Vemos claramente en esta parte que todo nuestro proceso de configuración del R1 se configura los POOL de direcciones las puertas de enlace predeterminadas, vemos los nombres de los dominios que de nuestra parte hemos creado.

Paso 2: Configurar los servidores

Configure los equipos host PC-A y PC-B para que utilicen DHCP para IPv4 y asigne estáticamente las direcciones IPv6 GUA y Link Local. Después de configurar cada servidor, registre las configuraciones de red del host con el comando **ipconfig /all**.

Figura 6 Configuración PCA - PCB escenario 1



Fuente: Autor

Tabla 9 - Configuración PC-A.

PC-A Network Configuration	
Descripción	*PC-A*
Dirección física	
Dirección IP	*10.19.9.53*
Máscara de subred	*255.255.255.224*
Gateway predeterminado	*10.19.8.1*
Gateway predeterminado IPv6	*FE80::1*

Tabla 10 - Configuración PC-B.

Configuración de red de PC-B	
Descripción	*PC-B*
Dirección física	*en blanco*
Dirección IP	*10.19.8,85*
Máscara de subred	*255.255.255.224*
Gateway predeterminado	*10.19.8,65*
Gateway predeterminado IPv6	*FE80::1*

Parte 3: Probar y verificar la conectividad de extremo a extremo

Parte 4:

Use el comando ping para probar la conectividad IPv4 e IPv6 entre todos los dispositivos de red.

Nota: Si fallan los pings en las computadoras host, desactive temporalmente el firewall de la computadora y vuelva a realizar la prueba.

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:

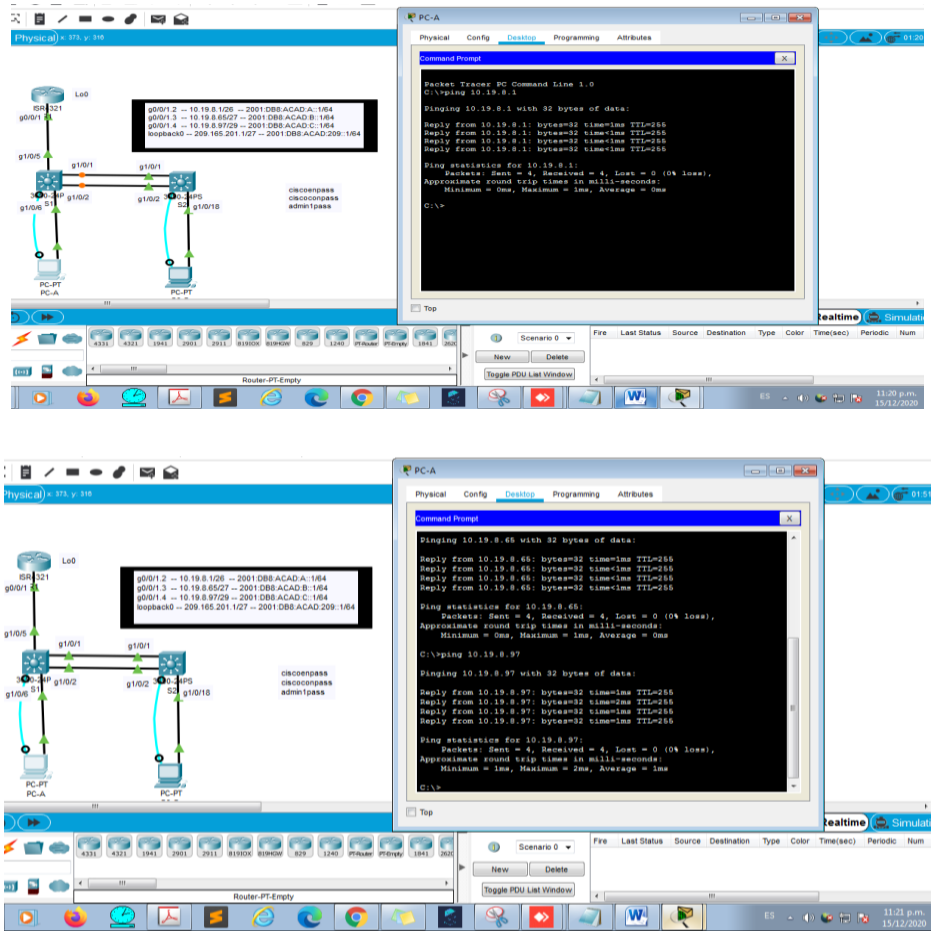
Tabla 11 – Verificación de Conectividad - Escenario 1

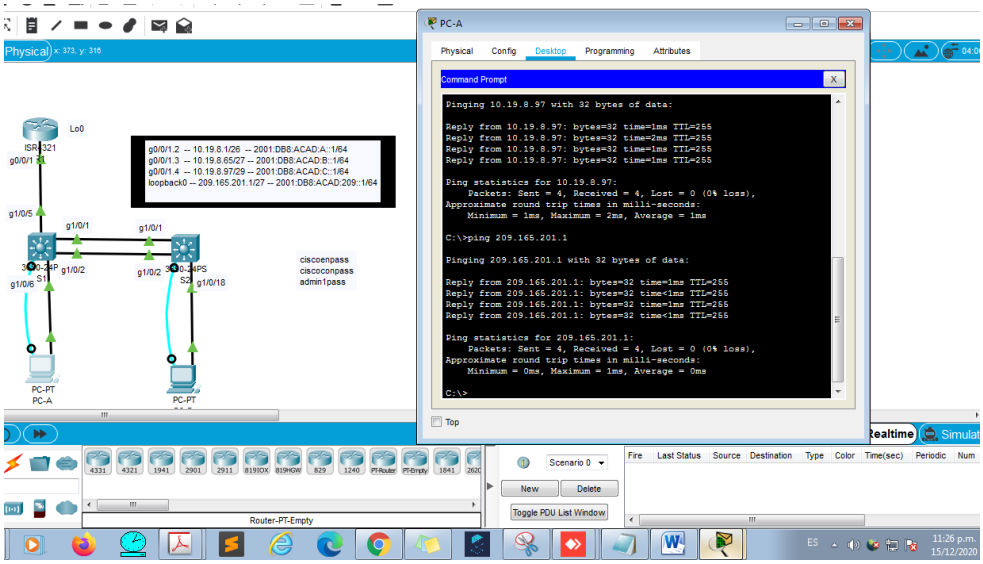
Desde	A	de Internet	Dirección IP	Resultados de ping
PC-A	R1, G0/0/1.2	Dirección	10.19.8.1	*exitoso*
PC-A	*R1, G0/0/1.2*	IPv6	2001:db8:acad:a: :1	exitoso
PC-A	R1, G0/0/1.3	Dirección	10.19.8.65	exitoso
PC-A	*R1, G0/0/1.3*	IPv6	2001:db8:acad:b: :1	exitoso
PC-A	R1, G0/0/1.4	Dirección	10.19.8.97	exitoso
PC-A	*R1, G0/0/1.4*	IPv6	2001:db8:acad:c: :1	exitoso
PC-A	S1, VLAN 4	Dirección	10.19.8.98	exitoso
PC-A	*S1, VLAN 4*	IPv6	2001:db8:acad:c: :98	exitoso
PC-A	S2, VLAN 4	Dirección	10.19.8.99.	exitoso
PC-A	*S2, VLAN 4*	IPv6	2001:db8:acad:c: :99	exitoso
PC-A	PC-B	Dirección	IP address will vary.	exitoso
PC-A	*PC-B*	IPv6	2001:db8:acad:b: :50	exitoso
PC-A	R1 Bucle 0	Dirección	209.165.201.1	exitoso
PC-A	*R1 Bucle 0*	IPv6	2001:db8:acad:209: :1	exitoso
PC-B	R1 Bucle 0	Dirección	209.165.201.1	exitoso
PC-B	*R1 Bucle 0*	IPv6	2001:db8:acad:209: :1	exitoso
PC-B	R1, G0/0/1.2	Dirección	10.19.8.1	exitoso
PC-B	*R1, G0/0/1.2*	IPv6	2001:db8:acad:a: :1	exitoso
PC-B	R1, G0/0/1.3	Dirección	10.19.8.65	exitoso
PC-B	*R1, G0/0/1.3*	IPv6	2001:db8:acad:b: :1	exitoso

Desde	A	de Internet	Dirección IP	Resultados de ping
PC-B	R1, G0/0/1.4	Dirección	10.19.8.97	exitoso
PC-B	*R1, G0/0/1.4*	IPv6	2001:db8:acad:c: :1	exitoso
PC-B	S1, VLAN 4	Dirección	10.19.8.98	exitoso
PC-B	*S1, VLAN 4*	IPv6	2001:db8:acad:c: :98	exitoso
PC-B	S2, VLAN 4	Dirección	10.19.8.99.	Exitoso
PC-B	*S2, VLAN 4*	IPv6	2001:db8:acad:c: :99	Exitoso

PRUEBAS DE CONECTIVIDAD ESCENARIO 1

Figura 10 PING, desde PC-A hacia los diferentes puntos de la red.





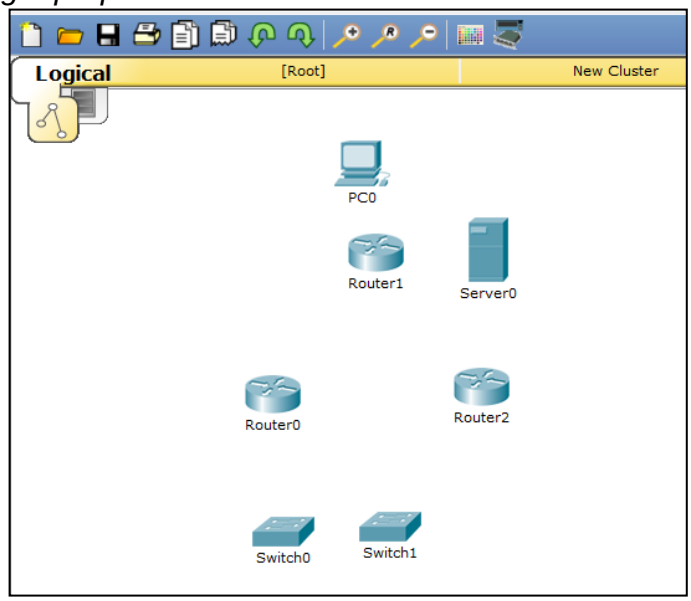
Fuente: autor.

Las pruebas de conectividad fueron realizadas desde los PC hacia la interfaz loopback del router R1, con esto verificamos que tenemos total conectividad entre los mismos.

