PRUEBA DE HABILIDADES PRACTICAS CCNA

ALEJANDRO MUÑOZ FORERO

UNIVERSIDAD NACIONAL ABIERTA YA DISTANCIA UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA
PROGRAMA DE INGENIERIA ELECTRONICA
SANTIAGO DE CALI
2020

PRUEBA DE HABILIDADES PRACTICAS CCNA

Diplomado de Profundización Cisco (Informe final para recibir el título de Ingeniero Electrónico)

TUTORA
Ingeniera Paulita Flor Salazar

UNIVERSIDAD NACIONAL ABIERTA YA DISTANCIA UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA
PROGRAMA DE INGENIERIA ELECTRONICA
SANTIAGO DE CALI
2020

Nota de Aceptación

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Santiago de Cali, 26 de Noviembre de 2020

Dedico este trabajo a todas las personas que se esfuerzan y trabajan por lograr sus sueños y su proyecto de vida, y a mi padre que ya no está con nosotros.

AGRADECIMIENTOS

Agradezco en primera medida a Dios por darme la fortaleza y persistencia todos estos años de estudio, las cuales han sido fundamentales para lograr este, mi proyecto de vida. También a mi madre, a mi esposa y a la familia Moncada Alvarez, por confiar en mi y estar en los momentos en que más los he necesitado y a todas esas personas que de una u otra manera han sido parte de mi proceso de formación, como profesional y ser humano.

Por último, agradezco a la universidad UNAD, por dejarme ser parte de esta gran institución educativa, a los tutores y compañeros virtuales y presenciales los cuales han sido primordial para mi avance hasta el punto de finalización de este proyecto.

CONTENIDO

Pág.

INDICE DE TABLAS

INDICE DE FIGURAS.

GLOSARIO

VLAN: Es una red de área local virtual.

DHCP: Protocolo el cual asigna direcciones IP predeterminadas a los hosts dentro de una red local.

IPV4: Es un sistema direccional de 32 bits el cual es utilizado para identificación de un dispositivo en una red.

DIRECCION MAC: Está formado por 48 bytes o 0x12 F el cual está representado en hexadecimal.

ENCAPSULACION: Proceso el cual consiste en colocar un mensaje dentro de otro formato de mensaje.

HOST: Dispositivo el cual participa directo con la comunicación de red.

RESUMEN

En este documento se propone dos escenarios simulados de conectividad mediante el software Cisco Packet tracer®. bajo los protocolos IPv4 y IPv6. La interconexión de 2 conmutadores (switches) y 3 enrutadores (routers) como columna vertebral (backbone) es el eje central de los escenarios. La conectividad se realiza mediante varias técnicas de interconexión como el encapsulamiento IEEE 802.1Q, y el protocolo de enlace troncal entre VLAN´s (VTP) , también se utiliza el protocolo DHCP para dar conectividad a los Hosts conectados a la red. También se realiza la simulación del protocolo de enrutamiento dinámico OSPF (Open Short Path first) para la interconexión de los 3 routers y la traducción de redes de internet privadas/públicas en IPV4 (NAT) y configuración de listas de accesos (ACL). Se sincronizan los routers en fecha y hora mediante el protocolo NTP, configurando de manera segura los enrutadores mediante claves encriptadas por medio de la conexión local y remota. Como resultado se muestra la simulación del envío y la respuesta de paquetes entre los hosts mediante la utilidad PING.

Palabras clave: IPv6, IEEE802.1Q, Listas de control de acceso, NAT, NTP, OSPF, VTP

ABSTRACT

This paper it proposes two simulated connectivity scenarios using Cisco Packet tracer® software under the IPv4 and IPv6 protocols. The interconnection of 2 switches (switches) and 3 routers (routers) as a backbone is the central axis of the scenarios. The connectivity is developed through various interconnection techniques such as IEEE 802.1Q encapsulation, and the trunk link protocol between VLANs (VTP), the DHCP protocol is also used to provide connectivity to the Hosts connected to the network. The simulation of the dynamic routing protocol OSPF (Open Short Path first) for the interconnection of the 3 routers and the translation of private / public internet networks in IPV4 (NAT) and configuration of access lists (ACL) is also performed. The routers are synchronized in date and time through the NTP protocol, configuring the routers securely using encrypted keys through the local and remote connection. As a result, the simulation of the sending and response of packets between the hosts is shown using the PING utility.

Keywords—: Access Control Lists, IPv6, IEEE802.1Q, NAT, NTP, OSPF, VTP.

1. INTRODUCCIÓN

Las redes de comunicación están en constante cambio, ya que las necesidades humanas en la actualidad están migrando a ser más digitales, cada dia el consumo de informacion (Voz, data, y video) por parte de los usuarios va en aumento y los nuevos servicios de entretenimiento en streaming y redes sociales han cambiado significativamente todos los aspectos de nuestra sociedad y nuestra cultura popular. El paradigma de intercambio de informacion entre las personas está cambiando a gran velocidad y está migrando de la modalidad presencial a la virtual gracias a las nuevas tecnologías de redes, software y hardware como smartphones, pc´s, tablets, smart tv entre otros, actualmente estamos asimilando y tratando de adaptarnos a todo este cambio cultural y tecnológico, mientras otra tecnología irruptora amenaza con llegar a nuestras vidas, la IoT (Internet of Things) donde además de personas, dispositivos electrónicos inteligentes junto con la IA(inteligencia artificial), también están participando en el intercambio de informacion con la humanidad utilizando como principal medio las redes de comunicación. Estos equipos están situados en diferentes lugares geográficos y diseñados para recolectar e intercambiar volúmenes de informacion y esta es almacenada, procesada, organizada y estudiada matemática, estadística y probabilísticamente, en grandes centro de datos (DataCenters) situados por todo el planeta, con el objetivo de poder predecir, investigar y observar comportamientos deterministas y estocásticos en todos las áreas del conocimiento y la cultura humana como por ejemplo redes sociales, cambio climático, tráfico aéreo, marítimo y terrestre, telemedicina, flujo de informacion, astronomía como por nombrar algunos.

Actualmente los usuarios colocan más y más informacion en las redes, servidores y centros de datos, exponiendo la privacidad empresarial e individual a ser accedida por parte de personas, entidades o naciones no deseadas. Por tal razón, las redes de comunicación, dispositivos y participantes deben bloquear accesos no deseados y el diplomado de profundización cisco enseña la introducción a este mundo. La prueba de habilidades del diplomado propone simular dos escenarios mediante el software cisco packet tracer®, el primero debe interconectar a 2 conmutadores (switches), 1 enrutador (router) como columna vertebral (Backbone) de la red LAN y simular la comunicación entre Hosts (2 PC´s), 1 salida con IP publica de internet con direcciones IPv4 e IPv6.

En el segundo escenario se interconecta 2 conmutadores, 3 enrutadores como columna vertebral (Back-bone) de la red y se realiza la conexión simulada a un servidor externo de Internet, bajo VLANs internas y protocolo IEEE802.1Q, También se simula la comunicación entre Hosts (2 PC´s), y el suministro de direcciones ip automáticas mediante el protocolo DHCP y también se realiza la simulación de comunicación de un servidor interno web con direcciones IPv4 e IPv6.

2 OBJETIVOS

Objetivo general

Demostrar los conocimientos adquiridos en el diplomado CISCO, mediante las soluciones simuladas de conectividad en redes, en escenarios propuestos por el diplomado de profundización.

Objetivos específicos

- Simular el funcionamiento y la configuración de la red, con la ayuda del software CISCO Packet Tracer®.
- Brindar interconexión y servicio a salida a redes externas a los participantes de los escenarios propuestos utilizando cableados y equipos de la forma más eficiente posible.
- Configurar las redes para que el mantenimiento y puesta en marcha de estas, se utilice en el menor tiempo posible y con los recursos adecuados.
- Configurar las redes de los escenarios propuestos de la forma más segura posible.
- Proteger la red contra intrusos y accesos no autorizados desde el interior y exterior de la red.

3 DESARROLLO DEL PROYECTO

ESCENARIO 1

En este escenario como se puede ver en Figura 1 se debe realizar la configuración de cada uno de los dispositivos el cual debe contar con conexión de direccionamiento ipv4, ipv6, EtherChannel, protocolo DHCP, entre otros como nombre de dominio y acceso controlado con usuario y contraseña.

Para este caso se va a simular el escenario con switches de capa 3, los cuales ya tienen por defecto dual-stack o coexistencia en ipv4 e ipv6.

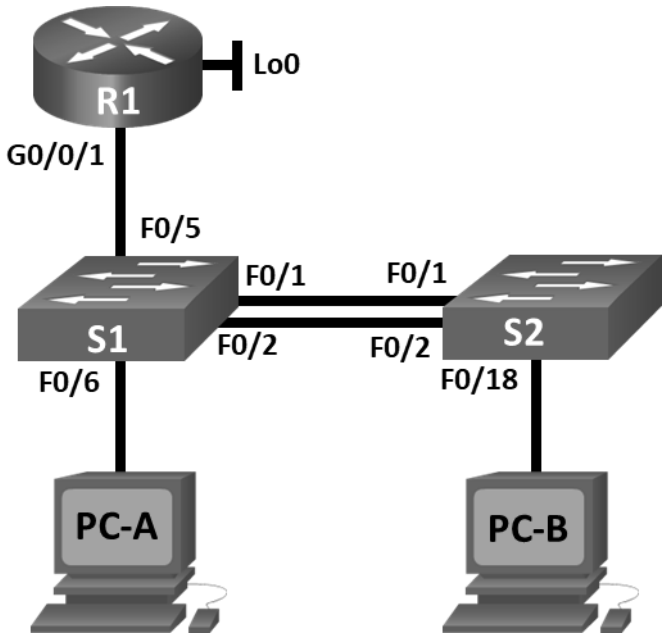


Figura 1 Topología Escenario 1.

En la Tabla 1 está la descripción y el número de las VLAN que vamos a configurar en este escenario y en Tabla 2, vamos a encontrar la tabla de asignación de direcciones para los dispositivos de la red.

También observamos la configuración del escenario desarrollado en el software cisco packet tracer®. (ver Figura 2)

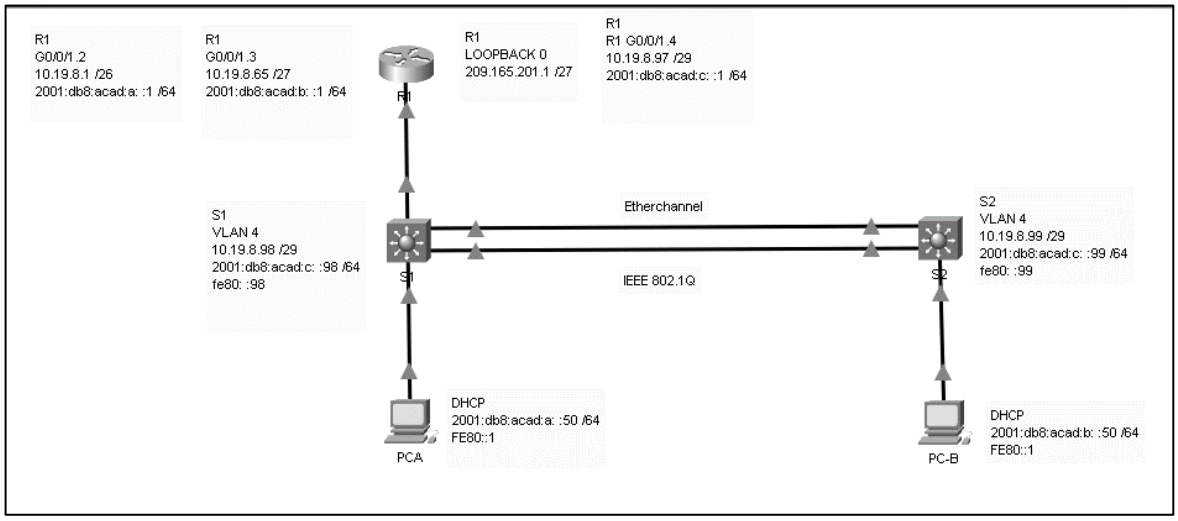


Figura 2 Topología del escenario en Packet Tracer®.

Tabla 1. Nombre de las VLAN escenario 1.

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

Tabla 2. 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
	2001:db8:acad:a: :1 /64	No corresponde
R1 G0/0/1.3	10.19.8.65 /27	No corresponde
	2001:db8:acad:b: :1 /64	No corresponde
R1 G0/0/1.4	10.19.8.97 /29	No corresponde

	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
	2001:db8:acad:209: :1 /64	No corresponde
S1 VLAN 4	10.19.8.98 /29	10.19.8.97
	2001:db8:acad:c: :98 /64	No corresponde
	fe80: :98	No corresponde
S2 VLAN 4	10.19.8.99 /29	10.19.8.97
	2001:db8:acad:c: :99 /64	No corresponde
	fe80: :99	No corresponde
PC-A NIC	Dirección DHCP para IPv4	DHCP para puerta de enlace predeterminada Ipv4
	2001:db8:acad:a: :50 /64	fe80::1
PC-B NIC	DHCP para dirección Ipv4	DHCP para puerta de enlace predeterminada Ipv4
	2001:db8:acad:b: :50 /64	fe80::1

3.1.1 Inicializar y volver a cargar el router y el switch

A continuación, se inicializa y se vuelve a cargar el router y switches donde se utilizan los siguientes comandos, para después iniciar con la asignación de nombre para identificar los dispositivos. En este paso se reinicia los equipos y se borran toda la configuración que esta guardada en la memoria interna de los equipos. (Alvarez, 2009).

Router R1	SWITCH 1	SWITCH 2
R1#erase startup-config R1 #delete flash:vlan.dat	Switch>enable Switch#configure terminal Switch(config)#hostname S1 S1 #erase startup-config S1 #delete flash:vlan.dat S1#reload	Switch>enable Switch#configure terminal Switch(config)#hostname S2 S2#erase startup-config S2#delete flash:vlan.dat S2#reload

3.1.2 Configurar R1

Las tareas de configuración para el router R1 incluyen los siguientes pasos:

En la siguiente tabla (ver Tabla 3), se muestra los diferentes comandos que se utilizaron para realizar las configuraciones que se requieren para cada una de las tareas solicitadas, implementando los protocolos que debe realizar el router.

Tabla 3. Configuración básica del R1 escenario 1

Tarea	Especificación
Desactivar la búsqueda DNS Con este comando se desactiva la búsqueda de cualquier dominio escrito en el prompt. (tecnologia y redes , 2014)	R1 (config)#no ip domain-lookup
Nombre del router Con este comando se da un nombre único en la red al Router (tecnologia y redes , 2014)	Router>enable Router#configure terminal Router(config)#hostname R1
Nombre de dominio (ccna-lab.com) Se define un nombre de dominio predeterminado a R1 (tecnologia y redes , 2014)	R1(config)#ip domain name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado (ciscoenpass) Se configura una contraseña para entrar al modo exec (tecnologia y redes , 2014)	R1(config)#enable secret ciscoenpass
Contraseña de acceso a la consola (ciscoconpass) Se configura una contraseña para la comunicación por consola (tecnologia y redes , 2014)	R1(config)#line console 0 R1(config-line)#password ciscoconpass R1(config-line)#login
Establecer la longitud mínima para las contraseñas (10 caracteres) Se establece que la contraseña debe tener mínimo 10 caracteres. (tecnologia y redes , 2014)	R1(config)#security password min-length 10
Crear un usuario administrativo en la base de datos local	R1(config)#username admin password admin1pass R1(config)#line console 0

Nombre de usuario: admin Password: admin1pass Se crea una clave para que sea de usuario administrativo y pueda comunicarse por medio de la consola. (tecnologia y redes , 2014)	R1(config-line)#login local
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local Se configura clave por medio de la comunicación Telnet. (tecnologia y redes , 2014)	R1(config)#line vty 0 4 R1(config-line)#login local R1(config-line)#exit
Configurar VTY solo aceptando SSH Se Configura que la comunicación Telnet sea segura por medio SSH (tecnologia y redes , 2014)	R1(config)#line vty 0 4 R1(config-line)#transport input ssh R1(config-line)#exit
Cifrar las contraseñas de texto no cifrado Se encripta la contraseña para que no sea husmeada por medio de un Sniffer de paquetes. (tecnologia y redes , 2014)	R1(config)#service password-encryption
Configure un MOTD Banner Se edita un aviso de advertencia a personal no autorizado en la consola. (tecnologia y redes , 2014)	R1(config)#banner motd “Prohibido el acceso a personas no autorizadas, por favor contactarse con el administrador de red”
Habilitar el routing Ipv6 Se habilita el dual-stack (tecnologia y redes , 2014)	R1(config)#int G0/0/1 R1(config-if)#ipv6 unicast-routing R1(config-if)#ipv6 enable
Configurar interfaz G0/0/1 y subinterfaces (Establezca la descripción Establece la dirección Ipv4. Establezca la dirección local de enlace Ipv6 como fe80: :1 Se establece la dirección Ipv6, Activar la interfaz. (Cisco networking Academy)	R1(config)#interface G0/0/1.2 R1(config-subif)#encapsulation dot1Q 2 R1(config-subif)#ip address 10.19.8.1 255.255.255.192 R1(config-subif)# ipv6 address 2001:db8:acad:a::1 /64 R1(config-subif)#no shut R1(config)#interface G0/0/1.3 R1(config-subif)#encapsulation dot1Q 3

Se activa la interface G0/0/1 y sus interfaces. También se habilita IEEE802.1Q para cada subinterfaz, para que tenga comunicación con las VLAN y sean sus default Gateway en ipv6 y ipv4 (Cisco networking academy)	R1(config-subif)#ip address 10.19.8.65 255.255.255.224 R1(config-subif)#ipv6 address 2001:db8:acad:b::1/64 R1(config-subif)#no shut R1(config)#interface G0/0/1.4 R1(config-subif)#encapsulation dot1Q 4 R1(config-subif)#ip address 10.19.8.97 255.255.255.248 R1(config-subif)#ipv6 address 2001:db8:acad:c::1/64 R1(config-subif)#ipv6 address fe80::1 link-local R1(config-subif)#no shut
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) Se habilita la interface Loopback en IPv6 y IPv4 (Cisco networking Academy)	R1(config)#interface loopback0 R1(config-if)#ip address 209.165.201.1 255.255.255.224 R1(config-if)#ipv6 address 2001:db8:acad:209::1/64 R1(config-if)#ipv6 address fe80::1 link-local R1(config-if)#no shut
Generar una clave de cifrado RSA Se fortalece la encriptación de la clave mediante un módulo de 10 bits, para la comunicación por medio de Telnet. (Cisco networking Academy)	R1(config)#crypto key generate rsa general-keys modulus 1024 R1(config)#line vty 0 4 R1(config-line)#login local R1(config-line)#transport input ssh

3.1.3 Configure S1 y S2.

Como se muestra en las siguientes tablas (Ver Tabla 4, Tabla 5), se realiza la configuración de los Switches 1 y 2 en donde se debe desactivar la búsqueda DNS, nombrarlo y darle un nombre de dominio para después utilizarlos diferentes comandos presentados en el cuadro como el control de acceso implementando un usuario y contraseña.