DESARROLLO DEL ESCENARIO 2

Debemos comenzar armando la topología según lo muestra la guía:

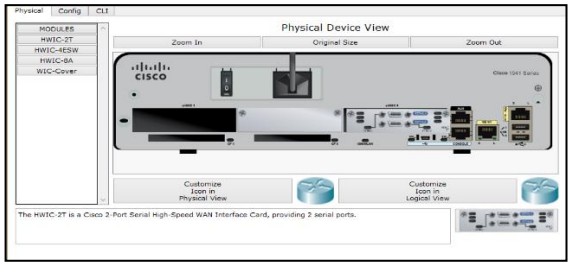
Figura 11 Topología propuesta escenario 2



Fuente: Autor

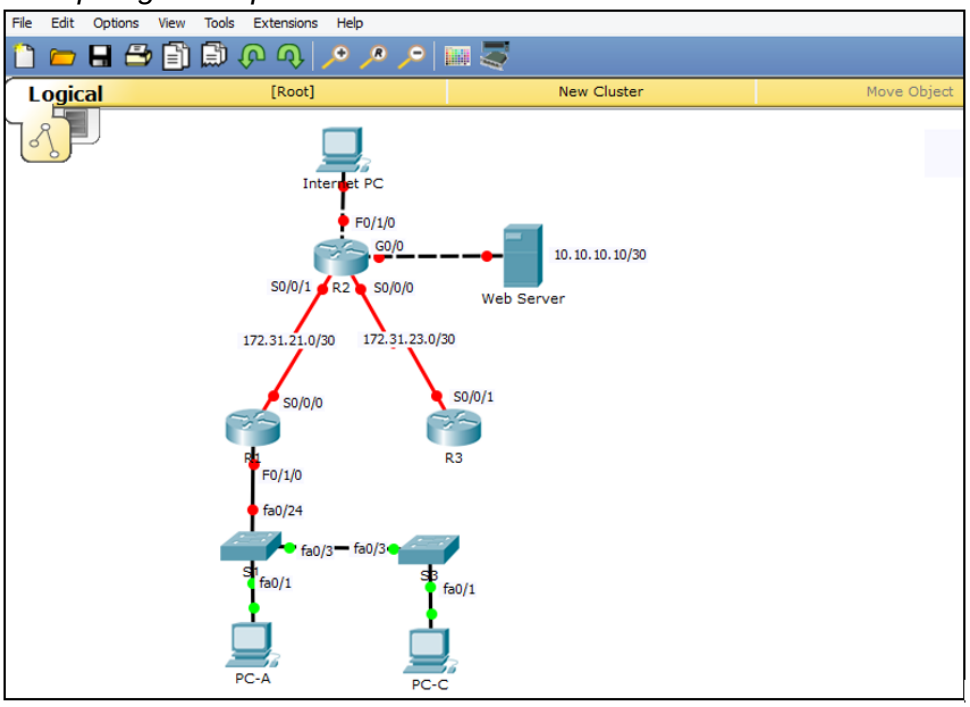
Agregamos los nombres de los dispositivos
Agregamos las interfaces físicas necesarias.

Figura 12 Configuración R1 escenario 2



Fuente: Autor

Figura 13 Topología completa escenario 2



Fuente: Autor

En los pasos anteriores realizamos la conexión de nuestra topología con esto ya conocemos cuales son las interfaces que se está utilizando en cada uno de los dispositivos, con lo cual podemos proceder a configurarlos.

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 12 – Inicializar Routers y los Switches- Escenario 2

Tarea	Comando de IOS
Eliminar el archivo startup-config de todos los routers	Para eliminar la configuración en los dispositivos debemos aplicar el commando: “erase startup-config”
Volver a cargar todos los routers	En este caso debemos aplicar el siguiente commando: “reload”
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	Para poder eliminar la totalidad de la confirguración debemos aplicar estos 2 comandos en los switches: - erase startup-config - delete vlan.dat
Volver a cargar ambos switches	Igualmente que en los routers en este caos aplicamos el commando: “Reload”
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	Para mirar en la memoria debemos aplicar el siguiente comendo: “show flash”

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):

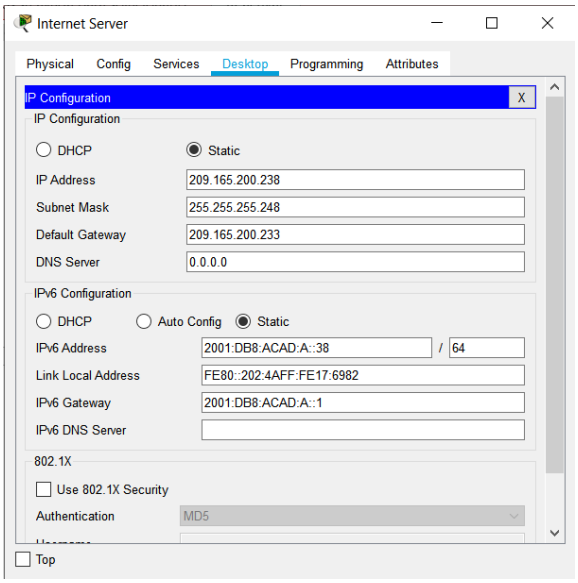
Recordemos que esta parte la debemos configurar de acuerdo a la información que nos suministra en la TOPOLIOGÍA:

Tabla 13 – Configuración de PC- Escenario 2

Elemento o tarea de configuración	Especificación
Dirección IPv4	209.165.200.230
Máscara de subred para IPv4	255.255.255.248
Gateway predeterminado	209.165.200.225
Dirección IPv6/subred	2001:DB8:ACAD:2::30/64
Gateway predeterminado IPv6	2001:DB8:ACAD:2::1

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.

Figura 14 Internet Server escenario 2



Fuente: Autor

Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 14 – Configuración R1 - Escenario 2

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Se ingresa a modo privilegiado, luego se ingresa a modo de configuración y en seguida se coloca el comando para desactivar la búsqueda DNS asi: ***no ip domain-lookup***
Nombre del router	En el modo de configuración podemos asignar un nombre al dispositivo R:1 ***hostname R1***
Contraseña de exec privilegiado cifrada	En modo de configuración se coloca el comando para asignar la contraseña para el modo EXEC privilegiado class ***enable secret class***
Contraseña de acceso a la consola	Asignamos la configuración de las contraseñas en el dispotivo: cisco ***line con 0*** ***password cisco*** ***login***
Contraseña de acceso Telnet	Configuramos la cotraseña cisco para las lineas vty. ***line vty 0 4*** ***password cisco*** ***login***
Cifrar las contraseñas de texto no cifrado	En modo de configuración se coloca el comando para cifrar las contraseñas de texto no cifradas asi: ***service password-encryption***

Mensaje MOTD	Se prohíbe el acceso no autorizado. ***banner motd ^CUnauthorized Access is Prohibited!^C***
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 ***interface Serial0/0/0*** ***description Connection to R2*** ***ip address 172.16.1.1 255.255.255.252*** ***ipv6 address 2001:DB8:ACAD:1::1/64*** ***clock rate 128000*** ***no shutdown***
Rutas predeterminadas	Configurar una ruta IPv4 predeterminada de S0/0/0 Configurar una ruta IPv6 predeterminada de S0/0/0 ***ip route 0.0.0.0 0.0.0.0 Serial0/0/0*** ***ipv6 route ::/0 Serial0/0/0***

Nota: Todavía no configure G0/1.

Paso 3: Configurar R2

La configuración del R2 incluye las siguientes tareas:

Tabla 15 – Configuración R2 - Escenario 2

Elemento o tarea de configuración	Especificación
Configuramos los datos más importantes del router, nombre, contraseñas, y aprovechamos para encriptar las mismas.	No ip domain-lookup Hostname R2 Enable secret class

	Line console 0 Password cisco Login Line vty 0 15 Password cisco Login Service password-encryption
Habilitamos el servidor DHCP	Comando no soportado por PACKET TRACER.
Le configuramos a este router igualmente el mensaje del mismo y configuramos las interfaces:	Banner motd % User Access Verification % Configuramos la interface serial: Interface serial 0/0/0 Description conexión con R1 Ip address 172.16.1.2 255.255.255.252 Ipv6 addres 2001:db8:acad:1::2/64 No shutdown
Procedemos a configurar la interface serial, agregamos una pequeña descripción, configuramos IPV4 como IPV6 y configuramos como clak rate.	Interface serial 0/0/1 Description conexión con R3 Ip address 172.16.2.2 255.255.255.252 Ipv6 addres 2001:db8:acad:2::2/64 Clock rate 128000 No shutdown
Procedemos ahora a configurar la interface g0/0 agregamos la descripción configuramos IPV4 e IPV6 y la activamos.	Interface g 0/0 Description conexión a INTERNET Ip address 209.165.200.233 255.255.255.248 Ipv6 addres 2001:db8:acad:a::1/64 No shutdown
Configuramos ahora la interface loopback que	Interface loopback 0

nos va a permitir similar nuestro servidor y de una vez le asignamos una IP.	Description WEB SERVER Ip address 10.10.10.10 255.255.255.255
Creamos nuestra ruta por defecto tanto IP-V4 como IP – V6:	Ruta por defecto Ip route 0.0.0.0 0.0.0.0 g0/0 Ipv6 route ::/0 g0/0

Paso 4: Configurar R3

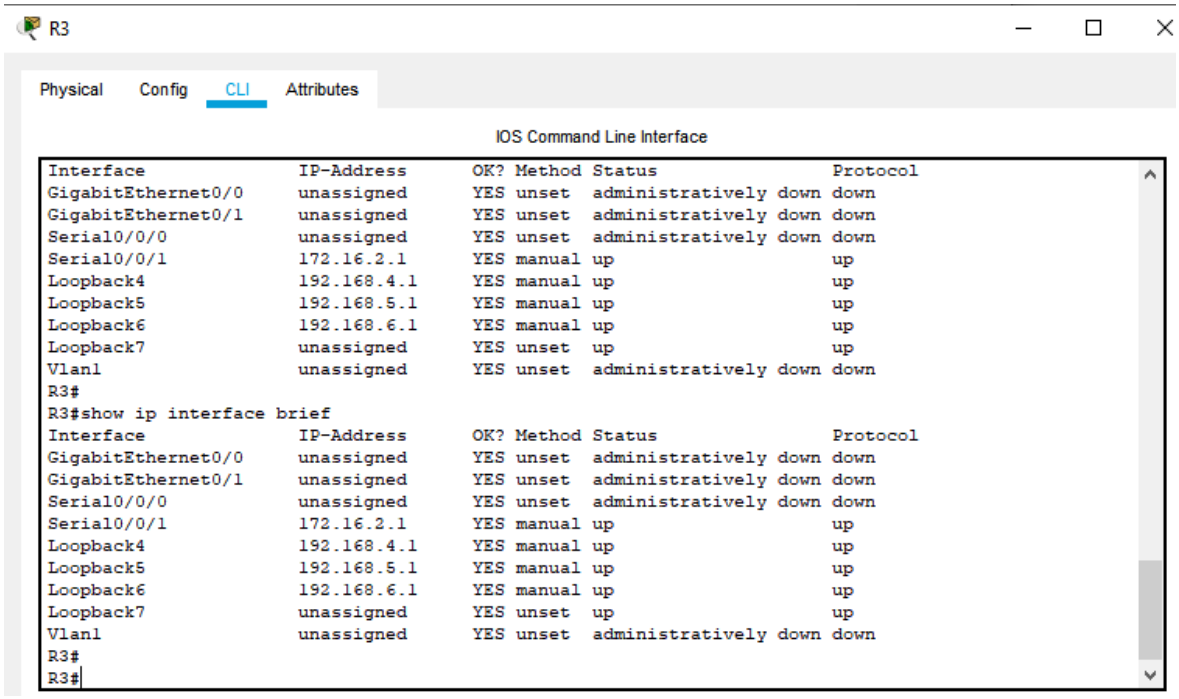
La configuración del R3 incluye las siguientes tareas:

Tabla 16 – Configuración R3 - Escenario 2

Elemento o tarea de configuración	Especificación
Configuramos los datos más importantes del router, nombre, contraseñas, y aprovechamos para encriptar las mismas.	No ip domain-lookp Hostname R3 Enable secret class Line console 0 Password cisco Login Line vty 0 15 Password cisco Login Service password-encryption
Le configuramos a este router igualmente el mensaje del mismo y configuramos las interfaces:	Banner moptd % User Access Verification % Configuramos las interaces: Interface s0/0/1 Description conexión con R2 Ip address 172.16.2.1 255.255.255.252 Ipv6 address 2001:db8:acad:2::1/64 No shutdown Int loopback 4 Ip address 192.168.4.1 255.255.255.0
Creamos con el comando indicado las Rutas por defecto IPV4 como IPV6.	Ip route 0.0.0.0 0.0.0.0 s0/0/1 Ipv6 route ::/0 s0/0/1
Configuramos en este equipo cada una de las interfaces LOOPBACK, para ello empleamos el siguiente comendo:	Int loopback 5 Ip address 192.168.5.1 255.255.255.0

	Int loopback 6 Ip address 192.168.6.1 255.255.255.0 Int loopback 7 Ipv6 address 2001:db8:acad:3::1/64

Figura 16 SHOW IP INTERFACE BRIEF, vemos configuracion de interfaces.



Fuente: autor.

Con la aplicación del comando SHOW IP INETRFACE BRIEF observamos la configuración realizada en el R3 en cada una de sus interfaces, la IP asignada y el estado de las mismas.

Paso 5: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 17 – Configuración S1 - Escenario 2

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	En este caso aplicamos el commando: “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	En este caso aplicamos el commando: Service password-encyption
Mensaje MOTD	Se prohíbe el acceso no autorizado.

Paso 6: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 18 – Configuración S3 - Escenario 2

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	En este caso aplicamos el commando: No ip domain lookup
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	En este caso debemos aplicar el comando: Service password-encyption
Mensaje MOTD	Se prohíbe el acceso no autorizado.

Paso 7: Verificar la conectividad de la red

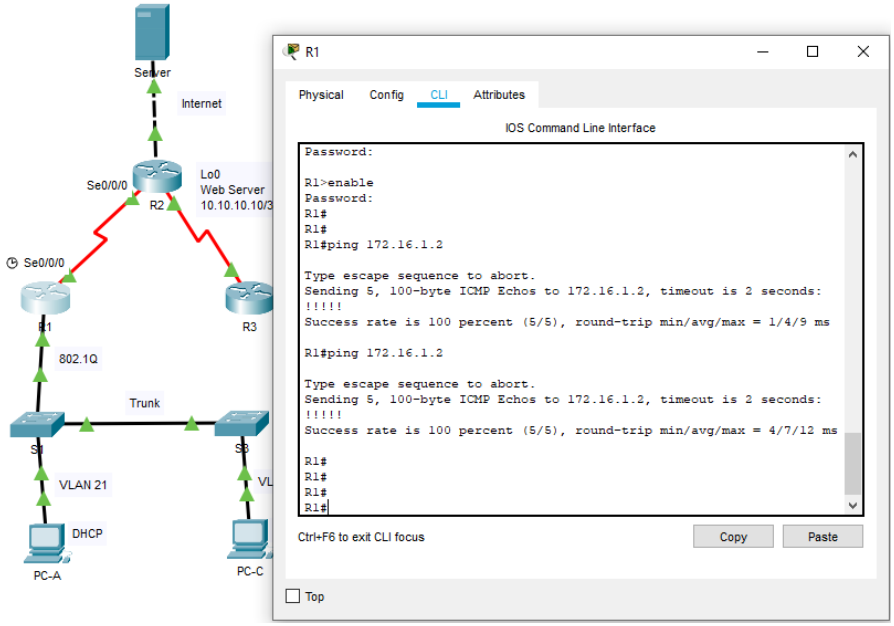
Utilice el comando **ping** para probar la conectividad entre los dispositivos de red.

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:

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	209.165.200.233	Exitoso

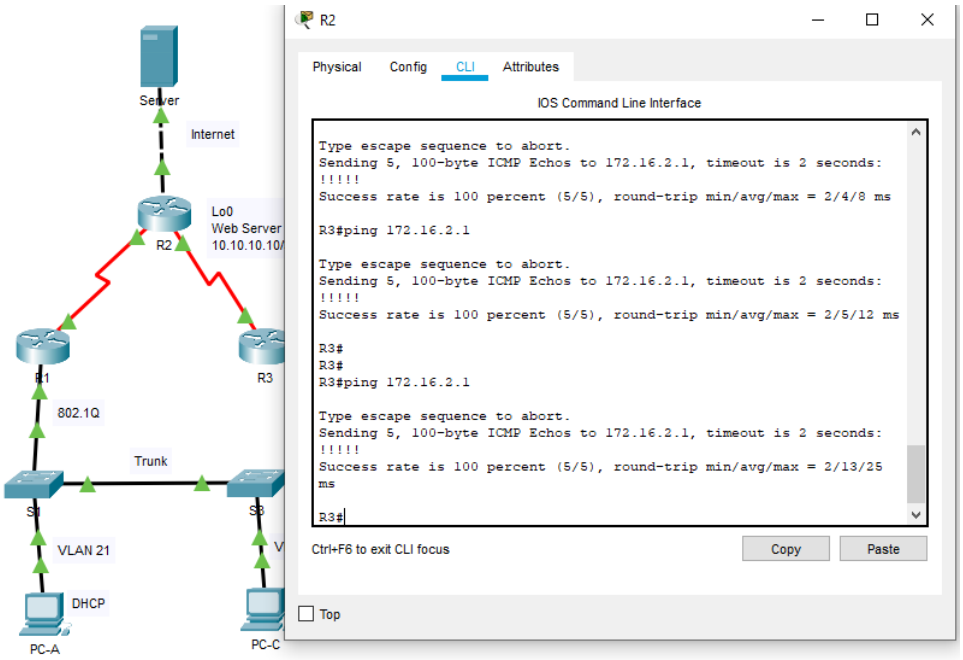
Nota: Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente.

Figura 17 PING desde R1 hacia diferentes puntos de la red.



Fuente: Autor

Figura 17 PING desde R2 hacia diferentes puntos de la red.



Fuente: Autor

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 19 – Configuración S1 - Escenario 2

Elemento o tarea de configuración	Especificación
El proceso a seguir para configurar las VLAN es el siguiente:	Vlan 21 **(creamos la VLAN)** Name accounting **(asignamos un nombre a la misma)** Vlan 23 Name engineering Vlan 99 Name management
ASIGNE LA IP a la VLAN MANAGEMET	Interface vlan 99 Ip address 192.168.99.2 255.255.255.0

	No shutdown
Asigne la puerta de enlace predeterminada	Ip default-gateway 192.168.99.1
Forzar un enlace troncal	Int f 0/3 **(ingresamos a la interfaz adecuada)** Switchport mode trunk **(configuramos modo troncal)** Switchport trunk native vlan 1 **(acceso a la vlan 1)** Int f 0/5 Switchport mode trunk Switchport trunk native vlan 1 Int range f0/1-2, f0/4, f0/6-24, g0/1-2 **(desactivamos todas estas interfaces)** Switchport mode access
Asignar f0/6 a la VLAN 21 Int f 0/6 Switch port acces vlan 21	Int f 0/6 Switch port acces vlan 21
Apague todos los puertos sin usar	Int range f0/1-2, f0/4, f0/7-24, g0/1-2 Shutdown

Paso 2: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 20 – Configuración S3 - Escenario 3

Elemento o tarea de configuración	Especificación
Crear la base de datos de la VLAN Creamos la base de datos de la VLAN según la tabla de la topología	Vlan 21 **(creamos la VLAN)** Name accounting **(asignamos un nombre a la VLAN)** Vlan 23

	Name engineering Vlan 99 Name management
ASIGNE LA IP a la VLAN MANAGEMET	Interface vlan 99 Ip address 192.168.99.3 255.255.255.0 No shutdown
Asigne la puerta de enlace predeterminada	Ip default-gateway 192.168.99.1
Forzar un enlace troncal	Int f 0/3 Switchport mode trunk Switchport trunk native vlan 1
Configurar todos los otros puertos como acceso	Int range f0/1-2, f0/4-24, g0/1-2 Switchport mode access
Asigne la f0/18 a la VLAN 23	Int f0/18 Siwtchport Access vlan 23
Apague todos los puertos sin usar	Int range f0/1-2, f0/4-17, f0/19-24, g0/1-2 Shutdown

Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 21 – Configuración R1 - Escenario 2

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 ***interface GigabitEthernet0/1.21*** ***description VLAN 21*** ***encapsulation dot1Q 21*** ***ip address 192.168.21.1 255.255.255.0***
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 ***interface GigabitEthernet0/1.23*** ***description VLAN 23*** ***encapsulation dot1Q 23*** ***ip address 192.168.23.1 255.255.255.0***
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 ***interface GigabitEthernet0/1.99*** ***description VLAN 99*** ***encapsulation dot1Q 99*** ***ip address 192.168.99.1 255.255.255.0***
Activar la interfaz G0/1	***interface GigabitEthernet0/1*** ***no shutdown***

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 21 – prueba de conectividad VLAN S1,S2 y S3.