Tabla 4. Configuración básica S1 escenario 1

Tarea	Especificación
Desactivar la búsqueda DNS Con este comando se desactiva la búsqueda de cualquier dominio escrito en el prompt. (tecnologia y redes , 2014)	SWITCH (config)#no ip domain-lookup
Nombre del switch Con este comando se da un nombre único en la red al Router (tecnologia y redes , 2014)	SWITCH(config)#hostname S1
Nombre de dominio Se configura el nombre del dominio. (tecnologia y redes , 2014)	S1(config)#ip domain name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado **ciscoenpass** Se configura una contraseña para entrar al modo exec (tecnologia y redes , 2014)	S1(config)#enable secret **ciscoenpass**
Contraseña de acceso a la consola Se configura una contraseña para la comunicación por consola (tecnologia y redes , 2014)	S1(config)#line console 0 S1(config-line)#password **ciscoconpass** S1(config-line)#login
Crear un usuario administrativo en la base de datos local Se crea una clave para que sea de usuario administrativo y pueda comunicarse por medio de la consola. (tecnologia y redes , 2014)	S1(config)#username admin password admin1pass S1(config)#line console 0 S1(config-line)#login local S1(config-line)#exit
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local. Se configura clave por medio de la comunicación Telnet. (tecnologia y redes , 2014)	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 Se configura que la comunicación Telnet sea segura por medio SSH (tecnologia y redes , 2014)	S1(config)#line vty 0 4 S1(config-line)#transport input ssh S1(config-line)#exit

Cifrar las contraseñas de texto no cifrado (tecnologia y redes , 2014) Se encripta la contraseña para que no sea husmeada por medio de un Sniffer de paquetes. (tecnologia y redes , 2014)	S1(config)#service password-encryption S1(config)#exit
Configurar un MOTD Banner Se edita un aviso de advertencia a personal no autorizado en la consola. (cisco networking academy)	S1(config)#banner motd “Prohibido el acceso a personas no autorizadas, Por favor contactarse con el admin de red “
Generar una clave de cifrado RSA Se fortalece la encriptación de la clave mediante un módulo de 10 bits, para la comunicación por medio de Telnet. (tecnologia y redes , 2014)	S1(config)#crypto key generate rsa general-keys modulus 1024 S1(config)#username admin secret admin1pass S1(config)#line vty 0 4 S1(config-line)#login local S1(config-line)#transport input ssh
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) Se crea la VLAN 4 como interfaz administrativa y se crea los enlaces locales en ipv6 para S1 y S2 (Cisco networking academy)	S1(config)#interface vlan4 S1(config-if)#ip address 10.19.8.98 255.255.255.248 S1(config)#sdm prefer dual-ipv4-and-ipv6 default S1#reload S1(config)#interface vlan4 S1 (config-if)#ipv6 enable S1 (config-if)#ipv6 address 2001:db8:acad:c::98/64 S1 (config-if)#no shut S1(config)#interface vlan4 S1 (config-if)#ipv6 address FE80::98 link-local S1 (config-if)#no shut
Configuración del gateway predeterminado Se crea gateway predeterminado (tecnologia y redes , 2014)	S1(config)# ip default-gateway 10.19.8.97

Tabla 5. Configuración básica S2 escenario 1

Tarea	Especificación
Desactivar la búsqueda DNS. Se desactiva la búsqueda de dominios. (tecnologia y redes , 2014)	SWITCH (config)#no ip domain-lookup
Nombre del switch Se nombra el switch como S1 (tecnologia y redes , 2014)	SWITCH(config)#hostname S2
Nombre de dominio Se da un nombre de dominio al switch. (tecnologia y redes , 2014)	S2(config)#ip domain name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado **ciscoenpass** Se crea una contraseña para entrar al modo privilegiado (tecnologia y redes , 2014)	S2(config)#enable secret ciscoenpass
Contraseña de acceso a la consola Se crea contraseña para acceder a la consola. (tecnologia y redes , 2014)	S2(config)#line console 0 S2(config-line)#password ciscoconpass S2(config-line)#login
Crear un usuario administrativo en la base de datos local Se crea un usuario administrativo con password. (tecnologia y redes , 2014)	S2(config)#username admin password admin1pass S2(config)#line console 0 S2(config-line)#login local
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local Se crea restricción para entrar por medio de Telnet (tecnologia y redes , 2014)	S2(config)#line vty 0 4 S2(config-line)#login local S2(config-line)#exit
Configurar las líneas VTY para que acepten únicamente las conexiones SSH Se incrementa la seguridad en telnet mediante el protocolo SSH (tecnologia y redes , 2014)	S2(config)#line vty 0 4 S2(config-line)#transport input ssh S2(config-line)#exit
Cifrar las contraseñas de texto no cifrado Se encripta las contraseñas (tecnologia y redes , 2014)	S2(config)#service password-encryption

Configurar un MOTD Banner Se edita un mensaje de usuario para personas no autorizadas. (tecnologia y redes , 2014)	S2(config)#banner motd “Prohibido el acceso a personas no autorizadas, Por favor contactarse con el admin de red “
Generar una clave de cifrado RSA Se aumenta la seguridad aumentando a 10 bit el algoritmo de encriptación. (cisco networking academy)	S2(config)#crypto key generate rsa general-keys modulus 1024 S2(config)#username admin secret admin1pass S2(config)#line vty 0 4 S2(config-line)#login local S2(config-line)#transport input ssh
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) Se crea la Vlan 4 como interfaz de administración y se crea los enlaces locales en ipv6 (Cisco networking academy)	S2(config)#interface vlan4 S2(config-if)#ip address 10.19.8.99 255.255.255.248 S2(config-if)#no shut S2(config)#sdm prefer dual-ipv4-and-ipv6 default S2#reload S2(config)#interface vlan4 S2 (config-if)#ipv6 enable S2 (config-if)#ipv6 address 2001:db8:acad:c::99/64 S2(config-if)#no shut S2(config)#interface vlan4 S2 (config-if)#ipv6 address FE80::99 link-local S2 (config-if)#no shut
Configuración del Gateway predeterminado Se configura la Puerta de enlace predeterminada para S2. (tecnologia y redes , 2014)	S2(config)# ip default-gateway 10.19.8.97

3.1.4 Configuración de la infraestructura de red (vlan, trunking, etherchannel)

Utilizando a la bibliografía del curso, se llegó satisfactoriamente en la conectividad de la red.

Al final el procedimiento que se realiza para la configuración de Etherchannel fue el siguiente

a) Crear un Port-channel incluyendo las 2 interfaces f0/1 y f0/2 en cada conmutador.

b) incluir la interfaz en modo encapsulamiento IEEE802.Q1

c) convertir la interfaz port-channel en modo trunk

d) incluir la interfaz por-channel a la vlan 6

e) luego conectar las 4 interfaces.

3.1.4.1 Configurar S1

En este ejercicio solicita que se debe realizar el nombramiento de las VLAN (ver Tabla 1), y la creación de la red troncal para la utilización de la VLAN6, la cual se le debe configurar las interfaces. También la creación de grupos de Etherchannel para capa 2 con las interfaces de un protocolo de negociación en este caso solicita que sea LACP.

También se debe realizar la configuración de puertos de host y los puertos de acceso, utilizando los comandos que se muestran a continuación. Todo está configuración se debe realizar en S1 Y S2. (ver Tabla 6 y Tabla 7)

Tabla 6. Configuración de VLANs en S1, Etherchannel y IEEE802.1Q en escenario 1.

Tarea	Especificación
Crear VLAN (VLAN 2, nombre Bikes VLAN 3, nombre Trikes VLAN 4, nombre Management VLAN 5, nombre Parking VLAN 6, nombre Native Se crean las VLANs en S1	S1(config)#vlan 2 S1(config-vlan)#name bikes S1(config-vlan)#exit S1(config)#vlan 3 S1(config-vlan)#name trikes S1(config-vlan)#exit S1(config)#vlan 4 S1(config-vlan)#name management S1(config-vlan)#exit S1(config)#vlan 5 S1(config-vlan)#name parking

(Cisco networking academy)	S1(config-vlan)#exit S1(config)#vlan 6 S1(config-vlan)#name native S1(config-vlan)#exit
Crear troncales 802.1Q que utilicen la VLAN 6 nativa (Interfaces F0/1, F0/2 y F0/5) Se configuran las interfaces en modo troncal mediante IEEE802.1Q y se asocia a la VLAN 6 como medio transporte. (Cisco networking academy)	S1(config)#interface FastEthernet0/1 S1(config-if)#switchport access vlan 6 S1(config-if)# switchport trunk encapsulation dot1q S1(config-if)# switchport mode trunk S1(config-if)#switchport trunk native vlan 6 S1(config)#interface FastEthernet0/2 S1(config-if)# switchport trunk encapsulation dot1q S1(config-if)# switchport mode trunk S1(config-if)#switchport trunk native vlan 6 S1(config)#interface f0/5 S1(config-if)#switchport trunk encapsulation dot1q S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 6
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2 (Usar el protocolo LACP para la negociación) Se configura las interfaces para que utilicen etherchannel en modo encapsulado IEEE802.1Q. (Cisco networking academy)	S1# configure terminal S1(config)# interface range fastEthernet 0/1 – 2 S1(config-if-range)# channel-group 1 mode active S1(config)#interface Port-channel 1 S1(config-if)# switchport trunk encapsulation dot1q S1(config-if)# switchport mode trunk S1(config-if)#switchport trunk native vlan 6
Configurar el puerto de acceso de host para VLAN 2 (Interface F0/6)	S1(config)#interface f0/6

Se configura la interface f0/6 como medio de acceso a la VLAN 2 (Cisco networking academy)	S1(config-if)#switchport access vlan 2 S1(config-if)#switchport mode access
Configurar la seguridad del puerto en los puertos de acceso, Permitir 3 direcciones MAC Se configura la interface f0/6 como interfaz segura y permita la conexión de equipos con MAC permitidas. (tecnologia y redes , 2014)	S1(config)#interface f0/6 S1(config-if)#switchport mode access S1(config-if)#switchport port-security S1(config-if)#switchport port-security maximum 3

3.1.4.2 Configure el S2.

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

Tabla 7. Configuración de VLANs en S2, Etherchannel y IEEE802.1Q en escenario 1

Tarea	Especificación
Crear VLAN (VLAN 2, name Bikes VLAN 3, name Trikes VLAN 4, name Management VLAN 5, nombre Parking VLAN 6, nombre Native) Se configuran las Vlans en S2 (Cisco networking academy)	S2(config)#vlan 2 S2(config-vlan)#name bikes S2(config-vlan)#exit S2(config)#vlan 3 S2(config-vlan)#name trikes S2(config-vlan)#exit S2(config)#vlan 4 S2(config-vlan)#name management S2(config-vlan)#exit S2(config)#vlan 5 S2(config-vlan)#name parking S2(config-vlan)#exit S2(config)#vlan 6 S2(config-vlan)#name native
Crear troncales 802.1Q que utilicen la VLAN 6 nativa (Interfaces F0/1 y F0/2) Se configuran las interfaces en modo troncal y que accedan a la VLAN 6 (Cisco networking academy)	S2(config)#interface FastEthernet0/1 S2(config-if)#switchport access vlan 6 S2(config-if)# switchport trunk encapsulation dot1q S2(config-if)# switchport mode trunk

	S2(config-if)#switchport trunk native vlan 6 S2(config)#interface FastEthernet0/2 S2(config-if)#switchport access vlan 6 S2(config-if)# switchport trunk encapsulation dot1q S2(config-if)# switchport mode trunk S2(config-if)#switchport trunk native vlan 6
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2 Se configura Etherchannel para f0/1 y f0/2 (Cisco networking academy)	S2# configure terminal S2(config)# interface range fastethernet 0/1 – 2 S2(config-if-range)# channel-group 1 mode active S2(config)#interface Port-channel 1 S2(config-if)# switchport trunk encapsulation dot1q S2(config-if)# switchport mode trunk S2(config-if)#switchport trunk native vlan 6
Configurar el puerto de acceso del host para la VLAN 3 Interfaz F0/18 Se configura f0/18 como interfaz de acceso a Vlan 3 (Cisco networking academy)	S2(config-if)#switchport access vlan 3 S2(config-if)#switchport mode access S2(config-if)#no shut
Configure port-security en los access ports permite 3 MAC addresses Se configura f0/18 como puerto seguro de conexión. (Cisco networking academy)	S2(config)#int f0/18 S2(config-if)#switchport port-security S2(config-if)#switchport port-security maximum 3 S2(config-if)#no shut
Asegure todas las interfaces no utilizadas.	S2(config)#int range f0/3-17,f0/19-24,g0/1-2 S2(config-if-range)#switchport mode access

Asignar a VLAN 5, Establecer en modo de acceso, agregar una descripción y apagar Se configura las demás interfaces en shutdown (cisco networking academy)	S2(config-if-range)#switchport access vlan 5 S2(config-if-range)#description "interface no utilizables" S2(config-if-range)#shutdown

3.1.5 Configurar soporte de host

3.1.5.1 Configure R1

Las tareas de configuración para R1 incluyen las siguientes (ver Tabla 8)

Tabla 8. Configuración DHCP y rutas predeterminadas en R1 escenario 1.

Tarea	Especificación
Configure Default Routing Crear rutas predeterminadas para Ipv4 e Ipv6 que dirijan el tráfico a la interfaz Loopback 0 Se configura Lo0 como medio de salida por defecto en ipv4/ipv6 (cisco networking academy)	R1(config)# ip route 0.0.0.0 0.0.0.0 loopback 0 %Default route without gateway, if not a point-to-point interface, may impact performance R1(config)#exit R1# %SYS-5-CONFIG_I: Configured from console by console R1#show ip route static S* 0.0.0.0/0 is directly connected, Loopback0 R1(config)#ipv6 route ::/0 loop R1(config)#ipv6 route ::/0 loopback 0 R1(config)#exit
Configurar Ipv4 DHCP para VLAN 2 Cree un grupo DHCP para VLAN 2, compuesto por las últimas 10 direcciones de la subred	R1(config)#ip dhcp pool vlan2

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 Se configura el servidor DHCP para la VLAN2 (Cisco networking academy)	R1(dhcp-config)#network 10.19.8.0 255.255.255.192 R1(dhcp-config)#default-router 10.19.8.1 R1(dhcp-config)#domain-name ccna-a.net R1(dhcp-config)#ip dhcp excluded-address 10.19.8.2 10.19.8.51 R1(config)#
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 Se configura servidor DHCP para VLAN 3 (Cisco networking academy)	R1(config)#ip dhcp pool vlan3 R1(dhcp-config)#network 10.19.8.64 255.255.255.224 R1(dhcp-config)#default-router 10.19.8.65 R1(dhcp-config)#domain-name ccna-a.net R1(dhcp-config)#ip dhcp excluded-address 10.19.8.66 10.19.8.83

3.1.5.2 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, (ver Tabla 9). (Cisco networking Academy)

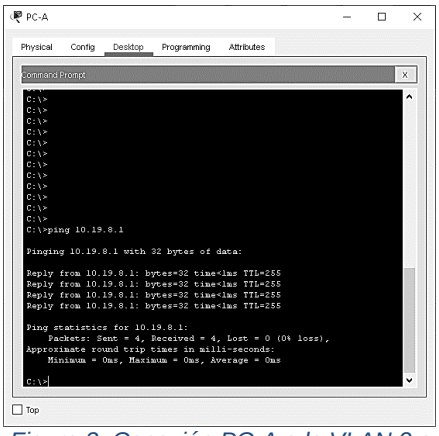
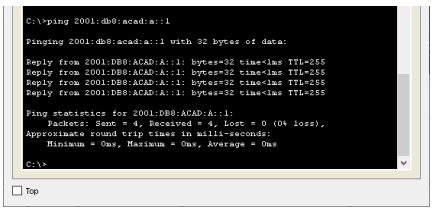
Tabla 9. Direccionamiento de los PCs en escenario 1.

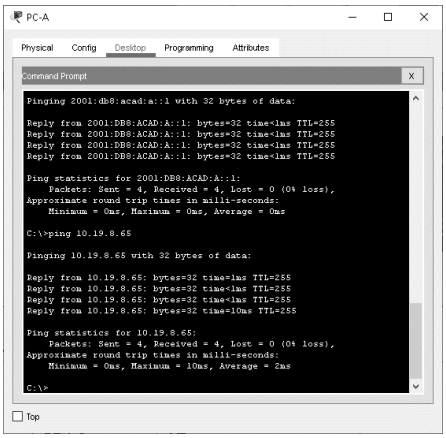
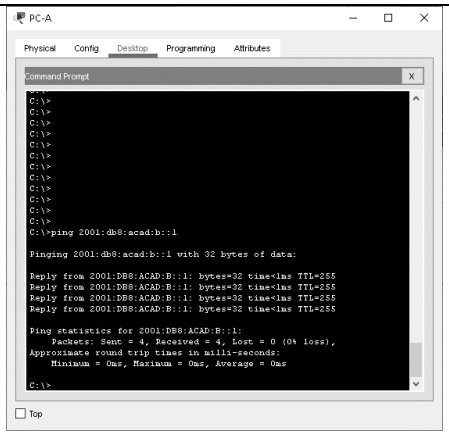
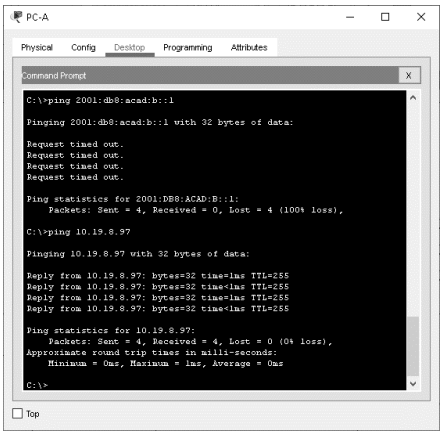
PC-A Network Configuration	
Descripción	Se realiza la configuración haciendo click en generación automática en DHCP
Dirección física	*0001.C9EC.225D*
Dirección IP	*10.19.8.52*
Máscara de subred	*255.255.255.192*
Gateway predeterminado	*10.19.8.1*
Gateway predeterminado Ipv6	*FE80::1*
Configuración de red de PC-B	
Descripción	Se realiza la configuración haciendo click en generación automática en DHCP
Dirección física	*0040.0B1B.8DE0*
Dirección IP	*10.19.8.84*
Máscara de subred	*255.255.255.224*
Gateway predeterminado	*10.19.8.65*
Gateway predeterminado Ipv6	*FE80::1*

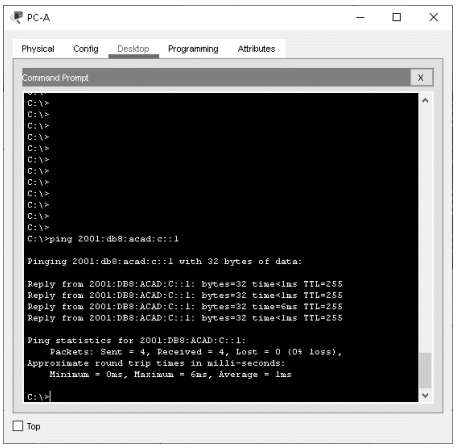
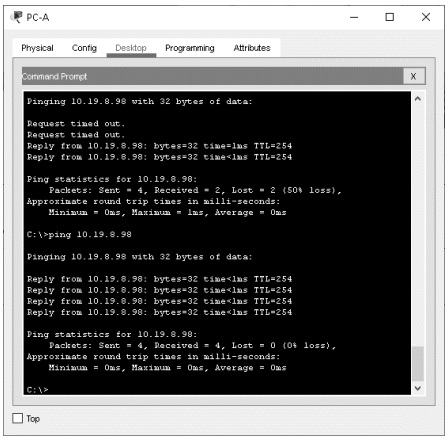
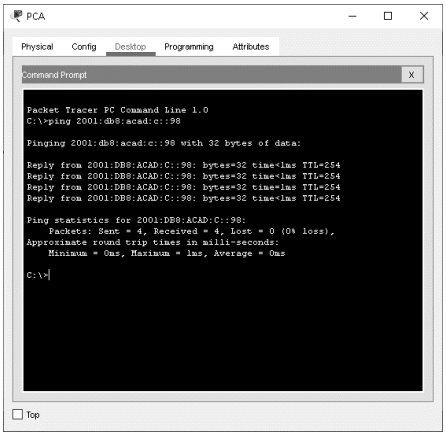
3.1.6 Probar y verificar la conectividad de extremo a extremo

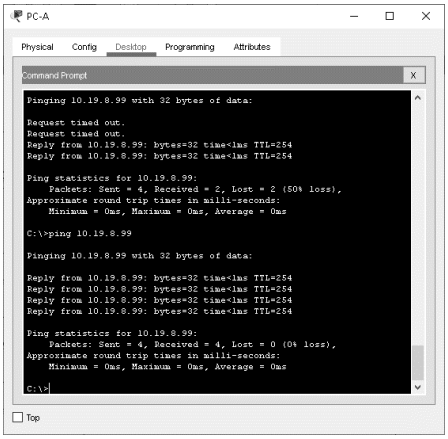
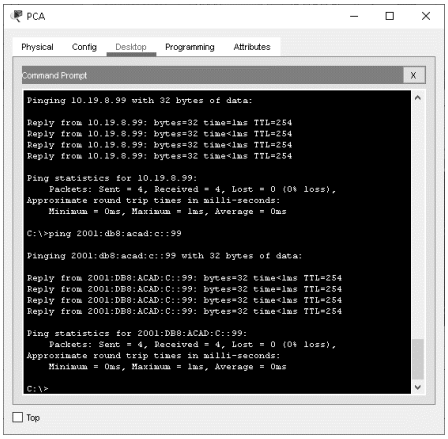
Use el comando ping para probar la conectividad Ipv4 e Ipv6 entre todos los dispositivos de red.