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

Figura 19 Ping S1 a 192.168.99.1

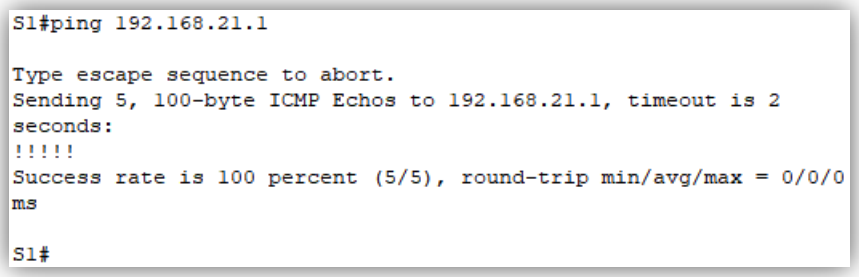
```
S1#ping 192.168.99.1

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

S1#
```

Fuente: Autor

Figura 20 Ping S1 a 192.168.21.1



Fuente: Autor

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:

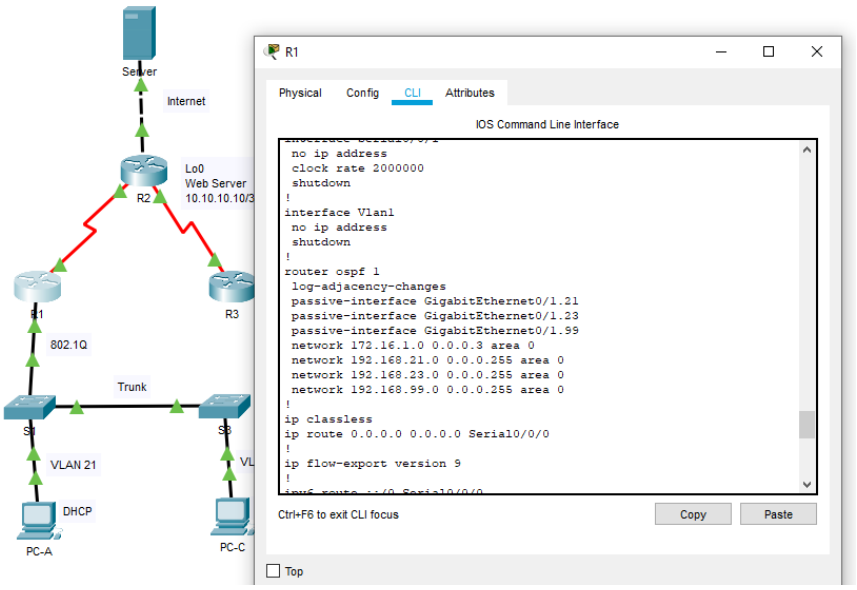
En nuestra red OSPF entra a cumplir funciones muy importantes, entre ellos para lo que fue hecho, permitir el intercambio de paquetes entre redes distantes, redes que no están conectadas directamente, el proceso a realizar en los ROUTERS es el que indicamos a continuación.

Tabla 23 – Configuración OSPF en el R1 - Escenario 2

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	Commando. router ospf 1

Anunciar las redes conectadas directamente	Asigne todas las redes conectadas directamente. network 172.16.1.0 0.0.0.3 area 0 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.
Establecer todas las interfaces LAN como pasivas	*passive-interface GigabitEthernet0/1.21* *passive-interface GigabitEthernet0/1.23* *passive-interface GigabitEthernet0/1.99* .
Desactive la sumarización automática	No auto-summary.

Figura 21 Configuración R1 escenario 2



Fuente: Autor

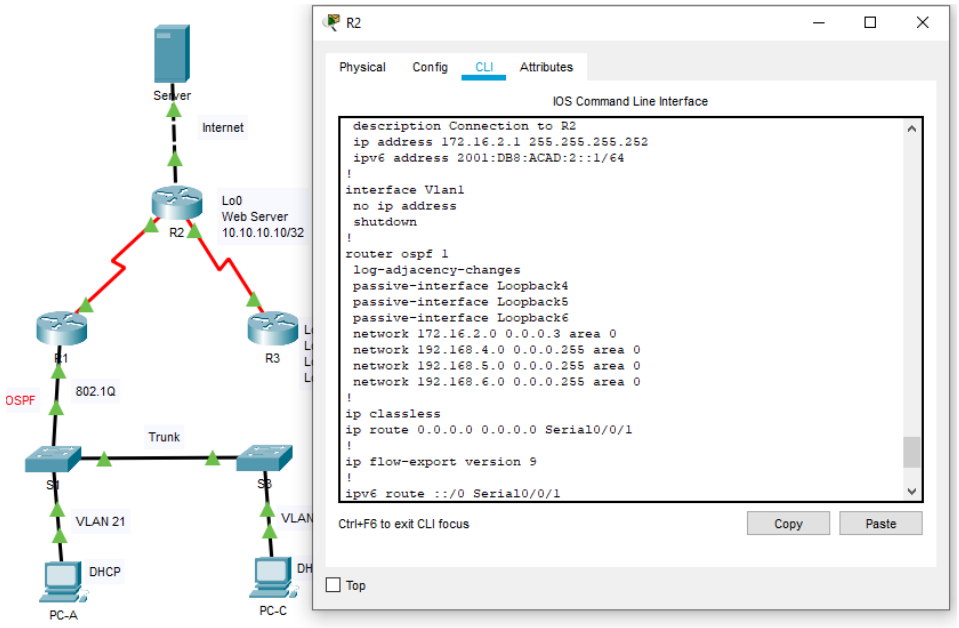
Paso 2: Configurar OSPF en el R2

La configuración del R2 incluye las siguientes tareas:

Tabla 24 – Configuración OSPF en el R2 - Escenario 2

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	router ospf 1.
Anunciar las redes conectadas directamente	**Nota:** Omitir la red G0/0. network 10.10.10.10 0.0.0.0 area 0 network 172.16.1.0 0.0.0.3 area 0 network 172.16.2.0 0.0.0.3 area 0.
Establecer la interfaz LAN (loopback) como pasiva	passive-interface Loopback0.
Desactive la sumarización automática.	No auto summary.

Figura 22 Configuración R2 escenario 2



Fuente: Autor

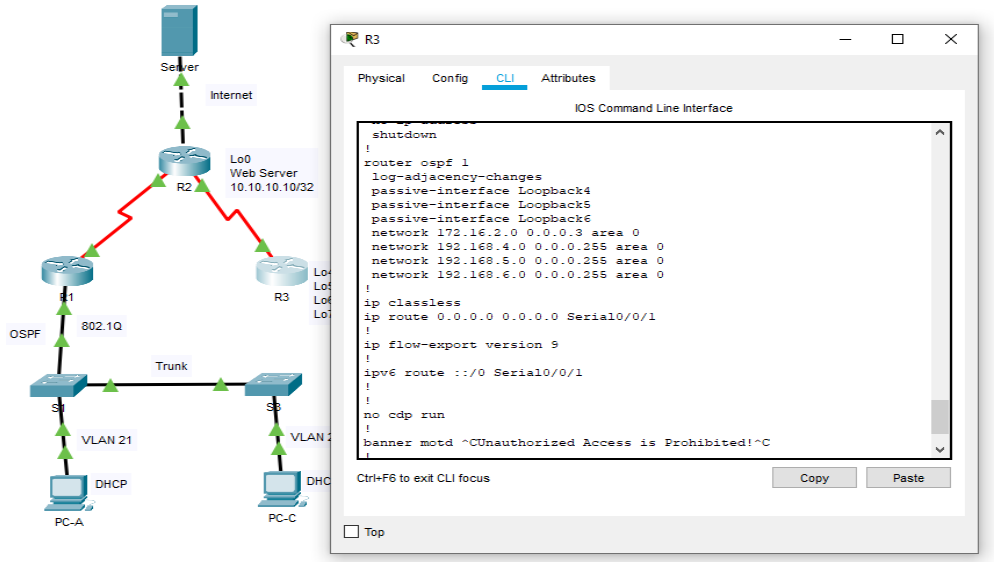
Paso 3: Configurar OSPFv3 en el R3

La configuración del R3 incluye las siguientes tareas:

Tabla 25 – Configuración OSPF en el R3 - Escenario 2

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	router ospf 1.
Anunciar redes IPv4 conectadas directamente	network 172.16.2.0 0.0.0.3 area 0 network 192.168.4.0 0.0.0.255 area 0 network 192.168.5.0 0.0.0.255 area 0 network 192.168.6.0 0.0.0.255 area 0.
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	passive-interface Loopback4 passive-interface Loopback5 passive-interface Loopback6.
Desactive la sumarización automática.	No auto-summary.

Figura 23 Configuración R3 escenario 2



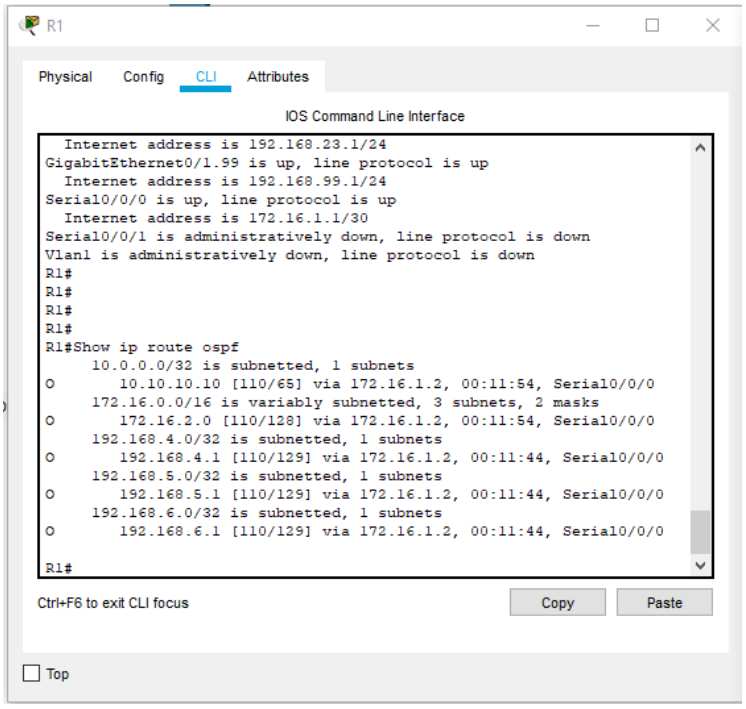
Fuente: Autor

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:

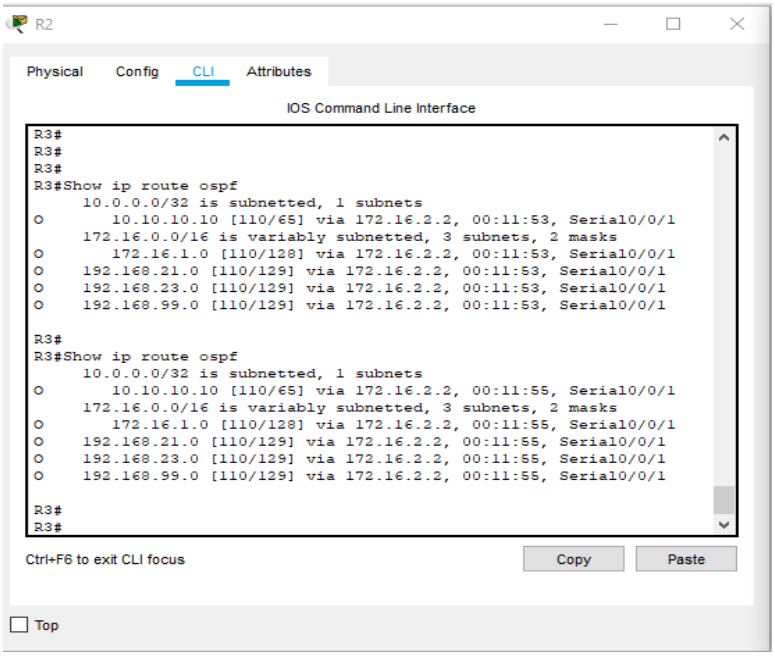
Pregunta	Respuesta
¿Con qué comando se muestran la ID del proceso OSPF, la ID del router, las redes de routing y las interfaces pasivas configuradas en un router?	*Show protocols* .
¿Qué comando muestra solo las rutas OSPF?	*Show ip route ospf*

Figura 24 verificación de OSPF en R1.



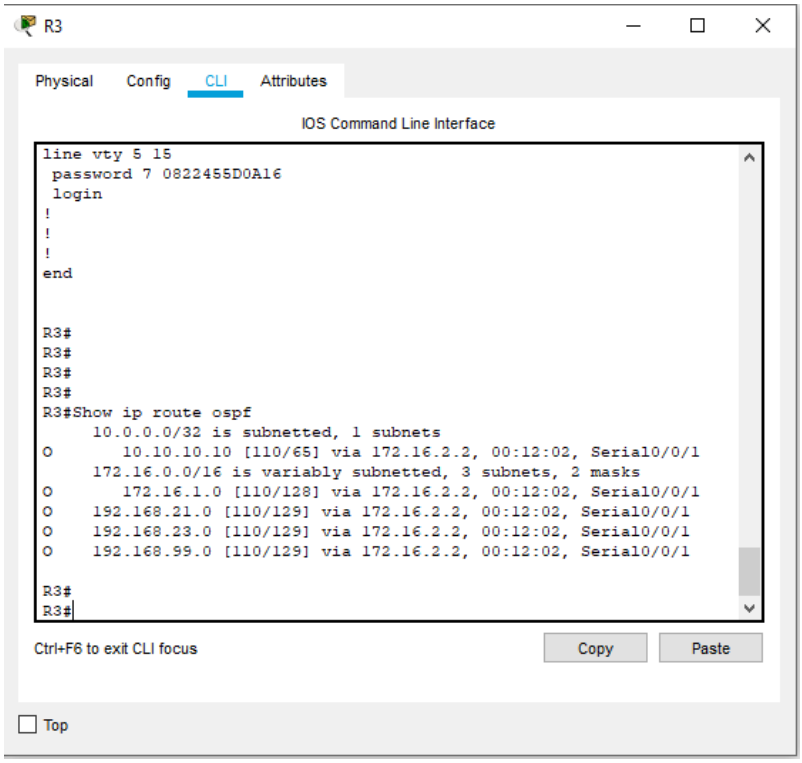
Fuente: Autor.

Figura 25 verificación de OSPF en R2.



Fuente: Autor.

Figura 26 verificación de OSPF en R3.



Fuente: Autor.

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 26 – Configuración de DHCP en R1

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	ip dhcp excluded-address 192.168.21.1 192.168.21.20
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
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 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.
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 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

Figura 27 DHCP VLAN escenario 2

```
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCil
!
!
ip dhcp excluded-address 192.168.21.1 192.168.21.20
ip dhcp excluded-address 192.168.23.1 192.168.23.20
!
```

Fuente: Autor

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

La configuración del R2 incluye las siguientes tareas:

Tabla 27 – Configuración de DHCP y NAT en R2

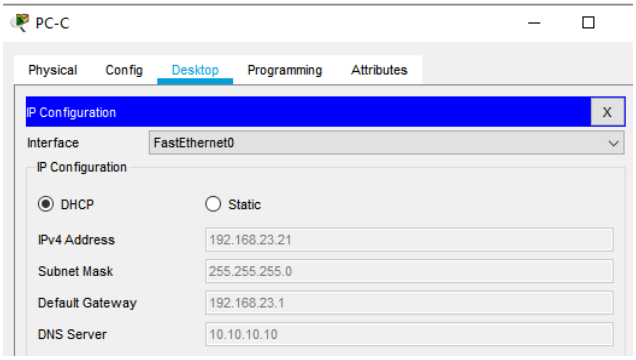
Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario	Nombre de usuario: **webuser** Contraseña: **cisco12345** Nivel de privilegio: **15** username webuser privilege 15 secret 5 cisco12345.
Habilitar el servicio del servidor HTTP	ip http server
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	ip http authentication local
Crear una NAT estática al servidor web.	Dirección global interna: **209.165.200.229** ip nat inside source static 10.10.10.10 209.165.200.237.

Asignar la interfaz interna y externa para la NAT estática	interface lo0 ip nat inside interface g0/0 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 access-list 1 permit 192.168.21.0 0.0.0.255 access-list 1 permit 192.168.23.0 0.0.0.255 access-list 1 permit 192.168.4.0 0.0.3.255.
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	ip nat inside source list 1 pool INTERNET

Paso 3: Verificar el protocolo DHCP y la NAT estática

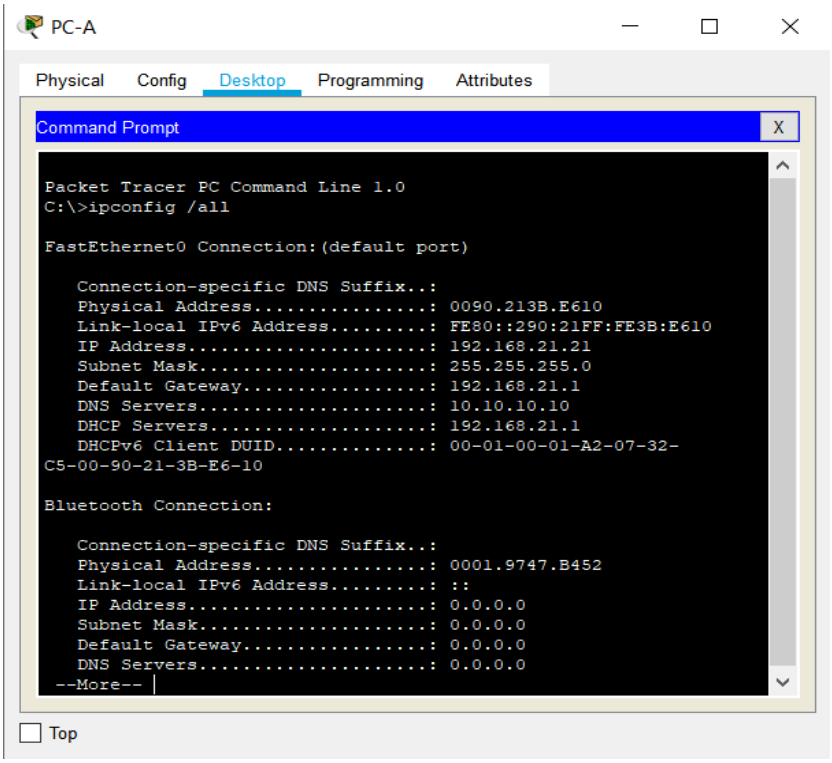
Utilice las siguientes tareas para verificar que las configuraciones de DHCP y NAT estática funcionen de forma correcta. Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente.

Tabla 28 – Verificamos funcionamiento de DHCP y NAT en R2

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	C:\>ipconfig /all FastEthernet0 Connection:(default port) Connection-specific DNS Suffix..: Physical Address.....: 0090.213B.E610 Link-local IPv6 Address.....: FE80::290:21FF:FE3B:E610 IP Address.....: 192.168.21.21 Subnet Mask.....: 255.255.255.0 Default Gateway.....: 192.168.21.1 DNS Servers.....: 10.10.10.10 DHCP Servers.....: 192.168.21.1 DHCPv6 Client DUID.....: 00-01-00-01-A2-07-32-C5-00-90-21-3B-E6-10
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	*Figura 27: PC-C con DHCP.* 
Verificar que la PC-A pueda hacer ping a la PC-C **Nota:** Quizá sea necesario deshabilitar el firewall de la PC.	C:\>ping 192.168.23.21 Pinging 192.168.23.21 with 32 bytes of data: Request timed out. Reply from 192.168.23.21: bytes=32 time=1ms TTL=127 Reply from 192.168.23.21: bytes=32 time<1ms TTL=127 Reply from 192.168.23.21: bytes=32 time<1ms TTL=127 Ping statistics for 192.168.23.21: Packets: Sent = 4, Received = 3, Lost = 1 (25% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 1ms, Average = 0ms

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**	El navegador debe mostrar a ventana de inicio de sesión que solicita usuario y contraseña, packet tracer no soporta este procedimiento.

Figura 28 IPCONFIG PC-A escenario 2



Fuente: Autor

Procedemos a configurar ahora el protocolo en tiempo de red.

Configurar NTP

Tabla 29 – configuración de NTP en los 3 ROUTERS.

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	**5 de marzo de 2016, 9 a. m.** clock set 09:00:00 5 March 2016
Configure R2 como un maestro NTP.	Nivel de estrato: **5** ntp manster 5
Configurar R1 como un cliente NTP.	Servidor: **R2**
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	ntp update-calendar
Verifique la configuración de NTP en R1.	R1#show ntp associations address ref clock st when poll reach delay offset disp *~172.16.1.2 127.127.1.1 5 2 64 1 4.00 1.00 0.00 * sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured

Parte 6: Configurar y verificar las listas de control de acceso (ACL)

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

Tabla 30 – configuración de las ACL, listas de control de acceso y restricciones VTY.

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	transport input telnet
Verificar que la ACL funcione como se espera	R1#telnet 172.16.1.2 Trying 172.16.1.2 ...OpenUnauthorized Access is Prohibited!^ User Access Verification Password: R2>en Password: R2#

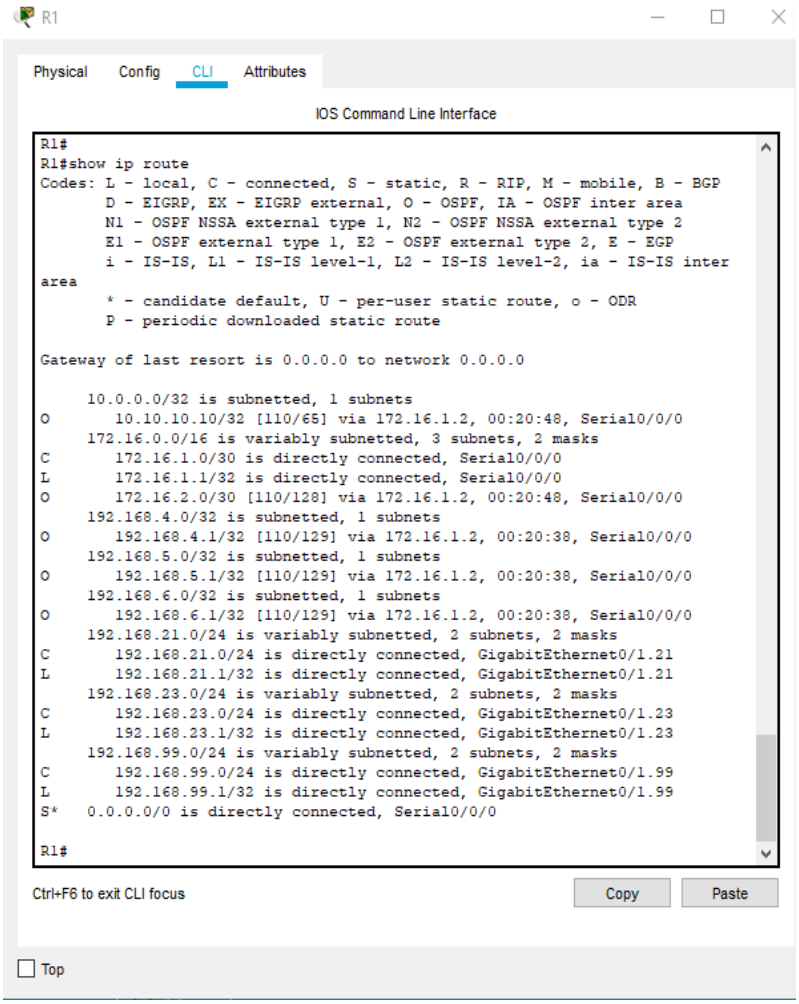
Paso 2: Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente

Tabla 31 – comandos de verificación desde la CLI.