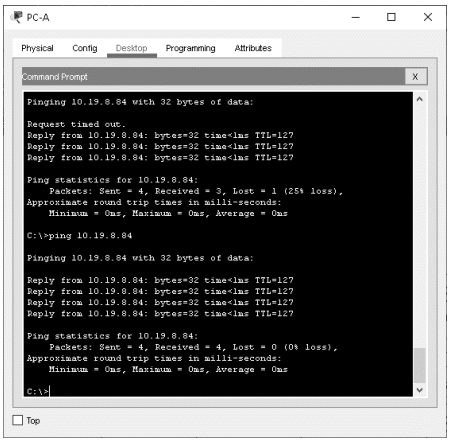
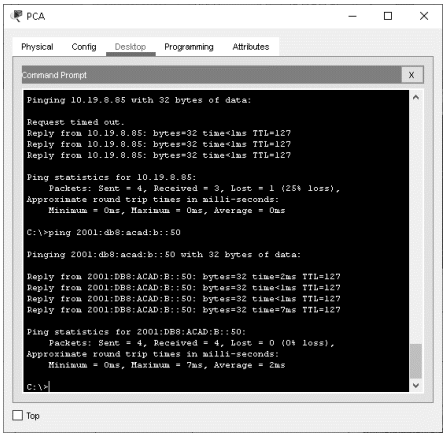
Tabla 10. Pruebas finales escenario 1

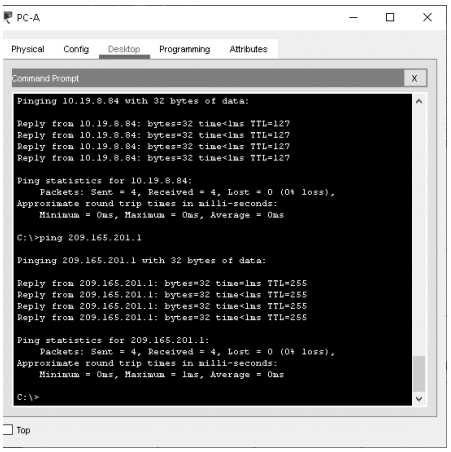
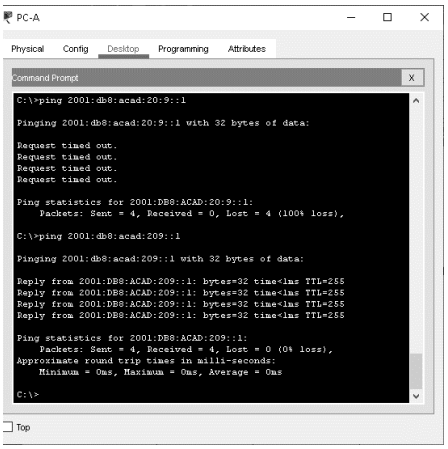
Desde	A	de Internet	Dirección IP	Resultados de ping
PC-A	R1, G0/0/1.2	Dirección	10.19.8.1	 *Figura 3. Conexión PC-A a la VLAN 2 en R1 con IPv4 .*
		Ipv6	2001:db8:acad:a: :1	 *Figura 4. Conexión PC-A a la VLAN 2 en R1 con IPv6 .*

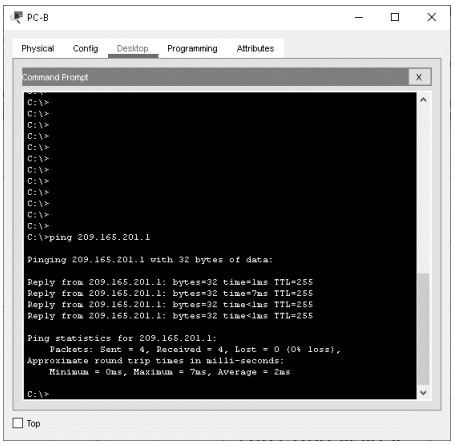
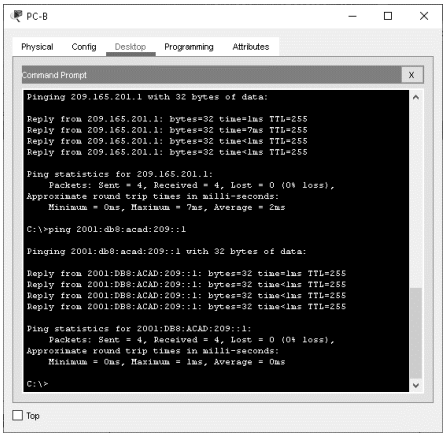
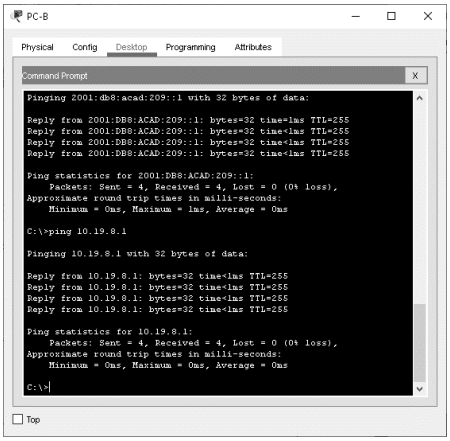
	R1, G0/0/1.3	Dirección	10.19.8.65	 *Figura 5. Conexión PC-A a la VLAN 3 en R1 con IPv4 .*
		Ipv6	2001:db8:acad:b: :1	 *Figura 6. Conexión PC-A a la VLAN 2 en R1 con IPv6 .*
	R1, G0/0/1.4	Dirección	10.19.8.97	 *Figura 7. Conexión PC-A a la VLAN 4 en R1 con IPv4 .*

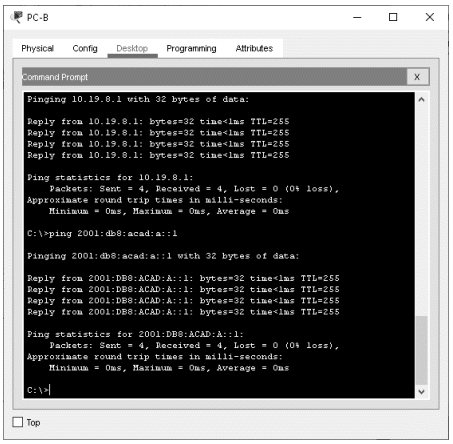
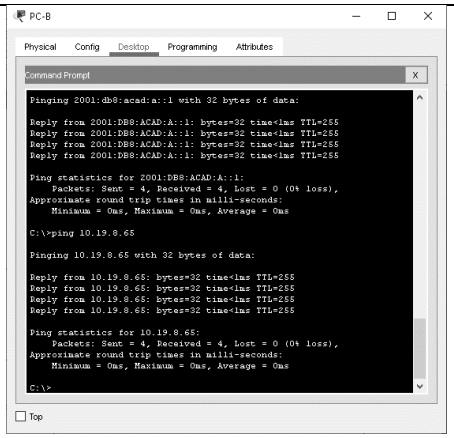
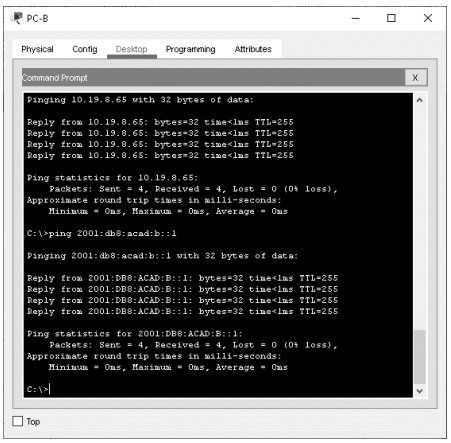
		Ipv6	2001:db8:acad:c: :1	 *Figura 8. Conexión PC-A a la VLAN 4 en R1 con IPv6 .*
	S1, VLAN 4	Dirección	10.19.8.98	 *Figura 9. Conexión PC-A a la VLAN 4 en S1 con IPv4 .*
		Ipv6	2001:db8:acad:c: :98	 *Figura 10. Conexión PC-A a la VLAN 4 en S1 con IPv6 .*

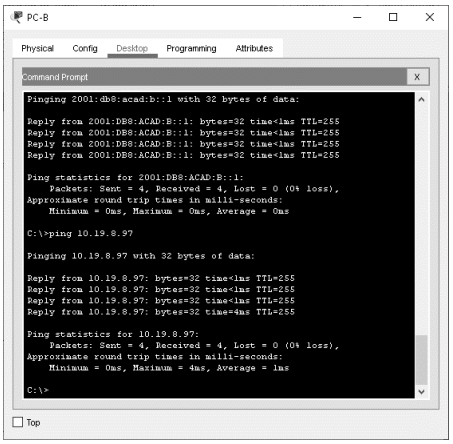
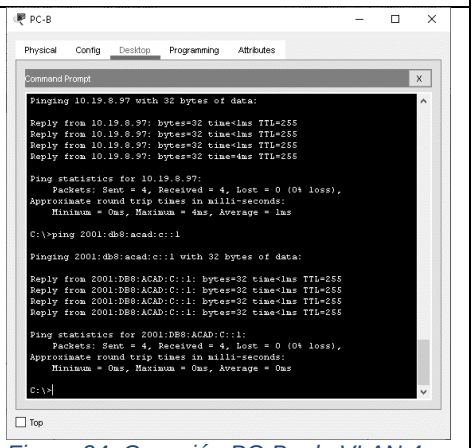
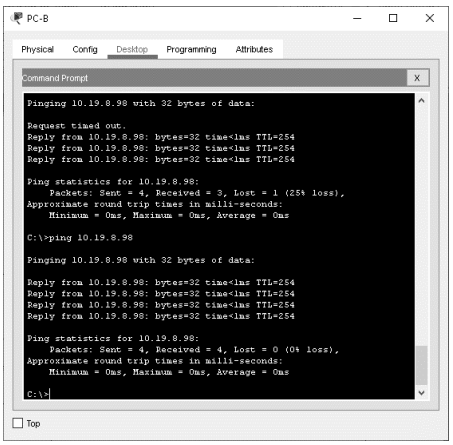
	S2, VLAN 4	Dirección	10.19.8.99.	 *Figura 11. Conexión PC-A a la VLAN 4 en S2 con IPv4 .*
		Ipv6	2001:db8:acad: c: :99	 *Figura 12. Conexión PC-A a la VLAN 4 en S2 con IPv6 .*

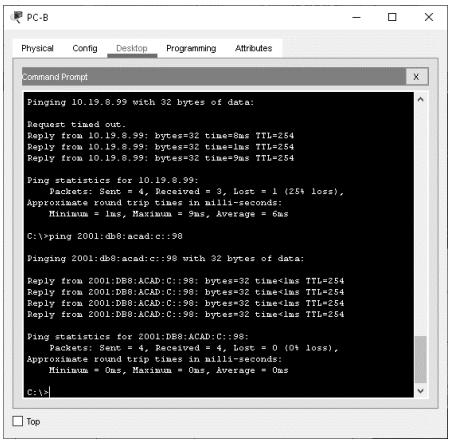
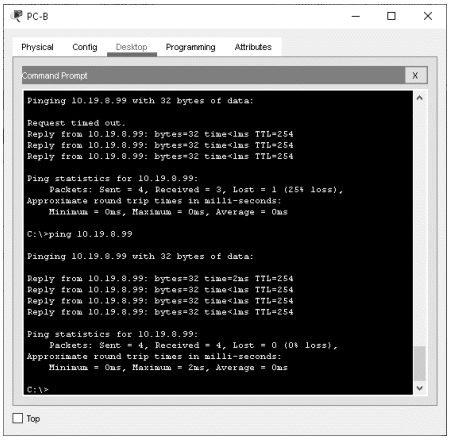
	PC-B	Dirección	IP address will vary.	 *Figura 13. Conexión PC-A a la PC-B con IPv4 .*
		Ipv6	2001:db8:acad: b: :50	 *Figura 14. Conexión PC-A a la PC-B con IPv6.*

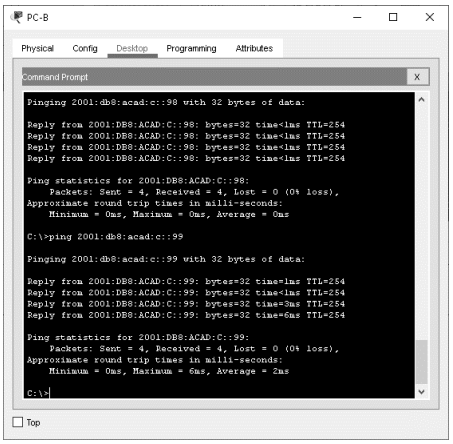
	R1 Bucle 0	Dirección	209.165.201.1	 *Figura 15. Conexión PC-A al Loopback 0 en R1 con IPv4.*
		Ipv6	2001:db8:acad: 209: :1	 *Figura 16. Conexión PC-A al Loopback 0 en R1 con IPv6.*

PC-B	R1 Bucle 0	Dirección	209.165.201.1	 *Figura 17. Conexión PC-B al Loopback 0 en R1 con IPv4.*
		Ipv6	2001:db8:acad: 209: :1	 *Figura 18. Conexión PC-B al Loopback 0 en R1 con IPv6.*
	R1, G0/0/1. 2	Dirección	10.19.8.1	 *Figura 19. Conexión PC-B a la VLAN 2 en R1 con IPv4 .*

		Ipv6	2001:db8:acad:a: :1	 *Figura 20. Conexión PC-B a la VLAN 2 en R1 con IPv6 .*
	R1, G0/0/1.3	Dirección	10.19.8.65	 *Figura 21. Conexión PC-B a la VLAN 3 en R1 con IPv4 .*
		Ipv6	2001:db8:acad:b: :1	 *Figura 22. Conexión PC-B a la VLAN 3 en R1 con IPv4 .*

	R1, G0/0/1.4	Dirección	10.19.8.97	 *Figura 23. Conexión PC-B a la VLAN 4 en R1 con IPv4 .*
		Ipv6	2001:db8:acad:c: :1	 *Figura 24. Conexión PC-B a la VLAN 4 en R1 con IPv6 .*
	S1, VLAN 4	Dirección	10.19.8.98	 *Figura 25.Conexión PC-B a la VLAN 4 en S1 con IPv4 .*

		Ipv6	2001:db8:acad:c: :98	 *Figura 26.Conexión PC-B a la VLAN 4 en S1 con IPv6 .*
	S2, VLAN 4	Dirección	10.19.8.99.	 *Figura 27.Conexión PC-B a la VLAN 4 en S2 con IPv4 .*

		Ipv6	2001:db8:acad:c: :99	 *Figura 28.Conexión PC-B a la VLAN 4 en S2 con IPv6 .*

3.2 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 (ver Figura 29. Topología escenario 2).

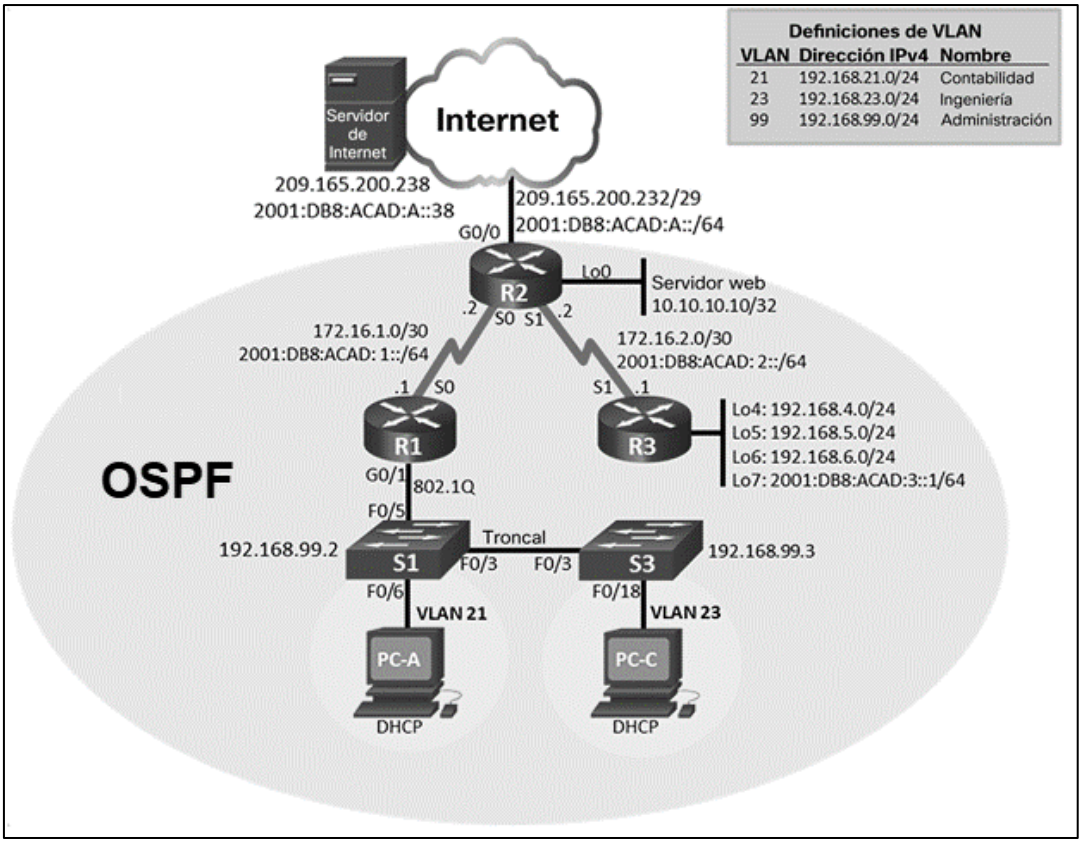


Figura 29. Topología escenario 2

A continuación, esta topología es configurada en el software, ver Figura 30. Topología del escenario 2 en Packet Tracer ®.