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-lists
Restablecer los contadores de una lista de acceso	clear ip access-list counters
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	show ip interface
¿Con qué comando se muestran las traducciones NAT?	**Nota:** Las traducciones para la PC-A y la PC-C se agregaron a la tabla cuando la computadora de Internet intentó hacer ping a esos equipos en el paso 2. Si hace ping a la computadora de Internet desde la PC-A o la PC-C, no se agregarán las traducciones a la tabla debido al modo de simulación de Internet en la red.

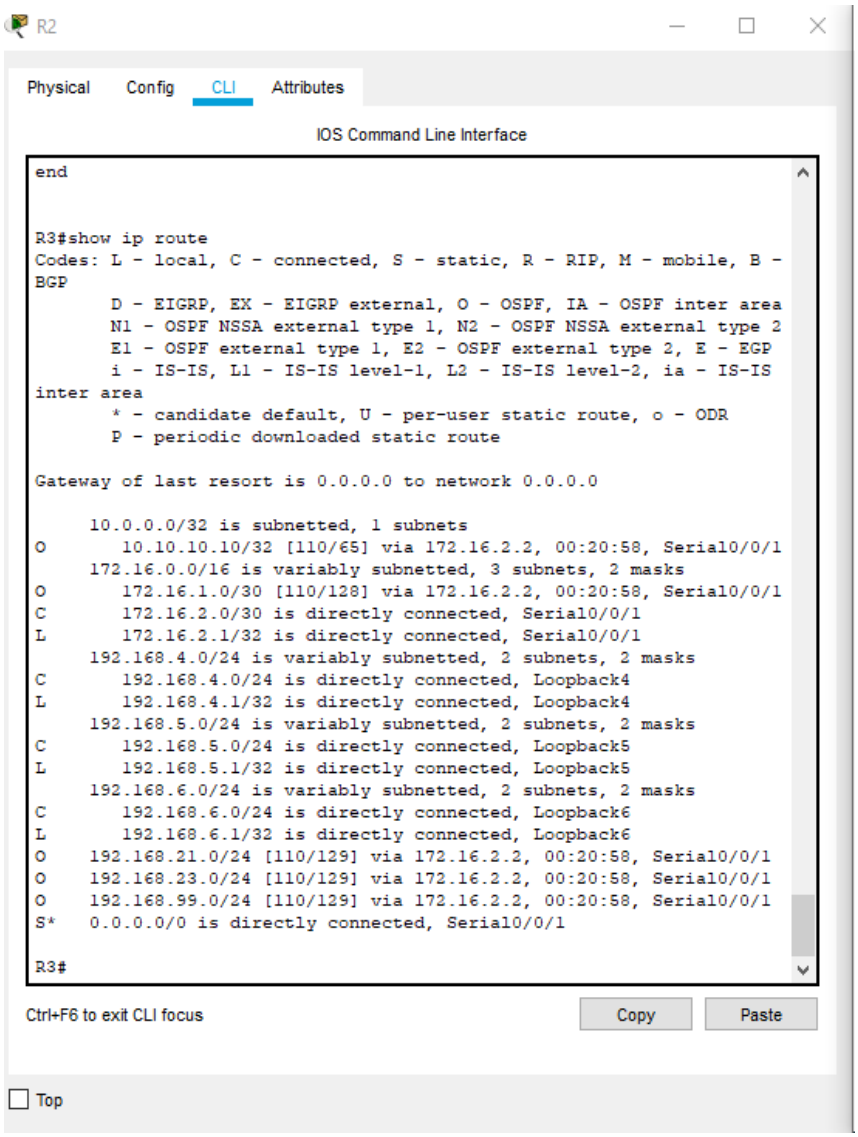
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	clear ip nat translations *

Figura 29 – show ip route R1, verificamos las rutas de cada uno de los routers.



Fuente: autor.

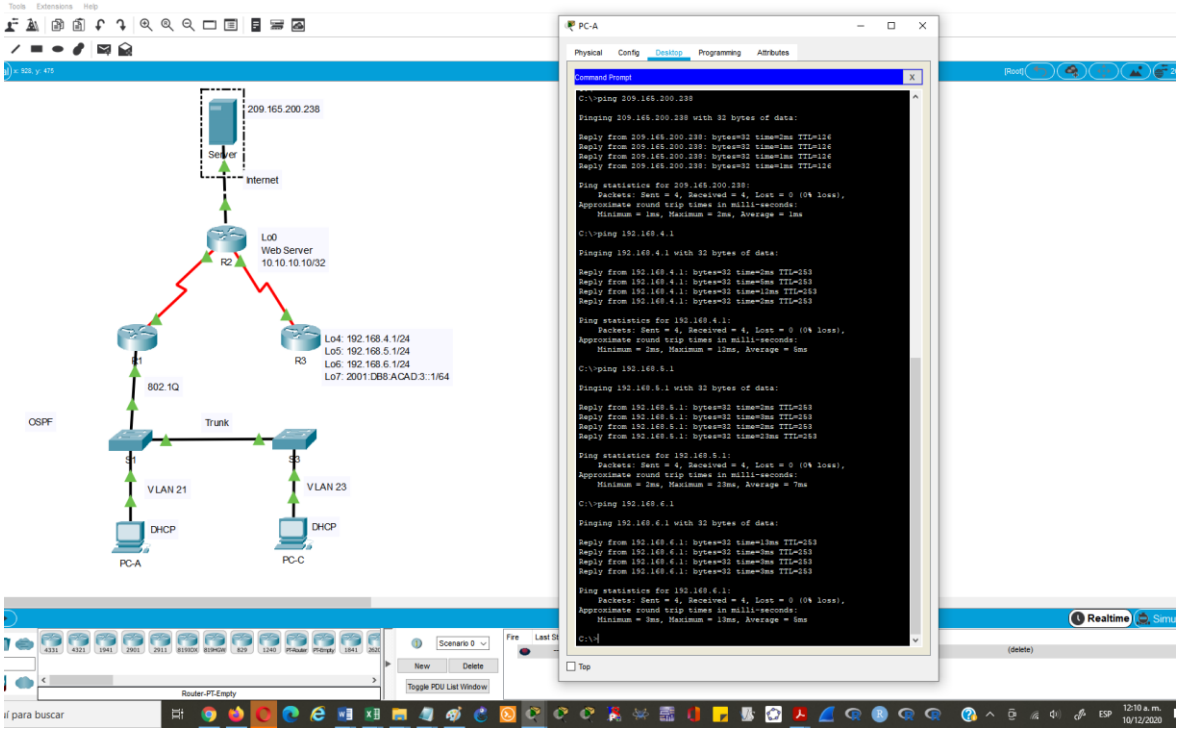
Figura 30 – show ip route – R2, verificamos las rutas de cada uno de los routers.



Fuente: autor.

PRUEBA DE CONECTIVIDAD ESCENARIO 2.

Figura 32 – PING desde el PC-A hacia los diferentes puntos de la red.



Fuente: autor.

La prueba anterior la hemos realizado desde la PCA hacia los puntos más lejanos de la red, entre ellos R3 y además el servidor, cada uno de ellos resulto satisfactorio.

CONCLUSIONES

- Hemos desarrollarlo dos redes corporativas empleando tecnología CISCO, gracias a lo cual nos permitió profundizar mucho más en este mundo de las telecomunicaciones.

- Comprendemos la forma como emplear los comandos básicos de configuración para los diferentes dispositivos que hacen parte de la red, desde la forma de cómo configurar los nombres hasta la forma de cómo se crean las VLAN, como se asigna seguridad a los dispositivos, como se enrutan los paquetes entre diferentes redes, subredes.

- El desarrollo de esta actividad nos ha permitido aplicar todo el conocimiento adquirido a lo largo de nuestra vida estudiantil.

- Haciendo énfasis en los conocimientos adquiridos a lo largo de este diplomado de profundización, correspondientes a los aspectos básicos y elementos de las redes de telecomunicaciones y técnicas de conmutación. Entre algunos de esos temas se encuentran los protocolos, servicios de seguridad de redes, modelos capa OSI y TCP/IP, configuración de dispositivos y enrutamientos, entre otros.

BIBLIOGRAFÍA Y WEBGRAFIA.

- Modulo CCNA2 Exploration 4.0. Conceptos y protocolos de enrutamiento. CISCO NetworkingAcademy.

- CISCO NETWORKING ACADEMY CCNA EXPLORATION 4.0. Conceptos y protocolos de enrutamiento, Fundamentos de Networking. Cisco Systems. 2008.

- CISCO NETWORKING ACADEMY CCNA EXPLORATION 4.0. Conceptos y protocolos de enrutamiento, Principios de enrutamiento. Cisco Systems. 2007

- WIKIPEDIA ENCICLOPEDIA LIBRE. Máscaras de Red < http://es.wikipedia.org/wiki/M%C3%A1scara_de_red> [citado 5 julio 2010]

ANEXOS

Anexo 1 Link Descarga Escenario 1

https://drive.google.com/file/d/1ZYeEJy6DEy8E6ArUZT6ri4qiYAA62Z80/view?usp=sharing

Anexo 2 Link Descarga Escenario 2

https://drive.google.com/file/d/12R6S_BkAYZbCcyvXIlHNvd32S7SlY6cq/view?usp=sharing

Anexo 3 Link Video de Sustención

https://www.youtube.com/watch?v=-InFtk19wFA&feature=youtu.be

Solución De Dos Escenarios Presentes En Entornos corporativos Bajo El Uso De Tecnología Cisco

EDWIN AUGUSTO VIRGUEZ
Universidad Nacional Abierta y a Distancia UNAD, eavirguezv@unadvirtual.edu.co

Resumen

El desarrollo de la presente actividad es de vital importancia para mí, pues he aplicado cada uno de los temas que a lo largo de mi proceso de estudio miré, las redes configuradas son 2 casos aplicados a una empresa corporativa, CASOS muy reales ajustados a problemas que muy seguramente vamos a tratar dentro de la vida profesional que nos espera.

Vamos a desarrollar una serie de actividades a lo largo de esta práctica en la cual buscamos que nos familiaricemos de una manera mucho más amena con todos los dispositivos y elementos que hacen parte de la red ya que podemos distinguir cada una de sus diferencias y posibilidades que se nos presentan.

Todo el montaje de la red la realizamos dentro del simulador, magnífica herramienta desarrollada por CISCO, llamada PACKET TRACER, gracias a este podemos ejecutar gran parte de los comandos que se pueden configurar dentro de los dispositivos reales.

Esperamos este trabajo sea del agrado de todos ustedes.

Palabras clave: CISCO, PACKET TRACER, VLSM, IPV4, IPV6, ROUTING.

Abstract:

The development of this activity is of vital importance to me, since I have applied each of the topics that I looked at throughout my study process, the configured networks are 2 cases applied to a corporate company, very real CASES adjusted to problems that we will very surely deal with within the professional life that awaits us.

We are going to develop a series of activities throughout this practice in which we seek to familiarize ourselves in a much more enjoyable way with all the devices and elements that are part of the network since we can distinguish each of their differences and possibilities that are presented to us.

All the assembly of the network is carried out within the simulator, a magnificent tool developed by CISCO, called PACKET TRACER, thanks to this we can execute a large part of the commands that can be configured within the real devices.

Keywords— *CISCO, PACKET TRACER, VLSM, IPV4, IPV6, ROUTING.*

I. INTRODUCCIÓN

Nuestra época definitivamente es un periodo de cambio, de revolución y de muchos avances tecnológicos donde cómo podemos observar las telecomunicaciones han jugado un papel supremamente importante.

Vemos entonces que es muy importante el hecho de que dentro de nuestra formación profesional tengamos un amplio conocimiento acerca de las redes de datos, y que mejor manera que podamos afianzar y mejorarlos a través de una ACTIVIDAD PRACTICA de estos 2 ESCENARIOS, escenarios que son muy similares a aspectos reales y que muy posiblemente encontraremos en nuestra vida profesional.

En primera instancia comenzaremos desarrollando un pequeño ejercicio en el cual aplicaremos el direccionamiento IPV4 empleando VLSM y además configuraremos el protocolo RIP, con el fin de observar su funcionamiento. Continuaremos en el SEGUNDO ESCENARIO caso a desarrollar una propuesta con el fin de mejorar considerablemente la red que en la actualidad posee, aplicaremos VLSM lo que nos permitirá un menor desperdicio de direcciones IP, además trabajaremos por consiguiente con protocolos como son EIGRP, OSPF y RIP V2. Estos protocolos trabajan de una manera mucho más eficiente, calculan sus rutas empleando algoritmos mucho más especializados dependiendo de cada una de las circunstancias.

II. TIPOS DE ARTÍCULOS PUBLICABLES

El desarrollo de esta actividad es el tipo de INVESTIGACIÓN APLICADA pues pretendemos a través de la implementación de 2 redes Corporativas aplicar y afianzar los conocimientos adquiridos.

1. **Artículo de investigación científica y tecnológica:** Documento que presenta, de manera detallada, los resultados originales de proyectos de investigación. La estructura debe contener las siguientes partes:

    - Resumen
    - Introducción
    - Metodología
    - Resultados

- Conclusiones.
- Referencias bibliográficas (mínimo 15)

III. IMPLEMENTACIÓN Y CONFIGURACIÓN.

Partimos de una topología dada que consta de un Router 4331, dos switch 3560 conectados entre sí por dos interfaces que forman un enlace troncal y dos PC de escritorio y se estructuran de la siguiente manera en la aplicación de Cisco Packet Tracer:

Escenario 1

TOPOLOGÍA

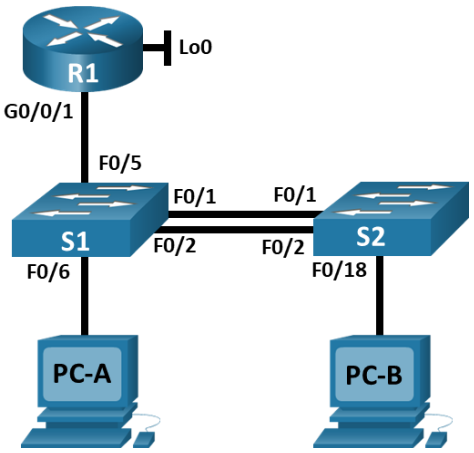


Figura 1Topología propuesta escenario 1

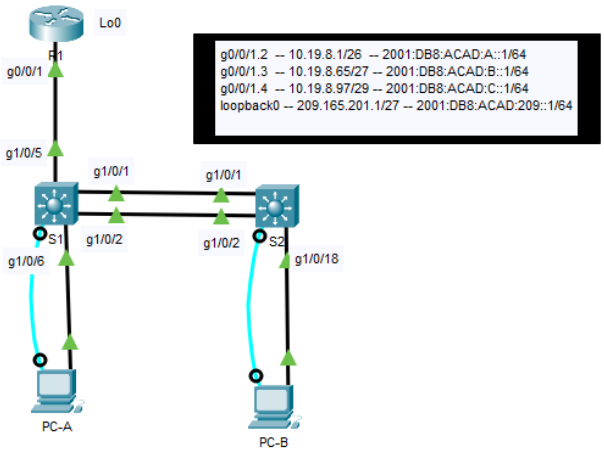


Figura 2 Topología desarrollada escenario 1 PKT.

En este primer escenario se configurarán los dispositivos de una red pequeña. Debe configurar un router, un switch y equipos que admitan tanto la conectividad IPv4 como IPv6 para los hosts soportados. El router y el switch también deben administrarse de forma segura. Configurará el enrutamiento entre VLAN, DHCP, Etherchannel y port-security.

TABLA DE VLAN

VLAN	Nombre de la VLAN
2	Bikes
3	Trikes
4	Management
5	Parking
6	Native

Tabla 1 - VLAN.

TABLA DE DIRECCIONAMIENTO ESCENARIO 1.

Dispositivo / interfaz	Dirección IP / Prefijo	Puerta de enlace predeterminada
R1 G0/0/1.2	10.19.8.1 /26	No corresponde
R1 G0/0/1.2	2001:db8:acad:a: :1 /64	No corresponde
R1 G0/0/1.3	10.19.8.65 /27	No corresponde
R1 G0/0/1.3	2001:db8:acad:b: :1 /64	No corresponde
R1 G0/0/1.4	10.19.8.97 /29	No corresponde
R1 G0/0/1.4	2001:db8:acad:c: :1 /64	No corresponde
R1 G0/0/1.6	No corresponde	No corresponde
R1 Loopback0	209.165.201.1 /27	No corresponde
R1 Loopback0	2001:db8:acad:209: :1 /64	No corresponde
S1 VLAN 4	10.19.8.98 /29	10.19.8.97
VLAN S1 4	2001:db8:acad:c: :98 /64	No corresponde
S1 VLAN 4	fe80: :98	No corresponde
S2 VLAN 4	10.19.8.99 /29	10.19.8.97
S2 VLAN 4	2001:db8:acad:c: :99 /64	No corresponde
S2 VLAN 4	fe80: :99	No corresponde
PC-A NIC	Dirección DHCP para IPv4	DHCP para puerta de enlace predeterminada IPv4
PC-A NIC	2001:db8:acad:a: :50 /64	fe80::1
PC-B NIC	DHCP para dirección IPv4	DHCP para puerta de enlace predeterminada IPv4
PC-B NIC	2001:db8:acad:b: :50 /64	fe80::1

Tabla 2 - TABLA DE DIRECCIONAMIENTO.

Nota: No hay ninguna interfaz en el router que admita VLAN 5.

Esta es la tabla más importante para el diseño de la red, ya que en ella se resume el 100% de la asignación IP de la red en general.

CONFIGURACIÓN BÁSICA:

Primero que todo comenzamos nuestro proceso reiniciando cada uno de los dispositivos esto con el fin de evitar algún tipo de conflicto con posibles configuraciones anteriores, para ello debemos aplicar los siguientes comandos:

Erase-startup-config
Delete vlan.dat
Reload

Aplicamos en cada uno de los dispositivos más comunes en la configuración de cada uno de ellos, entre ellos son los siguientes, estos comandos se aplican tanto en los SWITCH como ROUTERS.

Tarea	Especificación
Desactivar la búsqueda DNS	No ip domain-lookup
Nombre del router	Hostname ___
Nombre de dominio	ccna-lab.com ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	Ciscoenpass Enable secret ciscoenpass
Contraseña de acceso a la consola	Ciscoconpass Line console 0 Password ciscoconpass Login
Establecer la longitud mínima para las contraseñas	10 caracteres Security passwords min-leng 10
Crear un usuario administrativo en la base de datos local	Nombre de usuario: **admin** Password: **admin1pass** Username admin secret admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	Line vt 0 15 login local
Configurar VTY solo aceptando SSH	Transport input ssh
Cifrar las contraseñas de texto no cifrado	Service password-encryption
Configure un MOTD Banner	Banner motd % Prohibido el acceso no autorizado %
Habilitar el routing IPv6	Ipv6 unicast-routing

Tabla 3 - CONFIGURACIÓN BÁSICA..

Procedemos a configurar tanto las interfaces como las sub-interfaces, proceso que debemos realizar siguiendo las indicaciones de la TABLA DE DIRECCIONAMIENTO, además de ello debemos agregar las respectivas DESCRIPCIONES a cada una de ellas, esto con el fin de que nos sirva de soporte. La configuración se hace tanto en IPV4 como en IPV6.

CONFIGURACIÓN DE VLANS, TRUNKING Y ETHERCHANNEL.

La tabla de las VLAN se nos fue indicada junto a la tabla de direccionamiento, en esta parte debemos crearlos dentro de cada uno de los dispositivos para lo cual empleamos los siguientes comandos:

Vlan 2
Name bikes
Vlan 3
Name trikes
Vlan 4
Name management
Vlan 5
Name parking
Vlan 6
Name native

Luego de haber hecho todo el proceso indicado solo nos queda proceder a verificar lo hecho, para esto debemos aplicar y emplear los siguientes comandos.

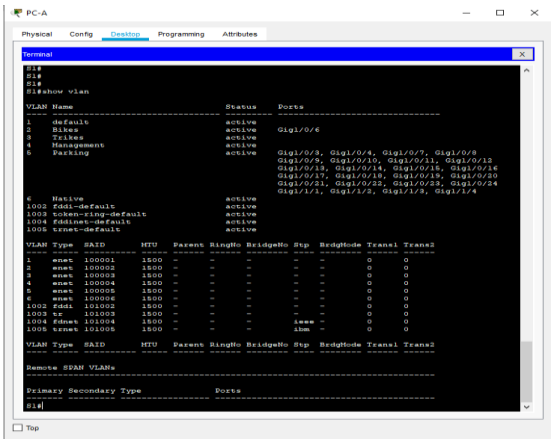


Figura 3 configuración S1 escenario 1

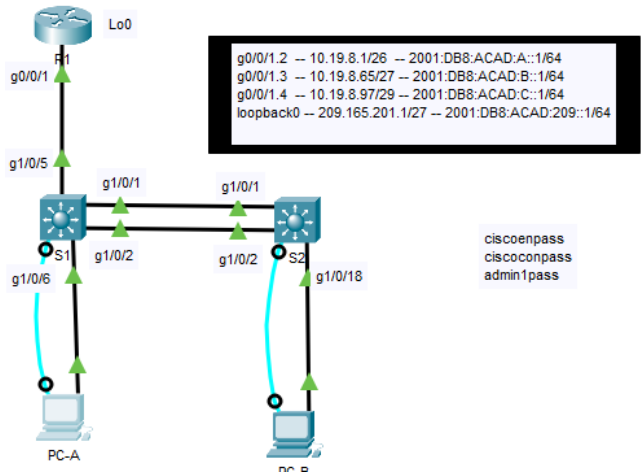


Figura 4 interfaces, PC, configuración IP.