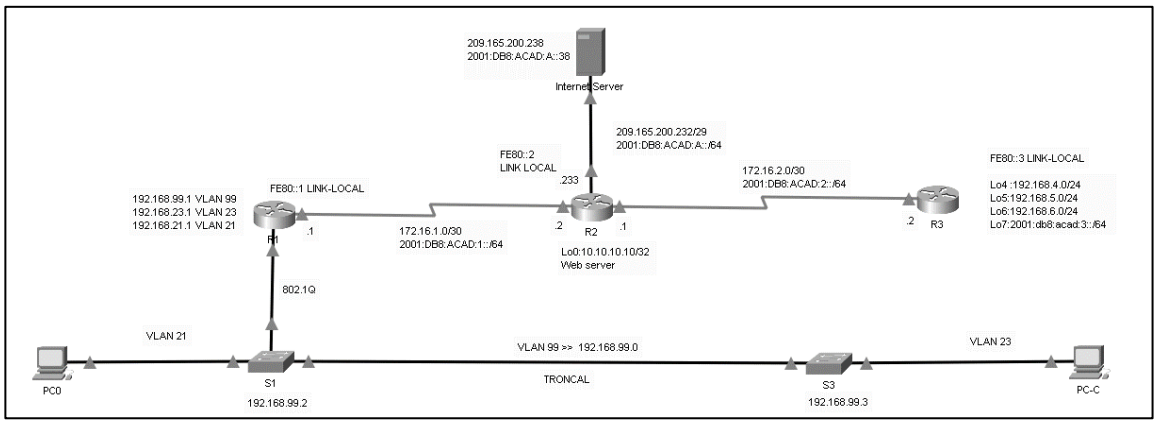


Figura 30. Topología del escenario 2 en Packet Tracer ®

3.2.1 Inicializar dispositivos

3.2.1.1 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.

Con los comandos de la Tabla 11, borramos alguna configuración anterior que tenga los routers y switches y reiniciamos en una configuración limpia.

Tabla 11. Borrar y reinicio de equipos escenario 2

Tarea	Comando de IOS
Eliminar el archivo startup-config de todos los routers	
Se borra alguna configuración previa en el equipo. (tecnologia y redes , 2014)	Router#erase startup-config
Volver a cargar todos los routers	
Se carga nuevamente la configuracion limpia. (tecnologia y redes , 2014)	Router#reload
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	Switch#erase startup-config Switch#delete flash:vlan.dat

Se elimina la base datos de Vlans anteriores. (tecnologia y redes , 2014) Volver a cargar ambos switches Recargamos nuevamente el Switch (cisco networking academy)	Switch#reload
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches. Confirmamos que el archivo Vlan.dat no se encuentre en la memoria Flash (cisco networking academy)	Switch>show flash

3.2.2 Configurar los parámetros básicos de los dispositivos

3.2.2.1 Configurar el servidor de Internet

Las tareas de configuración del servidor de Internet incluyen lo siguiente (para obtener información de las direcciones IP, consulte la topología), ver Tabla 12:

Tabla 12. Direccionamiento para el servidor de Internet simulado en escenario 2.

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
Gateway predeterminado IPv6	2001:DB8:ACAD:A::1

3.2.3 Configurar R1

Las tareas de configuración para R1 incluyen las siguientes (ver Tabla 13):

Tabla 13. Configuración básica R1 en escenario 2.

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS Se desactiva la búsqueda de dominio (tecnologia y redes , 2014)	Router(1)(config)#no ip domain-lookup
Nombre del router Se configura el nombre del router (tecnologia y redes , 2014)	Router(config)#hostname R1
Contraseña de exec privilegiado cifrada Se configura clave de acceso (tecnologia y redes , 2014)	R1(config)#enable secret class
Contraseña de acceso a la consola Se configura clave de acceso a la consola (tecnologia y redes , 2014)	R1(config)#line console 0 R1(config-line)#password cisco
Contraseña de acceso Telnet Se configura el acceso a Telnet con clave (tecnologia y redes , 2014)	R1(config-line)#login R1(config-line)#line vty 0 15 R1(config-line)#password cisco
Cifrar las contraseñas de texto no cifrado Se encripta las claves (tecnologia y redes , 2014)	R1(config-line)#login R1(config-line)#service password-encryption
Mensaje MOTD Se edita mensaje para usuarios no autorizados. (tecnologia y redes , 2014)	R1(config)#banner motd "Se prohíbe el acceso no autorizado."

Interfaz S0/1/0 Se configura la interfaz serial que está conectado a R2 a) Establezca la descripción b) Establecer la dirección IPv4 Consultar el diagrama de topología para conocer la información de direcciones c) Establecer la dirección IPv6 Consultar el diagrama de topología para conocer la información de direcciones d) Establecer la frecuencia de reloj en 128000 e) Activar la interfaz (cisco networking academy)	R1(config)#int s0/1/0 R1(config-if)#description "Conexión a R2" R1(config-if)#ip address 172.16.1.1 255.255.255.252 R1(config-if)#ipv6 address 2001:db8:acad:1::1/64 R1(config-if)#clock rate 128000 R1(config-if)#no shutdown
Rutas predeterminadas Se configura la ruta predeterminada o cuádruple cero a la interfaz serial conectada a R2 en ipv4/ipv6. a) Configurar una ruta IPv4 predeterminada de S0/1/0 b) Configurar una ruta IPv6 predeterminada de S0/1/0 (cisco networking academy)	R1(config-if)#exit R1(config)#ip route 0.0.0.0 0.0.0.0 s0/1/0 R1(config)#ipv6 route ::/0 s0/1/0

3.2.4 Configurar R2

La configuración del R2 incluye las siguientes tareas(ver

Tabla 14):

Tabla 14. Configuración básica R2 en escenario 2.

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS Se desactiva la búsqueda automática a dominios. (tecnologia y redes , 2014)	Router(config)#no ip domain-lookup
Nombre del router Se configura el nombre del Router (tecnologia y redes , 2014)	Router(config)#hostname R2
Contraseña de exec privilegiado cifrada Se configura la clave de acceso (tecnologia y redes , 2014)	R2(config)#enable secret class
Contraseña de acceso a la consola Se configura clave de acceso a la consola (tecnologia y redes , 2014)	R2(config)#line console 0 R2(config-line)#password cisco
Contraseña de acceso Telnet Se configura clave de acceso a Telnet (tecnologia y redes , 2014)	R2(config-line)#login R2(config-line)#line vty 0 15 R2(config-line)#password cisco
Cifrar las contraseñas de texto no cifrado Encriptamos las contraseñas (cisco networking academy)	R2(config-line)#login R2(config-line)#service password-encryption
Habilitar el servidor HTTP	No está habilitado para Packet tracer®
Mensaje MOTD Se edita mensaje para usuarios no autorizados. (tecnologia y redes , 2014)	R2(config)#banner motd "Se prohíbe el acceso no autorizado."

Interfaz S0/1/0 Se configura la interfaz serial que está conectada a R1 en ipv4/ipv6 a) Establezca la descripción b) Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. c) Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. d) Activar la interfaz (cisco networking academy)	R2(config)#int s0/1/0 R2(config-if)#description "conexión a R1" R2(config-if)#ip address 172.16.1.2 255.255.255.252 ipv6 address 2001:db8:acad:1::2/64 R2(config-if)#no shutdown
Interfaz S0/1/1 Se configura la interfaz serial que está conectada a R3 en ipv4/ipv6 a) Establecer la descripción b) Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. c) Establecer la frecuencia de reloj en 128000. d) Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. e) Activar la interfaz (cisco networking academy)	R2(config-if)#int s0/1/1 R2(config-if)#description "conexión a R3" R2(config-if)#ip address 172.16.2.1 255.255.255.252 (config-if)#ipv6 address 2001:db8:acad:2::1/64 R2(config-if)#clock rate 128000 R2(config-if)#no shutdown

Interfaz G0/0 (simulación de Internet) (cisco networking academy) Se configura la interfaz que está conectada al servidor de internet en ipv4/ipv6 a) Establecer la descripción. b) Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. c) Establezca la dirección IPv6. Utilizar la primera dirección disponible en la subred. d) Activar la interfaz	R2(config)#int g0/0 R2(config-if)#description " conexión a Internet" R2(config-if)#ip address 209.165.200.233 255.255.255.248 R2(config-if)#ipv6 address 2001:db8:acad:a::1/64 R2(config-if)#no shutdown
Interfaz loopback 0 (servidor web simulado) (cisco networking academy) Se configura la interfaz de bucle que simula el servidor web interno en ipv4 a) Establecer la descripción. b) Establezca la dirección IPv4.	R2(config)#interface loopback 0 R2(config-if)#ip address 10.10.10.10 255.255.255.255
Ruta predeterminada (Cisco networking Academy) Se configura la ruta estática predeterminada o cuádruple cero. En ipv4/ipv6 a) Configure una ruta IPv4 predeterminada de G0/0. b) Configure una ruta IPv6 predeterminada de G0/0.	R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0 ipv6 route ::/0 g0/0

3.2.5 Configurar R3

La configuración del R3 incluye las siguientes tareas (ver Tabla 15)

Tabla 15. Configuración básica R3 en escenario 2.

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS Se desactiva la búsqueda de dominios (tecnologia y redes , 2014)	Router(config)#no ip domain-lookup
Nombre del router Se nombra al router (tecnologia y redes , 2014)	R3 Router(config)#hostname R3
Contraseña de exec privilegiado cifrada Se configura clave de acceso (tecnologia y redes , 2014)	R3(config)#enable secret class
Contraseña de acceso a la consola Se configura clave de acceso a la consola (tecnologia y redes , 2014)	R3(config)#line console 0 R3(config-line)#password cisco
Contraseña de acceso Telnet Se configura clave a la conexión telnet (tecnologia y redes , 2014)	R3(config-line)#login R3(config-line)#line vty 0 15 R3(config-line)#password cisco
Cifrar las contraseñas de texto no cifrado Se encripta las contraseñas (tecnologia y redes , 2014)	R3(config-line)#login R3(config-line)#service password-encryption
Mensaje MOTD Se edita mensaje de advertencia a usuarios no autorizados. (tecnologia y redes , 2014)	R3(config)#banner motd "Se prohíbe el acceso no autorizado."

Interfaz S0/1/0 Se configura la interfaz serial conectada a R2 en ipv4/ipv6 a) Establecer la descripción b) Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. c) Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. d) Activar la interfaz (Cisco networking academy)	R3(config)#int s0/1/0 R3(config-if)#description "conexión a R2" R3(config-if)#ip address 172.16.2.2 255.255.255.252 ipv6 address 2001:db8:acad:2::2/64 R3(config-if)#no shutdown
Interfaz loopback 4 Se configura la interfaz Lo4 Se Establece la dirección IPv4. Utilizar la primera dirección disponible en la subred. (Cisco networking academy)	R3(config)#int loopback 4 R3(config-if)#ip address 192.168.4.1 255.255.255.0
Interfaz loopback 5 Se configura la interfaz Lo5 Se Establece la dirección IPv4. Utilizar la primera dirección disponible en la subred. (Cisco networking academy)	R3(config)#int loopback 5 R3(config-if)#ip address 192.168.5.1 255.255.255.0
Interfaz loopback 6 Se configura la interfaz Lo6 Se Establece la dirección IPv4. Utilizar la primera dirección disponible en la subred. (Cisco networking academy)	R3(config)#interface loopback 6 R3(config-if)#ip address 192.168.6.1 255.255.255.0
Interfaz loopback 7 Se configura la interfaz Lo6 Se Establece la dirección IPv6. (Cisco networking academy)	R3(config)#interface loopback 7 R3(config-if)#ipv6 address 2001:db8:acad:3::1/64

Ruta predeterminada Se configura la ruta estática predeterminada o cuádruple cero. En ipv4/ipv6 a) Configure una ruta IPv4 predeterminada de S0/1/0. b) Configure una ruta IPv6 predeterminada de S0/1/0. (Cisco networking Academy)	R3(config)#ip route 0.0.0.0 0.0.0.0 s0/1/0 R3(config)#ipv6 route ::/0 s0/1/0

3.2.6 Configurar S1

La configuración del S1 incluye las siguientes tareas (ver Tabla 16)

Tabla 16. Configuración básica S1 en escenario 2

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS Se desactiva la búsqueda automática de dominios. (tecnologia y redes , 2014)	Switch(config)#no ip domain-lookup
Nombre del switch Se nombra al switch S1 (tecnologia y redes , 2014)	Switch(config)#hostname S1
Contraseña de exec privilegiado cifrada Se configura clave de acceso (tecnologia y redes , 2014)	S1(config)#enable secret class
Contraseña de acceso a la consola Se configura clave de acceso a la consola (tecnologia y redes , 2014)	S1(config)#line console 0 S1(config-line)#password cisco
Contraseña de acceso Telnet Se configura clave de acceso a telnet (tecnologia y redes , 2014)	S1(config-line)#login S1(config-line)#line vty 0 15 S1(config-line)#password cisco

Cifrar las contraseñas de texto no cifrado Se encripta las claves de acceso (tecnologia y redes , 2014)	S1(config-line)#login S1(config-line)#service password-Encryption
Mensaje MOTD Se edita mensaje de advertencia a usuarios no autorizados. (cisco networking academy)	S1(config)#banner motd "Se prohíbe el acceso no autorizado."

3.2.7 Configurar el S3

La configuración del S3 incluye las siguientes tareas (Tabla 17)

Tabla 17. Configuración básica S3 en escenario 2.

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS Se desactiva la búsqueda automática de dominios. (tecnologia y redes , 2014)	Switch(config)#no ip domain-lookup
Nombre del switch Se nombra al switch S3 (tecnologia y redes , 2014)	Switch(config)#hostname S3
Contraseña de exec privilegiado cifrada Se configura clave de acceso (tecnologia y redes , 2014)	S1(config)#enable secret class
Contraseña de acceso a la consola Se configura clave de acceso a la consola (tecnologia y redes , 2014)	S1(config)#line console 0 S1(config-line)#password cisco
Contraseña de acceso Telnet Se configura clave de acceso a telnet (tecnologia y redes , 2014)	S1(config-line)#login S1(config-line)#line vty 0 15 S1(config-line)#password cisco
Cifrar las contraseñas de texto no cifrado Se encripta las claves de acceso (tecnologia y redes , 2014)	S1(config-line)#login S1(config-line)#service password-Encryption

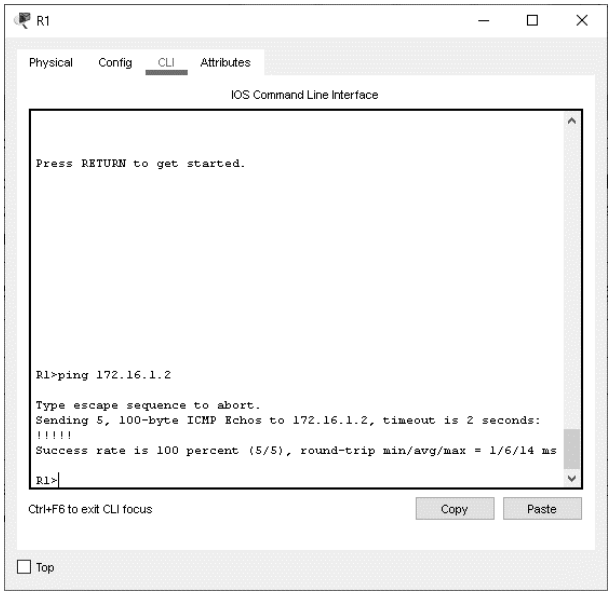
Mensaje MOTD Se edita mensaje de advertencia a usuarios no autorizados. (tecnologia y redes , 2014)	S1(config)#banner motd "Se prohíbe el acceso no autorizado."

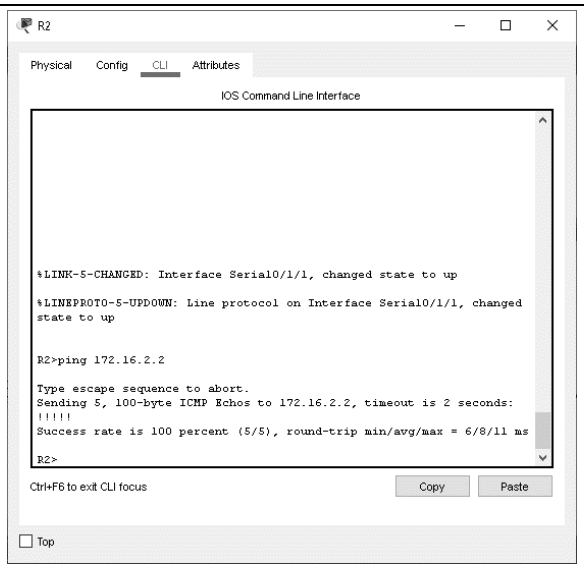
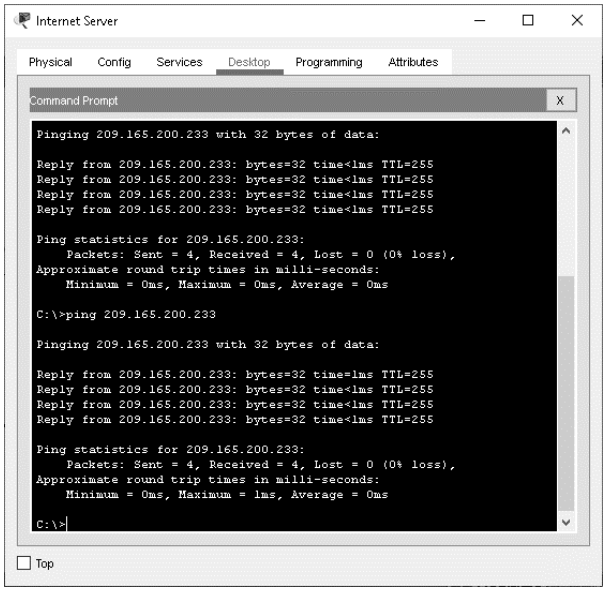
3.2.8 Verificar la conectividad de la red

Utilice el comando ping para probar la conectividad entre los dispositivos de red. (ver Tabla 18).