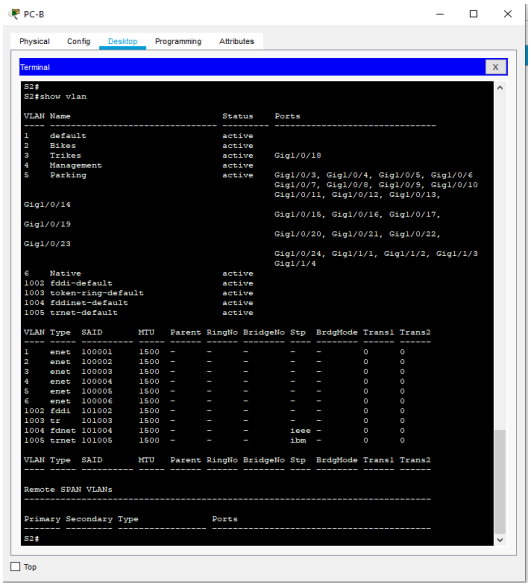


Figura 5 Activar etherchannel S1-S2 escenario 1

CONFIGURACIÓN RUTAS POR DEFECTO

En el Router 1 vamos a crear y configurar rutas por defecto, para lo cual empleamos los siguientes comandos:

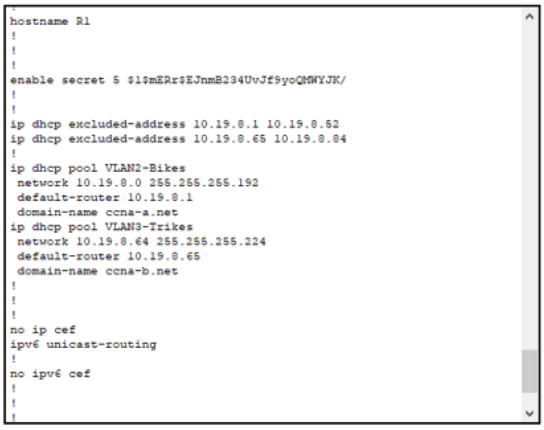
Ip route 0.0.0.0 0.0.0.0 loopback 0
Ipv6 route ::/0 loopback 0

CONFIGURACIÓN DHCP VLAN 1 y VLAN 2.

Debemos configurar ahora todo lo relacionado al direccionamiento DHCP, para lo cual debemos crear el POOL asignamos la red la ruta por defecto y el DOMINIO

Ip dhcp excluded-address 10.19.8.1 10.19.8.52

Ip dhcp POOL VLAN2-BIKES
Network 10.19.8.0 255.255.255.192
Default-route 10.19.8.1
Domain-name ccna-b.net



```
hostname R1
!
!
!
enable secret 5 $1$mERr$EJnmB234UvJf5yoQMWYJK/
!
!
ip dhcp excluded-address 10.19.8.1 10.19.8.52
ip dhcp excluded-address 10.19.8.65 10.19.8.84
!
ip dhcp pool VLAN2-Bikes
 network 10.19.8.0 255.255.255.192
 default-router 10.19.8.1
 domain-name ccna-a.net
ip dhcp pool VLAN3-Trikes
 network 10.19.8.64 255.255.255.224
 default-router 10.19.8.65
 domain-name ccna-b.net
!
!
!
no ip cef
ipv6 unicast-routing
!
no ipv6 cef
!
!
```

Figura 6 - DHCP en R1.

Verificamos que DHCP esté funcionando y asignando las direcciones correctas a los dispositivos dentro de cada una de las VLAN.

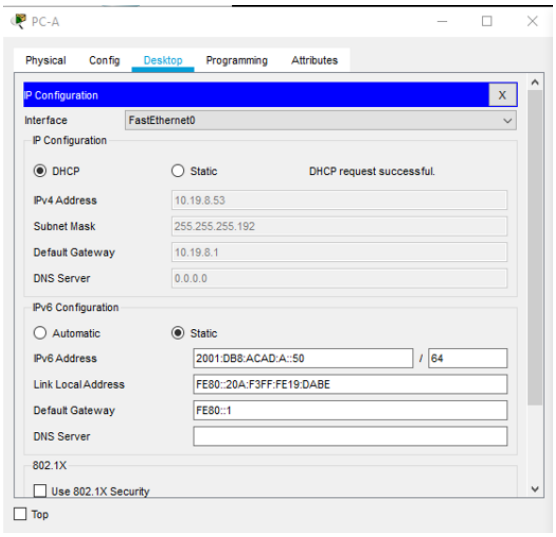


Figura 7 DHCP en PCA.

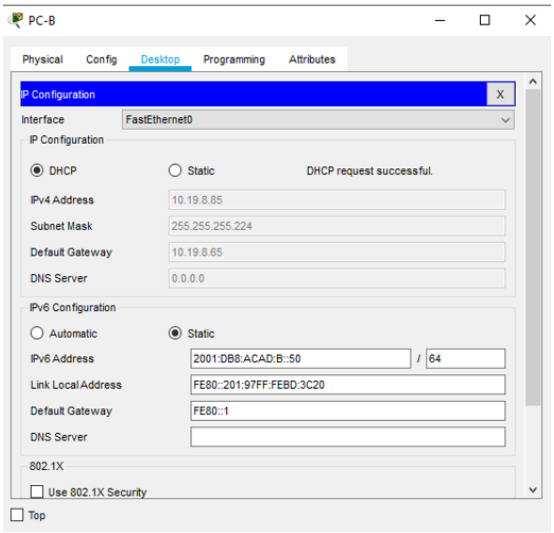


Figura 8 DHCP en PCA.

Nuestro proceso en este punto a finalizado, solo queda proceder a verificar si tenemos conectividad en cada uno de los puntos de la red.

Desde	**A**	**de Internet**	**Dirección IP**	**Resultados de ping**
PC-A	R1, G0/0/1.2	Dirección	10.19.8.1	*exitoso*
PC-A	*R1, G0/0/1.2*	IPv6	2001:db8:acad:a: :1	exitoso
PC-A	R1, G0/0/1.3	Dirección	10.19.8.65	exitoso
PC-A	*R1, G0/0/1.3*	IPv6	2001:db8:acad:b: :1	exitoso
PC-A	R1, G0/0/1.4	Dirección	10.19.8.97	exitoso
PC-A	*R1, G0/0/1.4*	IPv6	2001:db8:acad:c: :1	exitoso
PC-A	S1, VLAN 4	Dirección	10.19.8.98	exitoso
PC-A	*S1, VLAN 4*	IPv6	2001:db8:acad:c: :98	exitoso
PC-A	S2, VLAN 4	Dirección	10.19.8.99.	exitoso
PC-A	*S2, VLAN 4*	IPv6	2001:db8:acad:c: :99	exitoso
PC-A	PC-B	Dirección	IP address will vary.	exitoso
PC-A	*PC-B*	IPv6	2001:db8:acad:b: :50	exitoso
PC-A	R1 Bucle 0	Dirección	209.165.201.1	exitoso
PC-A	*R1 Bucle 0*	IPv6	2001:db8:acad:209: :1	exitoso
PC-B	R1 Bucle 0	Dirección	209.165.201.1	exitoso
PC-B	*R1 Bucle 0*	IPv6	2001:db8:acad:209: :1	exitoso
PC-B	R1, G0/0/1.2	Dirección	10.19.8.1	exitoso
PC-B	*R1, G0/0/1.2*	IPv6	2001:db8:acad:a: :1	exitoso
PC-B	R1, G0/0/1.3	Dirección	10.19.8.65	exitoso
PC-B	*R1, G0/0/1.3*	IPv6	2001:db8:acad:b: :1	exitoso
PC-B	R1, G0/0/1.4	Dirección	10.19.8.97	exitoso
PC-B	*R1, G0/0/1.4*	IPv6	2001:db8:acad:c: :1	exitoso
PC-B	S1, VLAN 4	Dirección	10.19.8.98	exitoso
PC-B	*S1, VLAN 4*	IPv6	2001:db8:acad:c: :98	exitoso
PC-B	S2, VLAN 4	Dirección	10.19.8.99.	exitoso
PC-B	*S2, VLAN 4*	IPv6	2001:db8:acad:c: :99	exitoso

Tabla 4 - TABLA de prueba de CONECTIVIDAD.

IV. Referencias

Las referencias son muy importantes, y se debe seguir el siguiente formato. El tamaño de letra es de 10 puntos:

Para artículos en revistas:

[1] [2]CISCO. (2019). Acceso a la red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#4

[2] Cortes Robles, D., 2015. Configurar DHCP Por VLAN En Equipos CISCO, Packet Tracer. [en linea] Seguridadyfirewall.cl. Disponible en: https://www.seguridadyfirewall.cl/2015/08/configurar-dhcp-por-vlan-en-equipos.html

[3] CISCO. (2017). Configuración de un sistema operativo de red. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#2.0.1.1

[4] Microsoft. (18 de Octubre de 2000). Introducción a Active Directory. Recuperado el 14 de Marzo de 2015, de http://support.microsoft.com/es-es/kb/196464/es

[5] CISCO. (2017). Capa de Aplicación. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module10/index.html#10.0.1.1

[6] Sites.google.com. n.d. 3.2 Enlaces Troncales De Las VLAN - MODULO 3 CISCO CCNA Exploration 3. [en linea] Disponible en: https://sites.google.com/site/paginamodulo3vlan/3-2-enlaces-troncales

[7] Camelo, L. (s.f.). Seguridad de la Información en Colombia. Recuperado el 20 de Abril de 2015, de http://seguridadinformacioncolombia.blogspot.com/2010/04/iso-27001-e-iso-27002-dominio-11.html

[8] 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#11

[9] CISCO. (2019). Configuración del Switch. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#5

[10] CISCO. (2019). Detección, Administración y Mantenimiento de Dispositivos. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#10
[11] CISCO. (2019). DHCP. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#8

BIOGRAFÍA

Edwin Augusto Virguez Vanegas (N'1987) nació en Colombia en el municipio de Villeta. El 09 de febrero de 1987. Se egresado del SENA como tecnólogo y actualmente cursa una carrera profesional en al Universidad Nacional Abierta y a Distancia UNAD.

Su experiencia laboral profesional incluye mas de 10 años en el área de las tecnologías y la computación, laborado en grandes empresas privadas como MPS Mayorista entre otra, publicas como el SENA y actualmente funcionario publica de planta por concurso de merito en la Alcaldía Municipal de la Vega Cundinamarca, como funcionario público aporta al mejoramiento de la comunidad