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 18. Prueba de conectividad entre routers escenario 2.

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/1/0	172.16.1.2	 *Figura 31.Prueba de conexión de R1 a R2.*

R2	R3, S0/1/0	172.16.2.2	 *Figura 32. Prueba de conexión de R1 a R3.*
PC de Internet	Gateway predeterminado	209.165.200.233	 *Figura 33. Prueba de conexión de desde Internet Server a R2.*

3.2.9 Configurar la seguridad del switch, las Vlan y el routing entre Vlan

3.2.9.1 Configurar S1

La configuración del S1 incluye las siguientes tareas (ver tabla 19):

Tabla 19. VLANs, y enlaces troncales y configuración de interfaces en S1 escenario 2

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN Se crean las VLAN según tabla de direccionamiento. (Cisco networking academy)	S1(config)#vlan 21 S1(config-vlan)#name Contabilidad S1(config-vlan)# vlan 23 S1(config-vlan)#name ingeniería S1(config-vlan)#vlan 99 S1(config-vlan)#name Administracion
Asignar la dirección IP de administración. Se asigna la dirección IPv4 a la VLAN de administración. Se Utiliza la dirección IP asignada al S1 en el diagrama de topología (Cisco networking academy)	S1(config)#int vlan 99 S1(config-if)#ip address 192.168.99.2 255.255.255.0
Asignar el gateway predeterminado Se asigna la primera dirección IPv4 de la subred como el gateway predeterminado. (Cisco networking academy)	S1(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3 Se utiliza f0/3 y la red VLAN 1 como VLAN nativa y enlace troncal (Cisco networking academy)	S1(config)#int f0/3 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1

Forzar el enlace troncal en la interfaz F0/5 Se utiliza f0/5 y la red VLAN 1 como VLAN nativa y enlace troncal (Cisco networking academy)	S1(config)#int f0/5 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1 S1(config-if)#no shutdown
Configurar el resto de los puertos como puertos de acceso Se utiliza el comando interface range para definir el resto de las interfaces en modo de acceso. (tecnologia y redes , 2014)	S1(config)#int range f0/1-2, f0/4, f0/6-24, g0/1-2 S1(config-if-range)#switchport mode access
Asignar F0/6 a la VLAN 21 Se configura f0/6 como interfaz de acceso a la VLAN 21 (Cisco networking academy)	S1(config-if-range)#int f0/6 S1(config-if)#switchport access vlan 21
Apagar todos los puertos sin usar (tecnologia y redes , 2014)	S1(config-if)#int range f0/1-2, f0/4, f0/7-24, g0/1-2 S1(config-if-range)#shutdown

3.2.9.2 Configurar S3

La configuración del S3 incluye las siguientes tareas (ver Tabla 20)

Tabla 20. VLANs, y enlaces troncales y configuración de interfaces en S3 escenario 2

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN Se utiliza la tabla de equivalencias de VLAN para topología para crear cada una de las VLAN que se indican en la tabla de direccionamiento. (Cisco networking academy)	S3(config)#vlan 21 S3(config-vlan)#name Contabilidad S3(config-vlan)#vlan 23 S3(config-vlan)#name ingeniería S3(config-vlan)#vlan 99 S3(config-vlan)#name Administracion

Asignar la dirección IP de administración Se asigna la dirección IPv4 a la VLAN de administración. Se utiliza la dirección IP asignada al S3 en el diagrama de topología (Cisco networking academy)	S3(config)#int vlan 99 S3(config-if)# S3(config-if)#ip address 192.168.99.3 255.255.255.0 S3(config-if)#no shutdown
Asignar el gateway predeterminado. Se asigna la primera dirección IP en la subred como gateway predeterminado. (Cisco networking academy)	S3(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3 Se utiliza f0/3 en la red VLAN 1 como VLAN nativa (Cisco networking academy)	S3(config)#int f0/3 S3(config-if)#switchport mode trunk S3(config-if)#switchport trunk native vlan 1
Configurar el resto de los puertos como puertos de acceso Se utiliza el comando interface range para definir el resto de las interfaces en modo de acceso. (Cisco networking academy)	S3(config)#int range f0/1-2, f0/4-24, g0/1-2 S3(config-if-range)#switchport mode access
Asignar F0/18 a la VLAN 23 Se configura f0/18 como interfaz de acceso a la VLAN 23 (Cisco networking academy)	S3(config)#int f0/18 S3(config-if)#switchport access vlan 23
Apagar todos los puertos sin usar (tecnologia y redes , 2014)	S3(config)#int range f0/1-2, f0/4-17, f0/19-24, g0/1-2 S3(config-if-range)#shutdown

3.2.9.3 Configurar R1

Las tareas de configuración para R1 incluyen las siguientes (ver Tabla 21)

Tabla 21. VLANs, y enlaces troncales y configuración de interfaces en R1 escenario 2

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1 Se configura la subinterface g0/1.21como puerta de enlace predeterminado de la VLAN 21 mediante IEEE802.1Q (Cisco networking academy) a) Descripción: LAN de Contabilidad b) Asignar la VLAN 21 c) Asignar la primera dirección disponible a esta interfaz	R1(config)#int g0/1.21 R1(config-subif)#description LAN de contabilidad R1(config-subif)#encapsulation dot1q 21 R1(config-subif)#ip address 192.168.21.1 255.255.255.0
Configurar la subinterfaz 802.1Q .23 en G0/1 Se configura la subinterface g0/1.23como puerta de enlace predeterminado de la VLAN 23 mediante IEEE802.1Q (Cisco networking academy) a) Descripción: LAN de Ingeniería b) Asignar la VLAN 23 c) Asignar la primera dirección disponible a esta interfaz	R1(config)#int g0/1.23 R1(config-subif)#description LAN de ingeniería R1(config-subif)#encapsulation dot1q 23 R1(config-subif)#ip address 192.168.23.1 255.255.255.0

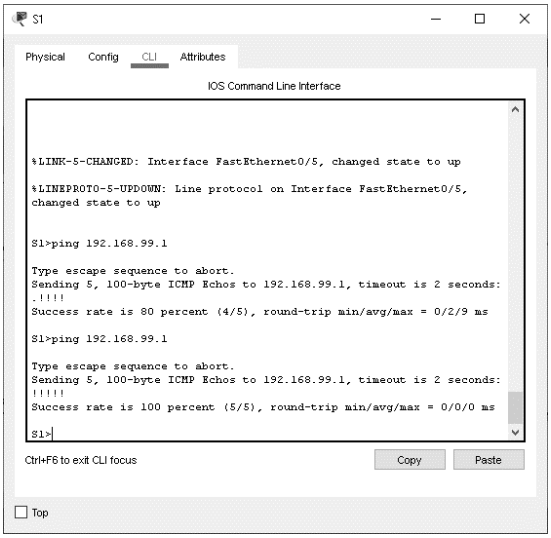
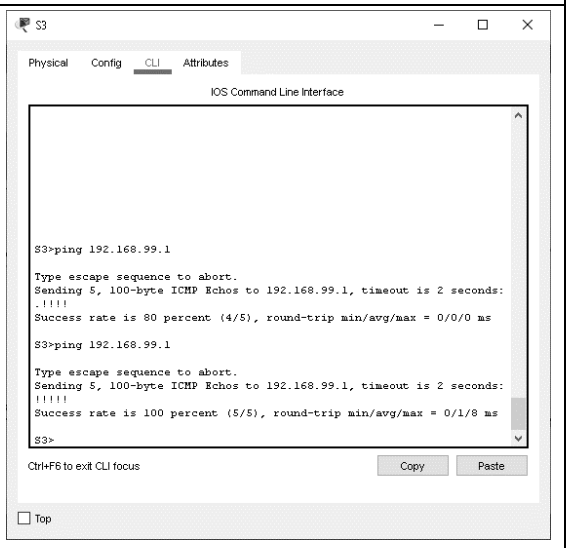
Configurar la subinterfaz 802.1Q .99 en G0/1. Se configura la subinterface g0/1.99 como puerta de enlace predeterminado de la VLAN 99 mediante IEEE802.1Q (Cisco networking academy) a) Descripción: LAN de Administración b) Asignar la primera dirección disponible a esta interfaz	R1(config)#int g0/1.99 R1(config-subif)#description LAN de administración R1(config-subif)#encapsulation dot1q 99 R1(config-subif)#ip address 192.168.99.1 255.255.255.0
Activar la interfaz G0/1 Iniciar la interfaz principal G0/1 para activar el enrutamiento entre VLANs. (tecnologia y redes , 2014)	R1(config)#int g0/1 R1(config-if)#no shutdown

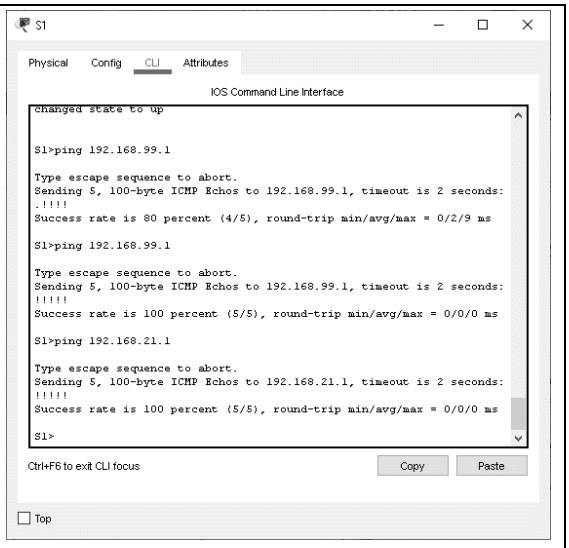
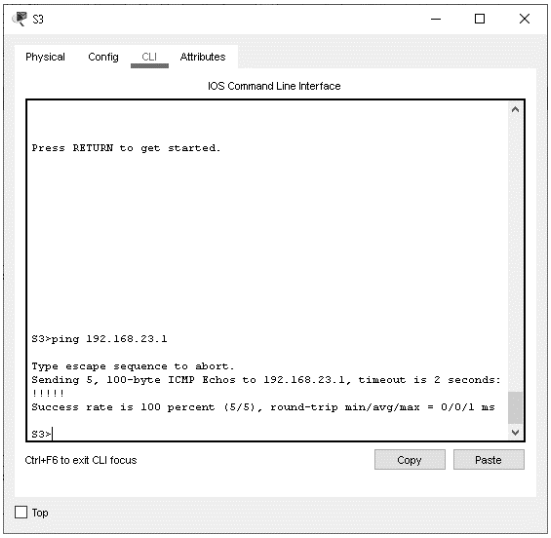
3.2.10 Verificar la conectividad de la red

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

Utilice la Tabla 22 para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Tabla 22. Prueba de conexión entre switches y routers en escenario 2

Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.1	 *Figura 34. Prueba de conexión desde S1 a R1 mediante la VLAN 99.*
S3	R1, dirección VLAN 99	192.168.99.1	 *Figura 35. Prueba de conexión desde S3 a R1 mediante la VLAN 99.*

S1	R1, dirección VLAN 21	192.168.21.1	 *Figura 36. Prueba de conexión desde S1 a R1 mediante la VLAN 21.*
S3	R1, dirección VLAN 23	192.168.23.1	 *Figura 37. Prueba de conexión desde S3 a R1 mediante la VLAN 23*

3.2.11 Configurar el protocolo de routing dinámico OSPF

3.2.11.1 Configurar OSPF en el R1

Las tareas de configuración para R1 incluyen las siguientes (ver Tabla 23):

Tabla 23. Configuración protocolo OSPF en R1

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0 Se inicia y se nombra el protocolo OSPF en R1 (Cisco neetworking academy)	R1(config)#router ospf 10 R1(config-router)#router-id 1.1.1.1
Anunciar las redes conectadas directamente Se configura las redes que tiene acceso R1 para que los demás routers puedan tener acceso. (Cisco neetworking academy)	Asigne todas las redes conectadas directamente. R1(config-router)#network 192.168.99.1 0.0.0.0 area 0 R1(config-router)#network 192.168.23.1 0.0.0.0 area 0 R1(config-router)#network 192.168.21.1 0.0.0.0 area 0 R1(config-router)#network 172.16.1.0 0.0.0.3 area 0 R1(config-router)#
Se establece todas las interfaces LAN como pasivas (Cisco networking academy)	R1(config-router)#passive-interface g0/1.21 R1(config-router)#passive-interface g0/1.23 R1(config-router)#passive-interface g0/1.99
Desactive la sumarización automática	No está disponible para packet tracer®.

3.2.11.2 Actividad Adicional: configuración OSPFv3 EN R1

Se determina configurar el enrutador R1 con el protocolo OSPFv3 ya que, también hay una comunicación en IPV6 por el puerto serie S0/1/0, (ver Figura 38. configuración protocolo OSPFv3 en R1.) (Cisco networking academy)

```
R1(config)#ipv6 unicast-routing
R1(config)#ipv6 router ospf 10
R1(config-rtr)#router-id 1.1.1.1
R1(config)#int s0/1/0
R1(config-if)#ipv6 address fe80::1 link-local
R1(config-if)#ipv6 ospf 10 area 0
```

Figura 38. configuración protocolo OSPFv3 en R1.

3.2.11.3 Configurar OSPF en el R2

La configuración del R2 incluye las siguientes tareas (Ver Tabla 24)

Tabla 24. Configuración protocolo OSPF en R2

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0 Se inicia y se nombra el protocolo OSPF en R2 (Cisco neetworking academy)	R2(config)#router ospf 10 R2(config-router)#router-id 2.2.2.2
Anunciar las redes conectadas directamente **Nota:** Omitir la red G0/0. Se configura las redes que tiene acceso R2 para que los demás routers puedan tener acceso. (Cisco neetworking academy)	R2(config-router)#network 172.16.1.0 0.0.0.3 area 0 R2(config-router)#network 172.16.2.0 0.0.0.3 area 0 R2(config-router)#network 10.10.10.10 0.0.0.0 area 0
Se establece la interfaz LAN (loopback) como pasiva (Cisco networking academy)	R2(config-router)#passive-interface loopback 0
Desactive la sumarización automática.	No está disponible para packet tracer®.

3.2.11.4 Configurar OSPFv3 en R2

La configuración del R2 incluye las siguientes tareas (ver Tabla 25)

Tabla 25. Configuración protocolo OSPFv3 en R2

Elemento o tarea de configuración	Especificación
Configurar OSPFv3 área 0 Se inicia y se nombra el protocolo OSPFv3 en R2 (Cisco networking academy)	R2(config)#ipv6 unicast-routing R2(config)#int g0/0 R2(config-if)#ipv6 address fe80::2 link-local R2(config-if)#int s0/1/0 R2(config-if)#ipv6 address fe80::2 link-local R2(config-if)#int s0/1/1 R2(config-if)#ipv6 address fe80::2 link-local R2(config)#ipv6 router ospf 10 R2(config-rtr)#router-id 2.2.2.2 R2(config-rtr)#auto-cost reference-bandwidth 1000
Anunciar redes IPv6 conectadas directamente (Cisco networking academy)	R2(config)#interface g0/0 R2(config-if)#ipv6 ospf 10 area 0 R2(config-if)#int s0/1/0 R2(config-if)#ipv6 ospf 10 area 0 R2(config-if)#int s0/1/1 R2(config-if)#ipv6 ospf 10 area 0 R2(config-if)#end
Se establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas (Cisco networking academy)	R2(config-router)#passive-interface loopback 0
Desactive la sumarización automática.	No disponible para packet tracer®.

3.2.11.5 Actividad adicional configurar OSPF en R3

La configuración del R3 incluye las siguientes tareas (ver Tabla 26)

Tabla 26. Configuración protocolo OSPF en R3

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0 Se inicia y se nombra el protocolo OSPF en R3	R3(config)#router ospf 10 R3(config-router)#router-id 3.3.3.3
Anunciar redes IPv4 conectadas directamente Se configura las redes que tiene acceso R2 para que los demás routers puedan tener acceso.	R3(config-router)#network 172.16.2.0 0.0.0.3 area 0 R3(config-router)#network 192.168.4.1 0.0.0.0 area 0 R3(config-router)#network 192.168.5.1 0.0.0.0 area 0 R3(config-router)#network 192.168.6.1 0.0.0.0 area 0
Se establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	R3(config-router)#passive-interface loopback 4 R3(config-router)#passive-interface loopback 5 R3(config-router)#passive-interface loopback 6
Desactive la sumarización automática.	No disponible para packet tracer®.

3.2.11.6 Actividad adicional configurar OSPFv3 en R3

La configuración del R3 incluye las siguientes tareas (ver Tabla 27. Configuración protocolo OSPFv3 en R3)

Tabla 27. Configuración protocolo OSPFv3 en R3

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0 Se inicia y se nombra el protocolo OSPFv3 en R3 (Cisco networking Academy)	R3(config)#ipv6 unicast-routing R3(config)#ipv6 router ospf 10 R3(config-rtr)#router-id 3.3.3.3

Anunciar redes IPv6 conectadas directamente (Cisco networking academy)	R3(config)#int s0/1/0 R3(config-if)#ipv6 ospf 10 area 0 R3(config-if)#ipv6 address fe80::3 link-local R3(config)#interface loopback 7 R3(config-if)#ipv6 address fe80::3 link-local R3(config-if)#ipv6 ospf 10 area 0
Se establece todas las interfaces de LAN IPv6 (Loopback) como pasivas (Cisco networking academy)	R3(config)#ipv6 router ospf 10 R3(config-rtr)#passive-interface loopback 7
Desactive la sumarización automática.	No disponible para packet tracer®

3.2.12 Verificar la información de OSPF

Verifique que OSPF esté funcionando como se espera. Introduzca el comando de CLI adecuado para obtener la siguiente información (ver Tabla 28. Comandos de Informacion protocolo y Tabla 29.)

Tabla 28. Comandos de Informacion protocolo OSPF obtenidos de R1

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? (tecnologia y redes , 2014)	R1#show ip protocols
¿Qué comando muestra solo las rutas OSPF? (Cisco networking academy)	R1#show ip route ospf
¿Qué comando muestra la sección de OSPF de la configuración en ejecución? (Cisco networking academy)	R1#show running-config | section router ospf

Tabla 29. Comandos de Informacion protocolo OSPFv3 obtenidos de R1

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? (Cisco networking Academy)	R1#show ipv6 protocols
¿Qué comando muestra solo las rutas OSPF? (Cisco networking Academy)	R1#show ipv6 route ospf
¿Qué comando muestra la sección de OSPF de la configuración en ejecución? (tecnologia y redes , 2014)	R1#show running-config | section router ospf

3.2.13 Implementar DHCP y NAT para IPv4

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

Las tareas de configuración para R1 incluyen las siguientes (ver Tabla 30)

Tabla 30. Configuración DHCP en VLANs en R1

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas Se configura DHCP y se excluye direcciones para V21 (tecnologia y redes , 2014)	R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.21
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas Se configura DHCP y se excluye direcciones para V23 (tecnologia y redes , 2014)	R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.21

Crear un pool de DHCP para la VLAN 21. Se nombra el servidor DHCP para el área de Contaduría. Se configura el servidor DNS Se configura la puerta de enlace predeterminado para VLAN 21 (tecnologia y redes , 2014)	Nombre: ACCT R1(config)#ip dhcp pool ACCT R1(dhcp-config)#network 192.168.21.0 255.255.255.0 Servidor DNS: 10.10.10.10 R1(dhcp-config)#dns-server 10.10.10.10 Nombre de dominio: ccna-sa.com R1(dhcp-config)#domain-name ccna-sa.com Establecer el gateway predeterminado R1(dhcp-config)#default-router 192.168.21.1
Crear un pool de DHCP para la VLAN 23 Se nombra el servidor DHCP para el área de ingeniería. Se configura el servidor DNS Se configura la puerta de enlace predeterminado para VLAN 23 (tecnologia y redes , 2014)	Nombre: ENGNR R1(config)#ip dhcp pool ENGNR Servidor DNS: 10.10.10.10 R1(dhcp-config)#dns-server 10.10.10.10 Nombre de dominio: ccna-sa.com R1(dhcp-config)#domain-name ccna-sa.com Establecer el gateway predeterminado R1(dhcp-config)#default-router 192.168.23.1

3.2.13.1 Configurar la NAT estática y dinámica en el R2

La configuración del R2 incluye las siguientes tareas (ver Tabla 31)

Tabla 31. Configuración de NAT dinámica y estática en R2

Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario (Cisco networking academy)	Nombre de usuario: webuser Contraseña: cisco12345 Nivel de privilegio: 15 R2(config)#username webuser privilege 15 secret cisco12345
Habilitar el servicio del servidor HTTP	No aplica para packet tracer®
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	No aplica para packet tracer®

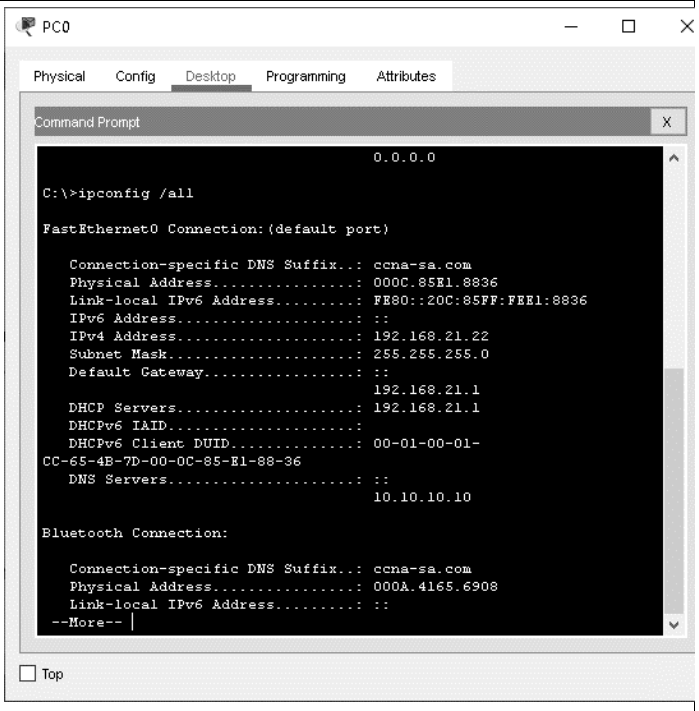
Crear una NAT estática al servidor web. Se Traduce la dirección privada del webserver a una dirección publica con salida a internet. (Cisco networking academy)	Dirección global interna: 209.165.200.229 R2(config)# ip nat inside source static 10.10.10.10 209.165.200.229
Se asigna la interfaz interna y externa para la NAT estática (Cisco networking academy)	R2(config)#int lo 0 R2(config-if)#ip nat outside R2(config-if)#exit R2(config)#int s0/1/0 R2(config-if)#ip nat inside R2(config-if)#exit
Configurar la NAT dinámica dentro de una ACL privada Se permite la traducción de un resumen de las redes Se Permite la traducción de las redes de Contabilidad y de Ingeniería en el R1 (Cisco networking academy)	Lista de acceso: 1 R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255 LAN (loopback) en el R3 R2(config)#access-list 1 permit 192.168.4.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.5.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.6.0 0.0.0.255 R2(config)#int s0/1/1 R2(config-if)#ip nat inside
Defina el pool de direcciones IP públicas utilizables. Se limita el número de direcciones públicas que puede tomar NAT según el número de conexiones internas. (Cisco networking academy)	Nombre del conjunto: INTERNET El conjunto de direcciones incluye: 209.165.200.225 **–** 209.165.200.228 R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.248

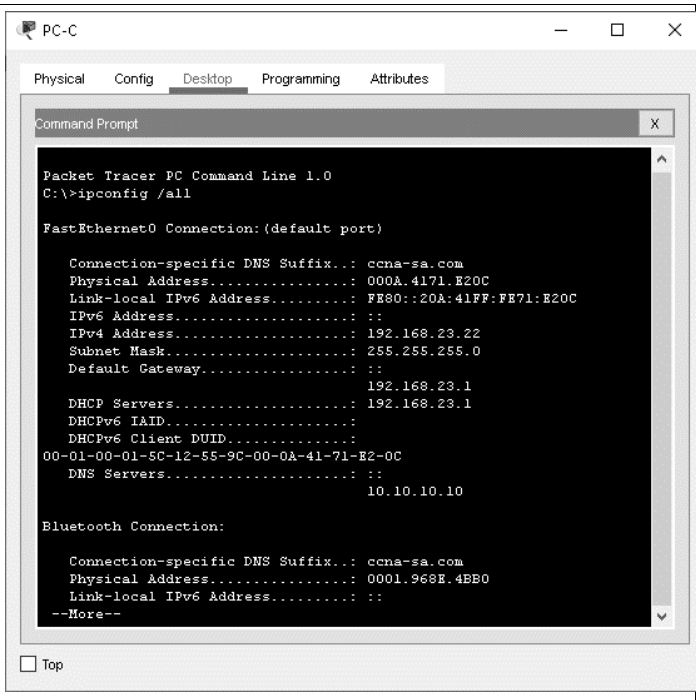
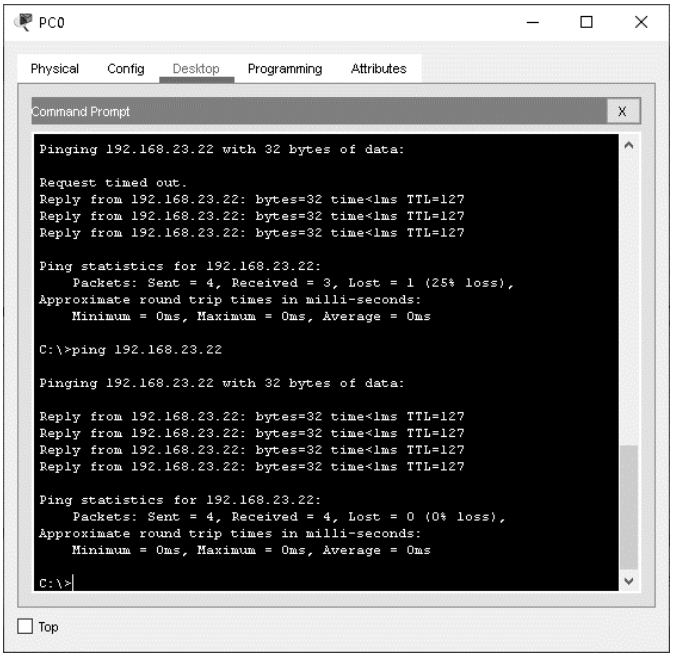
Definir la traducción de NAT dinámica Se configura que la interfaz g0/0 sea de salida hacia Internet. (Cisco networking academy)	R2(config)#ip nat inside source list 1 pool INTERNET R2(config)#int g0/0 R2(config-if)#ip nat outside

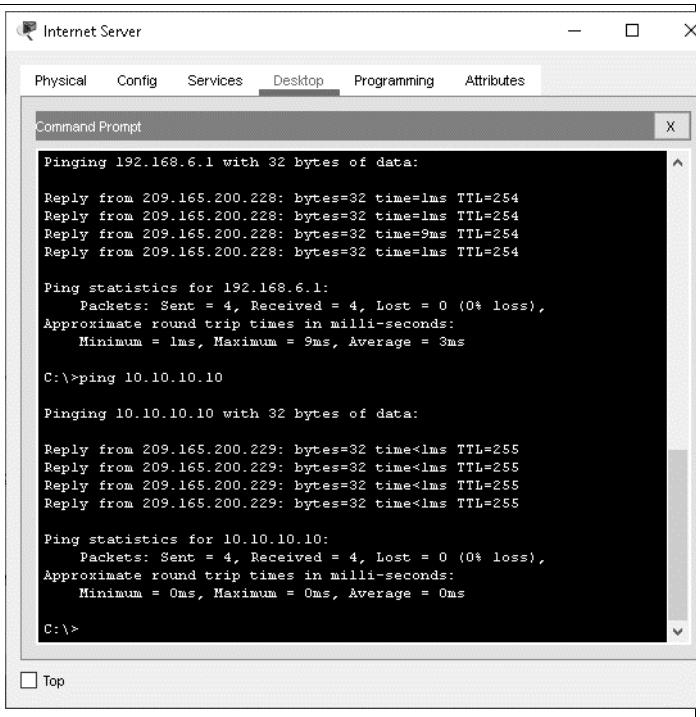
3.2.13.2 Verificar el protocolo DHCP y la NAT estática

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 (ver Tabla 32).

Tabla 32. Prueba de conexión DHCP entre los PCs

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	 *Figura 39. Prueba de conexión desde PC-A al servidor DHCP*

Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	 *Figura 40. Prueba de conexión desde PC-C al servidor DHCP*
Verificar que la PC-A pueda hacer ping a la PC-C	 *Figura 41. Prueba de conexión desde PC-A a PC-C*

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**	 *Figura 42. Conexión desde Internet server al web server interno.*

3.2.14 Configurar NTP

Tabla 33. Configuración servicio NTP maestro-servidor para routers

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2. Se ajustan fecha y hora. (Cisco networking academy)	12 de marzo de 2016, 9 a. m. R2#clock set 9:00:00 5 march 2016
Configure R2 como un maestro NTP. Se configura R2 como maestro NTP (Cisco networkig academy)	Nivel de estrato: 5 R2(config)#ntp master 5
Se configura R1 como un cliente NTP. (Cisco networkig academy)	Servidor: R2 R1(config)#ntp server 172.16.1.2
Se Configura R1 para actualizaciones de calendario periódicas con hora NTP. (Cisco networkig academy)	R1(config)#ntp update-calendar

Verifique la configuración de NTP en R1. (Cisco networkig academy)	R1#show ntp status

3.2.14.1 Configurar y verificar las listas de control de acceso (ACL)

Restringir el acceso a las líneas VTY en el R2 (ver Tabla 34).

Tabla 34. Configuración Lista de acceso a 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 (Cisco networking academy)	Nombre de la ACL: **ADMIN-MGT** R2(config)#ip access-list standard ADMIN-MGT R2(config-std-nacl)#permit host 172.16.1.1
Aplicar la ACL con nombre a las líneas VTY Se configura la conexión telnet (tecnologia y redes , 2014)	R2(config)#line vty 0 15 R2(config-line)#access-class ADMIN-MGT in
Permitir acceso por Telnet a las líneas de VTY (tecnologia y redes , 2014)	R2(config-line)#transport input telnet
Verificar que la ACL funcione como se espera (tecnologia y redes , 2014)	R1#telnet 172.16.1.2 R3#telnet 172.16.1.2

3.2.14.2 Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente

Tabla 35. Informacion de lista de accesos y traducciones NAT en R2.

Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció (tecnologia y redes , 2014)	R2#show access-lists
Restablecer los contadores de una lista de acceso (tecnologia y redes , 2014)	R2#clear access-list counters
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica? (tecnologia y redes , 2014)	R2#show ip interface *ID 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.

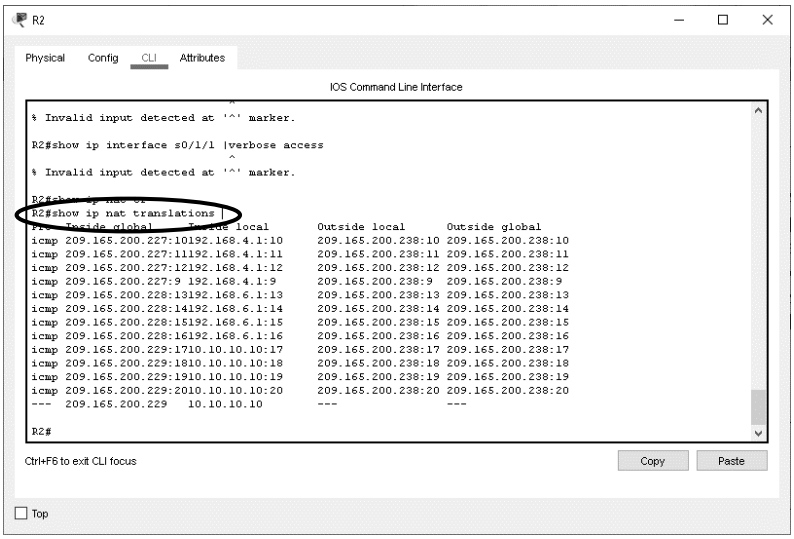


Figura 43. Direcciones de traslado NAT detectadas.

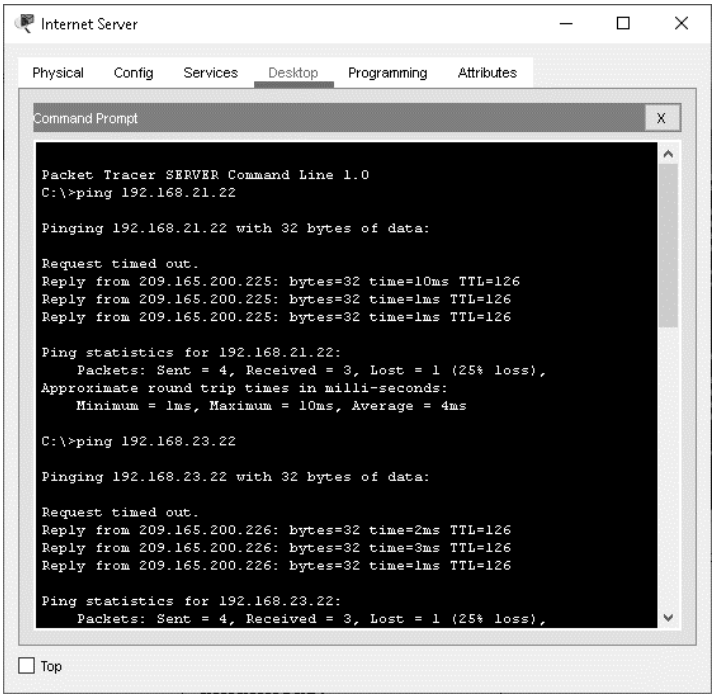


Figura 44. Prueba de conexión a las direcciones NAT publicas configuradas

¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas? (tecnologia y redes , 2014)	R2#clear ip nat translation

CONCLUSIONES

Packet tracer® ayuda simular el funcionamiento de cualquier topología de red, ayudando a minimizar los tiempos de instalación y puesta en marcha del sistema.

Los enlaces VLAN permiten la comunicación entre switches y ayuda a disminuir el cableado y hardware para la intercomunicación entre redes. Por medio de ellas podemos separar diferentes redes conectadas físicamente a switches comunes.

La encapsulación IEEE 802.1Q permite diferenciar diferentes tramas Ethernet asociadas a diferentes VLAN e interconectarlas con una misma comunicación troncal común.

El protocolo DHCP ayuda a los administradores de red a suministrar direcciones IP automáticamente a los Host de la red, reduciendo el tiempo de mantenimiento y puesta a punto de la red.

Las listas de control de acceso (ACL), ayudan a controlar el tráfico de paquetes en la red, mejorando la seguridad dentro y fuera de esta.

El protocolo NAT ayudan a mitigar el agotamiento de las direcciones IPv4 públicas, ayudan a la seguridad de la red, enmascarando y ocultando la informacion física de un host en particular.

REFERENCIAS

Alvarez, Alex. 2009. Entre Redes y Servidores. [En línea] mayo de 2009. https://alexalvarez0310.wordpress.com/category/comandos-basicos-de-un-router-cisco/.

Cama-pinto, Alejandro, De la Hoz, Emiro y Cama-pinto, Dora. Las redes de sensores inalámbricos y el Internet de las cosas. [En línea] http://hdl.handle.net/11323/1546.

Carvajal, Jaime Humberto. La Cuarta Revolución Industrial o Industria 4.0. [En línea] Universidad Antonio Nariño. http://www.laccei.org/LACCEI2017-BocaRaton/work_in_progress/WP386.pdf.

Cisco neetworking academy. 8.2.1.2 Modo de configuración de OSPF del router. [En línea] https://www.itesa.edu.mx/netacad/switching/course/module8/index.html#8.2.1.2.

Cisco Networkig Academy. 2020. Descargar Cisco Packet tracer. [En línea] Agosto de 2020. https://www.netacad.com/portal/resources/packet-tracer.

Cisco networkig academy. Funcionamiento de NTP. [En línea] https://contenthub.netacad.com/legacy/CCNA/RSE/6.0/es/index.html#10.2.1.2.

Cisco networking academy. 11.2.1.1 Configuración de NAT estática. [En línea] https://www.itesa.edu.mx/netacad/switching/course/module11/index.html#11.2.1.1.

—. 11.2.2.2 Configuración de NAT dinámica. [En línea] https://www.itesa.edu.mx/netacad/switching/course/module11/index.html#11.2.2.2.

—. 8.2.2.1 Habilitación de OSPF en las interfaces. [En línea] https://www.itesa.edu.mx/netacad/switching/course/module8/index.html#8.2.2.1.

—. 8.2.2.5 Configuración de interfaces pasivas. [En línea] https://www.itesa.edu.mx/netacad/switching/course/module8/index.html#8.2.2.5.

—. 8.2.4.2 Verificación de la configuración del protocolo OSPF. [En línea] https://www.itesa.edu.mx/netacad/switching/course/module8/index.html#8.2.4.2.

—. 8.3.2.6 Habilitación de OSPFv3 en las interfaces. [En línea] https://www.itesa.edu.mx/netacad/switching/course/module8/index.html#8.3.2.6.

Cisco networking Academy. 8.3.3.2 Verificación de la configuración del protocolo OSPFv3. [En línea] https://www.itesa.edu.mx/netacad/switching/course/module8/index.html#8.3.3.2.

Cisco networking academy. 8.3.3.3 Verificación de las interfaces OSPFv3. [En línea] https://www.itesa.edu.mx/netacad/switching/course/module8/index.html#8.3.3.3.

—. 9.3.2.1 Configurar las ACL extendidas. [En línea] https://www.itesa.edu.mx/netacad/switching/course/module9/index.html#9.3.2.1.

—. Capítulo 5: Enrutamiento entre VLAN. [En línea] https://www.itesa.edu.mx/netacad/switching/course/module5/index.html#5.1.3.2.

—. Configuración de router-on-a-stick: configuración de subinterfaces del router. [En línea] https://www.itesa.edu.mx/netacad/switching/course/module5/index.html#5.1.3.3.

—. Configuración del reloj del sistema. [En línea] https://contenthub.netacad.com/legacy/CCNA/RSE/6.0/es/index.html#10.2.1.1.

Cisco networking Academy. Introduccion a redes conmutadas. [En línea] https://www.itesa.edu.mx/netacad/switching/course/module1/index.html#1.0.1.1.

cisco networking academy. Introduccion a redes . [En línea] https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#1.2.2.1.

Diaz, Rodrigo. 2020. Prueba de Habilidades Prácticas CCNA. [En línea] 2020. https://repository.unad.edu.co/handle/10596/34037.

tecnologia y redes . 2014. tecnologia y redes. [En línea] 16 de Noviembre de 2014. http://tecnologiayredes.tyrdomains.com/node/16.

ANEXOS

Anexo A. Archivos de los 2 escenarios en packet tracer.

https://unadvirtualedu-my.sharepoint.com/:u:/g/personal/amunozf_unadvirtual_edu_co/EYUlxrNIn1hNvVp4PQ-D4A0BbpIrh9yhFXHnEbi1Kq9ojg?e=bJHshI

Anexo B. Articulo científico escenario 2.

Ver página siguiente.

Reporte sobre conectividad simulada en routing y switching bajo tecnología CISCO

Alejandro Muñoz Forero
Universidad nacional abierta y a distancia UNAD, amunozf@unadvirtual.edu.co

Resumen

En este documento se propuso un escenario simulado de conectividad mediante el software Cisco Packet tracer bajo los protocolos IPv4 y IPv6. La interconexión de 2 conmutadores (switches) y 3 enrutadores (routers) como columna vertebral (backbone) es el eje central del escenario. La conectividad se realizó mediante varias técnicas de interconexión como el encapsulamiento IEEE 802.1Q, y el protocolo de enlace troncal entre VLAN´s (VTP) , también se utilizó el protocolo DHCP para dar conectividad a los hosts conectados a la red. También se realizó la simulación del protocolo de enrutamiento dinámico OSPF (Open Short Path first) para la interconexión de los 3 routers y la traducción de redes de internet privadas/públicas en IPV4 (NAT) y configuración de listas de accesos (ACL). Se sincronizaron los routers en fecha y hora mediante el protocolo NTP y por supuesto se configuraron de manera segura los enrutadores mediante claves encriptadas por medio de la conexión local y remota. Como resultado se muestra la simulación del envío y la respuesta de paquetes entre los hosts mediante la utilidad PING.

Palabras clave: IPv6, IEEE802.1Q, Listas de control de acceso, NAT, NTP, OSPF, VTP.

Abstract:

In this paper, we proposed a simulated connectivity scenario with Cisco Packet tracer software under the IPv4 and IPv6 protocols. The interconnection of 2 switches (switches) and 3 routers (routers) as a backbone is the central axis of this scenario. The connectivity was carried out through various interconnection techniques such as IEEE 802.1Q encapsulation, and the trunking protocol between VLANs (VTP), the DHCP protocol was also used to provide connectivity to the hosts connected to the network. The simulation of the dynamic routing protocol OSPF (Open Short Path first) was also carried out for the interconnection of the 3 routers and the translation of private / public internet networks in IPV4 (NAT) and access lists configuration (ACL). The routers were synchronized in date and time using the NTP protocol and of course the routers were configured in a secure way using encrypted keys through the local and remote connection. As a result, the simulation of the sending and response of packets between the hosts is shown using the PING utility.

Keywords—: Access Control Lists, IPv6, IEEE802.1Q, NAT, NTP, OSPF, VTP.

I. Introducción

Las redes de comunicación están en constante cambio, ya que las necesidades humanas en la actualidad están migrando a ser más digitales, cada dia el consumo de informacion (Voz, data, y video) por parte de los usuarios va en aumento y los nuevos servicios de entretenimiento en streaming y redes sociales han cambiado significativamente todos los aspectos de nuestra sociedad y nuestra cultura popular. El paradigma de intercambio de informacion entre las personas está cambiando a gran velocidad y está migrando de la modalidad presencial a la virtual gracias a las nuevas tecnologías de redes, software y hardware como smartphones, pc´s, tablets, smart tv entre otros, actualmente estamos asimilando y tratando de adaptarnos a todo este cambio cultural y tecnológico, mientras otra tecnología irruptora amenaza con llegar a nuestras vidas, la IoT (Internet of Things) donde además de personas, dispositivos electrónicos inteligentes junto con la IA(inteligencia artificial), también están participando en el intercambio de informacion con la humanidad utilizando como principal medio las redes de comunicación. Estos equipos están situados en diferentes lugares geográficos y diseñados para recolectar e intercambiar volúmenes de informacion y esta es almacenada, procesada, organizada y estudiada matemática, estadística y probabilísticamente, en grandes centro de datos (DataCenters) situados por todo el planeta, con el objetivo de poder predecir, investigar y observar comportamientos deterministas y estocásticos en todos las áreas del conocimiento y la cultura humana como por ejemplo redes sociales, cambio climático, tráfico aéreo, marítimo y terrestre, telemedicina, flujo de informacion, astronomía como por nombrar algunos. Actualmente los usuarios colocan más y más informacion en las redes, servidores y centros de datos, exponiendo la privacidad empresarial e individual a ser accedida por parte de personas, entidades o naciones no deseadas. Por tal razón, las redes de comunicación, dispositivos y participantes deben bloquear accesos no deseados y el diplomado de profundización cisco enseña la introducción a este mundo. La prueba de habilidades del diplomado propone simular

dos escenarios mediante el software cisco packet tracer®, el primero debe interconectar a 2 conmutadores (switches), 1 enrutador (router) como columna vertebral (Backbone) de la red LAN y simular la comunicación entre Hosts (2 PC´s), 1 salida con IP publica de internet con direcciones IPv4 e IPv6. En el segundo escenario se interconecta 2 conmutadores, 3 enrutadores como columna vertebral (Back-bone) de la red y se realiza la conexión simulada a un servidor externo de Internet, bajo VLANs internas y protocolo IEEE802.1Q, También se simula la comunicación entre Hosts (2 PC´s), y el suministro de direcciones ip automáticas mediante el protocolo DHCP y también se realiza la simulación de comunicación de un servidor interno web con direcciones IPv4 e IPv6.

II. DESCRIPCIÓN DEL PROBLEMA

Configurar una red interna LAN que requiere contar con varios protocolos y servicios como DHCP, NAT, NTP, VTP, HTTP además de la creación de VLANs para dividir el tráfico, zonas de acceso, y una salida a un servicio de INTERNET. Actualmente se cuenta con la topología definida y suministrada en el curso sin embargo no se tiene aún la configuración y la simulación realizada.

III. JUSTIFICACIÓN

Las habilidades en el conocimiento de redes por parte de los profesionales en las áreas de sistemas/eléctrica/electrónica y telecomunicaciones es de gran importancia para la época actual. La generación, transmisión, distribución y consumo de datos de informacion actualmente es un pilar fundamental para nuestra civilización es por eso por lo que el conocimiento de tecnologías en Internet-networking será fundamental para el progreso económico y tecnológico del país. En este caso en concreto se escogió este escenario simulado para dar solución a la interconexión de esta red, ya que es un ejemplo muy claro de un montaje real de red interna y su interconexión con redes externas y salidas a Internet. En este escenario se aplicaron las técnicas aprendidas en el curso y da pie para seguir aplicando este tipo de tecnologías para la interconexión de sistemas IoT en el futuro.

IV. OBJETIVO GENERAL

Demostrar los conocimientos adquiridos en el diplomado CISCO, mediante las soluciones simuladas de conectividad en redes, en escenarios propuestos por el diplomado de profundización.

A. Objetivos específicos

1. Simular el funcionamiento y la configuración de la red, con la ayuda del software CISCO Packet Tracer®.
2. Brindar interconexión y servicio a salida a redes externas a los participantes de los escenarios propuestos utilizando cableados y equipos de la forma más eficiente posible.
3. Configurar las redes para que el mantenimiento y puesta en marcha de estas, se utilice en el menor tiempo posible y con los recursos adecuados.
4. Configurar las redes de los escenarios propuestos de la forma más segura posible.
5. Proteger la red contra intrusos y accesos no autorizados desde el interior y exterior de la red.

V. METODOLOGIA

La metodología para el desarrollo de este caso está basada en un reporte técnico con la ayuda del software Packet Tracer®. Las etapas realizadas fueron las siguientes

A. Instalación software packet tracer

El instalador del software PACKET TRACER fue descargado desde la página del curso e instalado en un computador portátil Lenovo ideapad, procesador I5 64 bits, 8 G de memoria RAM y disco duro de 1 TB, con sistema operativo Windows 10.

B. Configuración de la topología propuesta en el software packet tracer.

La topología propuesta por parte del curso fue la siguiente

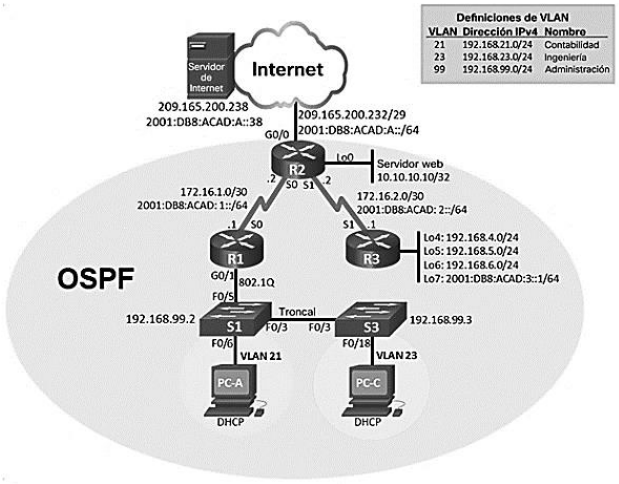


Ilustración 1. Topología de red propuesta

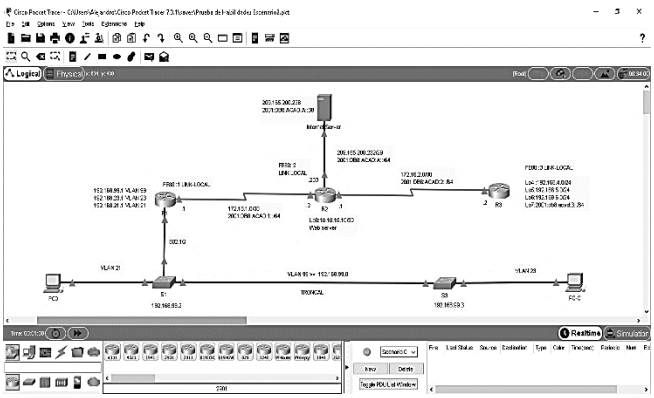


Ilustración 2. Topología instalada en packet tracer.

C. Configuración de equipos

Cada uno de los Hosts de la red fue configurado con cada protocolo de comunicación propuesto, siguiendo los lineamientos propuestos en el curso.

D. Presentación de resultados por medio de prueba de conexión.

Al terminar la configuración de los hosts, se realizó una prueba de conexión entre host, con el fin de verificar su correcto funcionamientos para cada uno delos protocolos propuestos.

VI. CONFIGURACION Y DESARROLLO

Escenario: 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.

A. Iniciar dispositivos

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. Configurar los parámetros básicos de los dispositivos, configurar el servidor de Internet. Las tareas de configuración del servidor de Internet incluyen lo siguiente (para obtener información de las direcciones IP, consulte la topología):

Tabla 1

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
Gateway predeterminado IPv6	2001:DB8:ACAD:A::1

B. configuración R1, R2 y R3

Las tareas de configuración para R1 también son las mismas para R2 y R3, las cuales son :

Desactivar la búsqueda DNS, Nombre del router ,dar seguridad al router mediante encriptación de claves, restringir la conexión a personal no autorizado. [1]

Elemento o tarea de configuración	**Especificación**
Interfaz S0/1/0	Rx(config)#int s0/1/0 R1(config-if)#description "Conexión a R2" R1(config-if)#ip address 172.16.1.1 255.255.255.252 R1(config-if)#ipv6 address 2001:db8:acad:1::1/64 Rx(config-if)#clock rate 128000 Rx(config-if)#no shutdown
Rutas predeterminadas	R1(config)#ip route 0.0.0.0 0.0.0.0 s0/1/0 R1(config)#ipv6 route ::/0 s0/1/0
Interfaz S0/1/0	R2(config)#int s0/1/0 R2(config-if)#description "conexión a R1" R2(config-if)#ip address 172.16.1.2 255.255.255.252 R2(config-if)#ipv6 address 2001:db8:acad:1::2/64 R2(config-if)#no shutdown
Interfaz S0/1/1	R2(config-if)#int s0/1/1 R2(config-if)#description "conexión a R3" R2(config-if)#ip address 172.16.2.1 255.255.255.252 R2(config-if)#ipv6 address 2001:db8:acad:2::1/64 R2(config-if)#clock rate 128000 R2(config-if)#no shutdown

Interfaz G0/0 (simulación de Internet)	R2(config)#int g0/0 R2(config-if)#description " conexión a Internet" R2(config-if)#ip address 209.165.200.233 255.255.255.248 R2(config-if)#ipv6 address 2001:db8:acad:a::1/64 Activar la interfaz R2(config-if)#no shutdown
Interfaz loopback 0 (servidor web simulado)	R2(config)#interface loopback 0 R2(config-if)#description "Servidor Web" R2(config-if)#ip address 10.10.10.10 255.255.255.255
Ruta predeterminada	R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0 R2(config)#ipv6 route ::/0 g0/0
Interfaz loopback 4	R3(config)#int loopback 4 R3(config-if)#ip address 192.168.4.1 255.255.255.0
Interfaz loopback 5	R3(config)#int loopback 5 R3(config-if)#ip address 192.168.5.1 255.255.255.0
Interfaz loopback 6	R3(config)#interface loopback 6 R3(config-if)#ip address 192.168.6.1 255.255.255.0
Interfaz loopback 7	R3(config)#interface loopback 7 R3(config-if)#ipv6 address 2001:db8:acad:3::1/64
Ruta predeterminada	R3(config)#ip route 0.0.0.0 0.0.0.0 s0/1/0 R3(config)#ipv6 route ::/0 s0/1/0

C. Configurar S1 y S3

La configuración del S1 y S3 incluye las siguientes tareas iguales a R1: Desactivar la búsqueda DNS, nombre del router, dar seguridad al router mediante encriptación de claves, restringir la conexión a personal no autorizado. [1].

Verificar la conectividad de la red

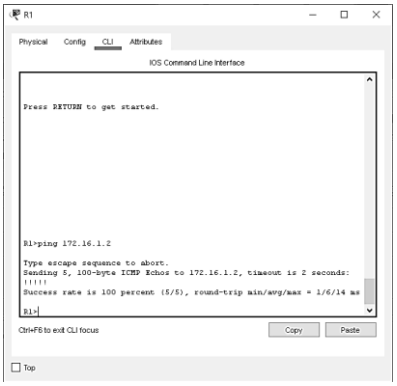


Ilustración 3. Comando ping de conexión de R1 a R2

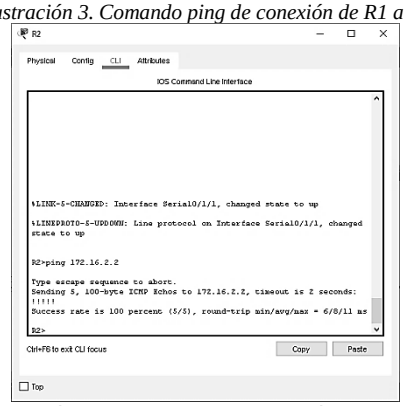


Ilustración 4. Comando ping de conexión de R2 a R3

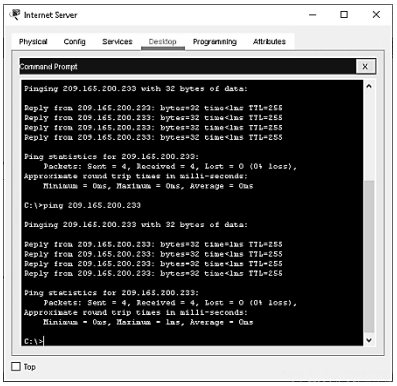


Ilustración 5. Comando ping de conexión de Servidor de Inter

D. Configurar la seguridad del switch, las VLAN y el routing entre VLAN

1. Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 2

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN [2]	S1>en S1#config t S1(config)#vlan 21 S1(config-vlan)#name contabilidad S1(config-vlan)# vlan 23 S1(config-vlan)#name ingeniería S1(config-vlan)#vlan 99 S1(config-vlan)#name administración
Asignar la dirección IP de administración. [2]	S1(config)#int vlan 99 S1(config-if)#ip address 192.168.99.2 255.255.255.0
Asignar el gateway predeterminado [2]	S1(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3 [2]	S1(config)#int f0/3 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1
Forzar el enlace troncal en la interfaz F0/5 [2]	S1(config)#int f0/5 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1 S1(config-if)#no shutdown
Configurar el resto de los puertos como puertos de acceso [1]	Utilizar el comando interface range S1(config)#int range f0/1-2, f0/4, f0/6-24, g0/1-2 S1(config-if-range)#switchport mode access
Asignar F0/6 a la VLAN 21 [2]	S1(config-if-range)#int f0/6 S1(config-if)#switchport access vlan 21
Apagar todos los puertos sin usar [1]	S1(config-if)#int range f0/1-2, f0/4, f0/7-24, g0/1-2 S1(config-if-range)#shutdown

2. Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 3

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN [2]	S3>en S3#config t S3(config)#vlan 21 S3(config-vlan)#name contabilidad S3(config-vlan)#vlan 23 S3(config-vlan)#name ingeniería S3(config-vlan)#vlan 99 S3(config-vlan)#name administración
Asignar la dirección IP de administración [2]	S3(config)#int vlan 99 S3(config-if)#ip address 192.168.99.3 255.255.255.0 S3(config-if)#no shutdown
Asignar el gateway predeterminado. [2]	S3(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3 [2]	S3(config)#int f0/3 S3(config-if)#switchport mode trunk S3(config-if)#switchport trunk native vlan 1 S3(config-if)#
Configurar el resto de los puertos como puertos de acceso [1]	S3(config)#int range f0/1-2, f0/4-24, g0/1-2 S3(config-if-range)#switchport mode access
Asignar F0/18 a la VLAN 23 [2]	S3(config)#int f0/18 S3(config-if)#switchport access vlan 23
Apagar todos los puertos sin usar [1]	S3(config)#int range f0/1-2, f0/4-17,f0/19-24, g0/1-2 S3(config-if-range)#shutdownn

3. Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 4

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1 [3]	R1(config)#int g0/1.21 R1(config-subif)#description LAN de contabilidad R1(config-subif)#encapsulation dot1q 21 R1(config-subif)#ip address 192.168.21.1 255.255.255.0
Configurar la subinterfaz 802.1Q .23 en G0/1 [3]	R1(config)#int g0/1.23 R1(config-subif)#description LAN de Ingenieria R1(config-subif)#encapsulation dot1q 23 R1(config-subif)#ip address 192.168.23.1 255.255.255.0
Configurar la subinterfaz 802.1Q .99 en G0/1 [3]	R1(config)#int g0/1.99 R1(config-subif)#description LAN de administración R1(config-subif)#encapsulation dot1q 99 R1(config-subif)#ip address 192.168.99.1 255.255.255.0
Activar la interfaz G0/1 [1]	R1(config)#int g0/1 R1(config-if)#no shutdown

4. Verificar la conectividad de la red

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

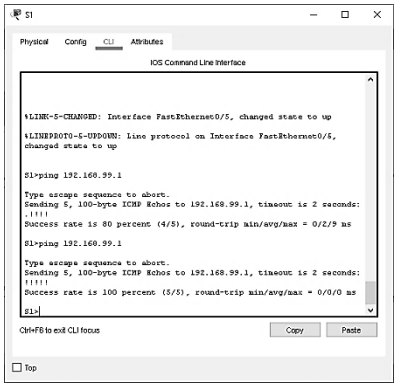


Ilustración 6. Comando ping de conexión de S2 a la puerta de enlace predeterminada de Vlan 99 en R1.

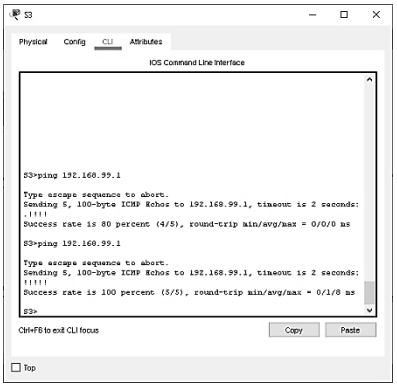


Ilustración 7. Comando ping de conexión de S3 a la puerta de enlace predeterminada de Vlan 99 en R1.

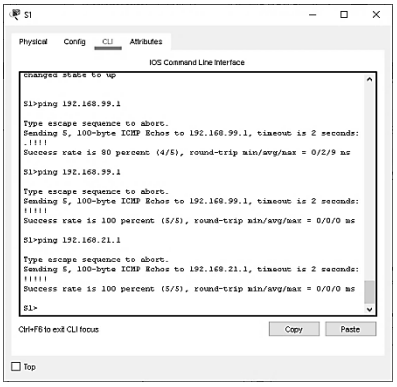


Ilustración 8. Comando ping de conexión de S1 a la puerta de enlace predeterminada de Vlan 21 en R1.

E. Configurar el protocolo de routing dinámico OSPF

1. Configurar OSPF en el R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 5

Elemento o tarea de configuración	**Especificación**
Configurar OSPF área 0 [4]	R1(config)#router ospf 10 R1(config-router)#router-id 1.1.1.1
Anunciar las redes conectadas directamente [5]	R1(config-router)#network 192.168.99.1 0.0.0.0 área 0 R1(config-router)#network 192.168.23.1 0.0.0.0 área 0 R1(config-router)#network 192.168.21.1 0.0.0.0 área 0 R1(config-router)#network 172.16.1.0 0.0.0.3 área 0

Establecer todas las interfaces LAN como pasivas [6]	R1(config-router)#passive-interface g0/1.21 R1(config-router)#passive-interface g0/1.23 R1(config-router)#passive-interface g0/1.99
Desactive la sumarización automática	No aplica en la simulación de Packet tracer

2. Actividad Adicional: configuración OSPFv3 EN R1

Se determinó que se debía configurar el enrutador R1 con el protocolo OSPFv3 ya que, también hay una comunicación en IPV6 por el puerto serie S0/1/0. [7]

```
R1>en
R1#config t
R1(config)#ipv6 unicast-routing
R1(config)#ipv6 router ospf 10
R1(config-rtr)#router-id 1.1.1.1
R1(config-rtr)#exit
R1(config)#int s0/1/0
R1(config-if)#ipv6 address fe80::1 link-local
R1(config-if)#ipv6 ospf 10 area 0
```

3. Configurar OSPF en el R2

La configuración del R2 incluye las siguientes tareas:

Tabla 6

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0 [4]	R2#config t R2(config)#router ospf 10 R2(config-router)#router-id 2.2.2.2
Anunciar las redes conectadas directamente [5] Nota: Omitir la red G0/0.	R2(config-router)#network 172.16.1.0 0.0.0.3 area 0 R2(config-router)#network 172.16.2.0 0.0.0.3 area 0 R2(config-router)#network 10.10.10.10 0.0.0.0 area 0
Establecer la interfaz LAN (loopback) como pasiva [6]	R2(config-router)#passive-interface loopback 0
Desactive la sumarización automática.	No aplica en la simulación de Packet tracer

4. Configurar OSPFv3 en el R2

La configuración del R2 incluye las siguientes tareas:

Tabla 7

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0 [7]	R2(config)#ipv6 unicast-routing R2(config)#int g0/0 R2(config-if)#ipv6 address fe80::2 link-local R2(config-if)#int s0/1/0 R2(config-if)#ipv6 address fe80::2 link-local R2(config-if)#int s0/1/1 R2(config-if)#ipv6 address fe80::2 link-local R2(config)#ipv6 router ospf 10 R2(config-rtr)#router-id 2.2.2.2 R2(config-rtr)#auto-cost reference-bandwidth 1000
Anunciar redes IPv6 conectadas directamente [7]	R2(config)#interface g0/0 R2(config-if)#ipv6 ospf 10 area 0 R2(config-if)#int s0/1/0 R2(config-if)#ipv6 ospf 10 area 0 R2(config-if)#int s0/1/1 R2(config-if)#ipv6 ospf 10 area 0
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas [6] [8]	R2(config-router)#passive-interface loopback 0
Desactive la sumarización automática.	No aplica en la simulación de Packet tracer

5. 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 8

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? [8]	R1#show ip protocols
¿Qué comando muestra solo las rutas OSPF? [8]	R1#show ip route ospf

¿Qué comando muestra la sección de OSPF de la configuración en ejecución? [1]	R1#show running-config | section router ospf
¿Con qué comando se muestran la ID del proceso OSPFv3, la ID del router, las redes de routing y las interfaces pasivas configuradas en un router? [9]	R1#show ipv6 protocols R1#show ipv6 ospf
¿Qué comando muestra solo las rutas OSPFv3? [10]	R1#show ipv6 route ospf
¿Qué comando muestra la sección de OSPF de la configuración en ejecución? [1]	R1#show running-config | section router ospf

F. Implementar DHCP y NAT para IPv4

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

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 9

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.21
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.21
Crear un pool de DHCP para la VLAN 21.	R1(config)#ip dhcp pool ACCT R1(dhcp-config)#network 192.168.21.0 255.255.255.0 R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com R1(dhcp-config)#default-router 192.168.21.1
Crear un pool de DHCP para la VLAN 23	R1(config)#ip dhcp pool ENGNR R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com R1(dhcp-config)#default-router 192.168.23.1

2. Configurar la NAT estática y dinámica en el R2

La configuración del R2 incluye las siguientes tareas:

Tabla 10

Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario [1]	R2(config)#username webuser privilege 15 secret cisco12345
Habilitar el servicio del servidor HTTP	No aplica el packet tracer
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	No aplica en el packet tracer
Crear una NAT estática al servidor web. [11]	R2(config)# ip nat inside source static 10.10.10.10 209.165.200.229
Asignar la interfaz interna y externa para la NAT estática [11]	R2(config)#int lo 0 R2(config-if)#ip nat outside R2(config-if)#exit R2(config)#int s0/1/0 R2(config-if)#ip nat inside R2(config-if)#exit

Configurar la NAT dinámica dentro de una ACL privada [12]	R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.4.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.5.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.6.0 0.0.0.255 R2(config)#int s0/1/1 R2(config-if)#ip nat inside
Defina el pool de direcciones IP públicas utilizables. [12]	R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.248
Definir la traducción de NAT dinámica [12]	R2(config)#ip nat inside source list 1 pool INTERNET R2(config)#int g0/0 R2(config-if)#ip nat outside

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.

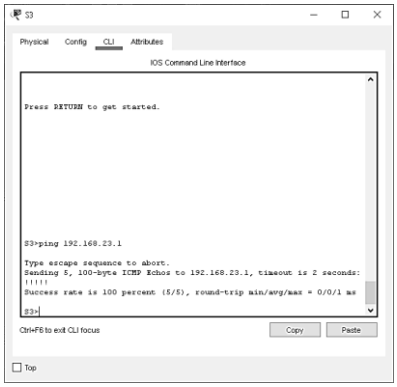


Ilustración 9. Comando ping de conexión de S3 a la puerta de enlace predeterminada de Vlan 23 en R1.Configurar NTP

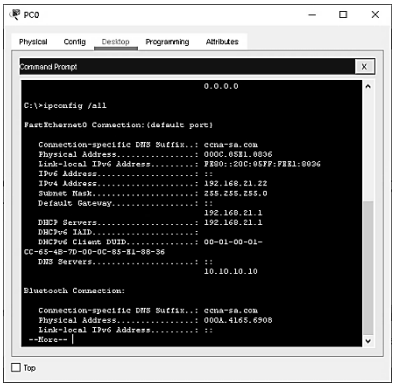


Ilustración 10. Configuración Ethernet de PC0, incluye la comunicación desde el server DHCP de la red.

Tabla 11

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2. [13]	R2#clock set 9:00:00 5 march 2016
Configure R2 como un maestro NTP. [14]	R2(config)#ntp master 5
Configurar R1 como un cliente NTP. [14]	Servidor: R2 R1(config)#ntp server 172.16.1.2
Configure R1 para actualizaciones de calendario periódicas con hora NTP. [15]	R1(config)#ntp update-calendar
Verifique la configuración de NTP en R1. [16]	R1#show ntp status

4. Configurar y verificar las listas de control de acceso (ACL)

5. Restringir el acceso a las líneas VTY en el R2

Tabla 12

Elemento o tarea de configuración	Especificación
Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2. [17]	R2(config)#ip access-list standard ADMIN-MGT R2(config-std-nacl)#permit host 172.16.1.1
Aplicar la ACL con nombre a las líneas VTY [18]	R2(config)#line vty 0 15 R2(config-line)#access-class ADMIN-MGT in
Permitir acceso por Telnet a las líneas de VTY [18]	R2(config-line)#transport input telnet

Verificar que la ACL funcione como se espera [18]	R1>en R1#telnet 172.16.1.2 R3>en R3#telnet 172.16.1.2

6. 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 [18]	R2#show access-lists
Restablecer los contadores de una lista de acceso [18]	R2#clear access-list counters
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica? [18]	R2#show ip interface ***ID interface***

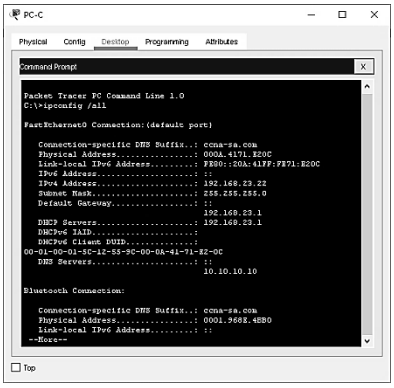


Ilustración 11. Configuración Ethernet de PC_C, incluye la comunicación desde el server DHCP de la red.

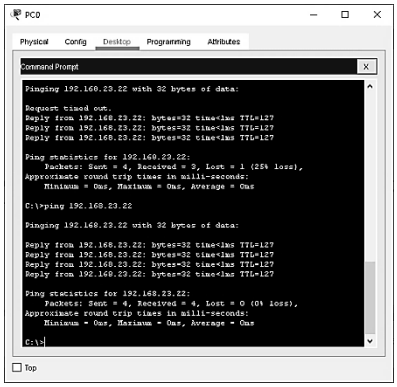


Ilustración 12. Comando Ping de PC_0 a PC_C

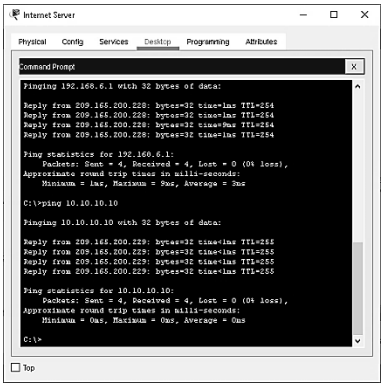


Ilustración 13. Comando ping desde el servidor de internet al servidor web interno (10.10.10.10), mediante NAT estático.

VII. CONCLUSIONES

A. Packet tracer nos ayuda simular el funcionamiento de cualquier topología de red, ayudando a minimizar los tiempos de instalación y puesta en marcha del sistema.

B. Los enlaces VLAN permiten la comunicación entre switches y nos ayuda a disminuir el cableado y hardware para la intercomunicación entre redes. Por medio de ellas podemos separar diferentes redes conectadas físicamente a switches comunes.

C. La encapsulación IEEE 802.1Q nos permite diferenciar diferentes tramas Ethernet asociadas a diferentes VLAN e interconectarlas con una misma comunicación troncal en común.

D. Gracias protocolo DHCP ayuda a los administradores de red a suministrar direcciones IP automáticamente a los Host de la red, reduciendo el tiempo de mantenimiento y puesta a punto de la red.

E. Las listas de control de acceso (ACL), nos ayudan controlar el tráfico de paquetes en la red, mejorando la seguridad dentro y fuera de esta.

F. Las NAT ayuda a mitigar el agotamiento de las direcciones IPv4 públicas, ayuda a la seguridad de la red, enmascarando y ocultando la informacion física de un host en particular, reduce la carga administrativa.

VIII. REFERENCIAS

[1] «tecnología y redes,» 16 Noviembre 2014. [En línea]. Available: http://tecnologiayredes.tyrdomains.com/node/16.

[2] Cisco networking academy, «Capítulo 5: Enrutamiento entre VLAN,» Instituto Tecnológico Superior del Oriente del Estado de Hidalgo, [En línea]. Available: https://www.itesa.edu.mx/netacad/switching/course/module5/index.html#5.1.3.2.

[3] Cisco networking academy, «Configuración de router-on-a-stick: configuración de subinterfaces del router,» [En línea]. Available: https://www.itesa.edu.mx/netacad/switching/course/module5/index.html#5.1.3.3.

[4] Cisco neetworking academy, «8.2.1.2 Modo de configuración de OSPF del router,» [En línea]. Available: https://www.itesa.edu.mx/netacad/switching/course/module8/index.html#8.2.1.2.

[5] Cisco networking academy, «8.2.2.1 Habilitación de OSPF en las interfaces,» [En línea]. Available: https://www.itesa.edu.mx/netacad/switching/course/module8/index.html#8.2.2.1.

[6] Cisco networking academy, «8.2.2.5 Configuración de interfaces pasivas,» [En línea]. Available: https://www.itesa.edu.mx/netacad/switching/course/module8/index.html#8.2.2.5.

[7] Cisco networking academy, «8.3.2.6 Habilitación de OSPFv3 en las interfaces,» [En línea]. Available: https://www.itesa.edu.mx/netacad/switching/course/module8/index.html#8.3.2.6.

[8] Cisco networking academy, «8.2.4.2 Verificación de la configuración del protocolo OSPF,» [En línea]. Available: https://www.itesa.edu.mx/netacad/switching/course/module8/index.html#8.2.4.2.

[9] «8.3.3.2 Verificación de la configuración del protocolo OSPFv3,» [En línea]. Available: https://www.itesa.edu.mx/netacad/switching/course/module8/index.html#8.3.3.2.

[10] Cisco networking academy, «8.3.3.3 Verificación de las interfaces OSPFv3,» [En línea]. Available: https://www.itesa.edu.mx/netacad/switching/course/module8/index.html#8.3.3.3.

[11] Cisco networking academy, «11.2.1.1 Configuración de NAT estática,» [En línea]. Available: https://www.itesa.edu.mx/netacad/switching/course/module11/index.html#11.2.1.1.

[12] Cisco networking academy, «11.2.2.2 Configuración de NAT dinámica,» [En línea]. Available: https://www.itesa.edu.mx/netacad/switching/course/module11/index.html#11.2.2.2.

[13] Cisco networking academy, «Configuración del reloj del sistema,» [En línea]. Available: https://contenthub.netacad.com/legacy/CCNA/RSE/6.0/es/index.html#10.2.1.1.

[14] Cisco networkig academy, «Funcionamiento de NTP,» [En línea]. Available: https://contenthub.netacad.com/legacy/CCNA/RSE/6.0/es/index.html#10.2.1.2.

[15] Unified compliance framework, «The network element must use two or more NTP servers to synchronize time.,» [En línea]. Available: https://www.stigviewer.com/stig/layer_2_switch_-_cisco/2019-01-09/finding/V-23747#:~:text=The%20ntp%20update%2Dcalendar%20command,to%20an%20authoritative%20time%20server..

[16] Cisco, «Verificación del estado de NTP,» [En línea]. Available: https://www.cisco.com/c/es_mx/support/docs/ios-nx-os-software/ios-software-releases-110/15171-ntpassoc.pdf.

[17] Cisco networking academy, «9.3.2.1 Configurar las ACL extendidas,» [En línea]. Available: https://www.itesa.edu.mx/netacad/switching/course/module9/index.html#9.3.2.1.

[18] R. Diaz, «Prueba de Habilidades Prácticas CCNA,» 2020. [En línea]. Available: https://repository.unad.edu.co/handle/10596/34037.

[19] Cisco Networkig Academy, «Descargar Cisco Packet tracer,» Agosto 2020. [En línea]. Available: https://www.netacad.com/portal/resources/packet-tracer.

BIOGRAFÍA

Alejandro Muñoz Forero Nació en Santafé de Bogotá, en 1977. Recibió grado de técnico profesional en instrumentación industrial y control de procesos SENA en el año 2000. De 2000 a 2006, trabajo como Técnico en programación de PLC y montaje de proyectos electroneumáticos, 2007 a 2010 trabajo como asesor técnico donde asesoró el mantenimiento predictivo y correctivo de motores eléctricos AC y DC, integro sistemas de montaje de variadores de velocidad para motores AC y servo posicionamiento eléctrico. En 2011 ingresó a la escuela de ingeniería electrónica en la UNAD. Actualmente labora como asesor técnico en AMF INGENIERIA y tutor docente en el área de matemáticas. Su conocimiento se enfoca en el área de instrumentación industrial, control y automatización de procesos, su currículo puede ser visto en https://co.linkedin.com/in/amunozforero.