EVALUACIÓN –PRUEBA DE HABILIDADES PRÁCTICAS CCNP

PRESENTADO POR:
FREDY QUINTERO QUINTERO

GRUPO
208014_8

DIPLOMADO DE PROFUNDIZACION CISCO

PRESENTADO A:

ING. GERARDO GRANADOS ACUÑA

UNIVERSIDAD NACIONAL ABIERTA Y ADISTANCIA
BOGOTÁ
2018

Contenido

INTRODUCCIÓN

El actual informe comprende el desarrollo del diplomado CCNP, el cual cuenta con temas avanzado sobre instalación, configuración y operación de redes de área local y área amplia. Este diplomado se centra en el desarrollo de las habilidades necesarias la implementación de redes escalables, construction de redes que abarquen un campus, diseñe e instale intranets globales, así como la detección y solución de problemas.

En el siguiente trabajo encontraremos un ejercicio del módulo CCNP ROUTE donde se abordarán conceptos principales como protocolos de enrutamiento EIGRP, OSPF, BGP, redistribución de rutas, entre otros, nuevos e importantes temas, como Dynamic Multi VPN, VRF Lite y protocolos en IPv6. De igual forma un ejercicio del módulo CCNP SWITCH que se aplican y coloca enpractica conceptos principales como operaciones y puertos de swtiches, VLANs y troncales, Spanning Tree, manejo de ataques de spoofing y configuración de usuarios.

OBJETIVOS

Objetivo General

Configurar y administrar dispositivos de Networking orientados al diseño de redes escalables y de conmutación, mediante el estudio del modelo OSI, la arquitectura TCP/IP; establecer niveles de seguridad básicos, mediante la definición de criterios y políticas de seguridad aplicadas a diversos escenarios de red; realizar enrutamiento de Gateway interior y comprender el uso y funcionamieto de VLAN, Protocolo de enlace troncal de VLAN (VTP), Protocolo rápido de árbol de expansión (Rapid Spanning Tree Protocol - RSTP), Protocolo de árbol de expansión por VLAN (Spanning Tree per VLAN - PVSTP) y encpasulamiento por 802.1q.

Objetivos específicos

- Realizar configuración y administracion dispositivos de Networking
- Fortalecer la importancia de establecer niveles de seguridad básicos,
- Desarrollar y verificar operaciones básicas de enrutamiento de Gateway
- Diseñar redes escalables mediante el uso del modelo jerárquico de tres niveles.

EVALUACIÓN –PRUEBA DE HABILIDADES PRÁCTICAS CCNP

Descripción general de la prueba de habilidades.

La evaluación denominada “Prueba de habilidades prácticas”, forma parte de las actividades evaluativas del Diplomado de Profundización CCNP, la cual busca identificar el grado de desarrollo de competencias y habilidades que fueron adquiridas a lo largo del diplomado y a través de la cual se pondrá a prueba los niveles de comprensión y solución de problemas relacionados con diversos aspectos de Networking.

Para esta actividad, el estudiante dispone de cerca de dos semanas para realizar las tareas asignadas en cada uno de los escenarios propuestos, acompañado de los respectivos procesos de documentación de la solución, correspondientes al registro de la configuración de cada uno de los dispositivos, la descripción detallada del paso a paso de cada una de las etapas realizadas durante su desarrollo, el registro de los procesos de verificación de conectividad mediante el uso de comandos ping, traceroute, show ip route, entre otros.

Teniendo en cuenta que la Prueba de habilidades está conformada por dos escenarios, el estudiante deberá realizar el proceso de configuración de un escenario en el Laboratorio SmartLab y el otro mediante el uso de herramientas de Simulación (Puede ser Packet Tracer o GNS3). El estudiante es libre de escoger bajo qué mediación tecnológica resolverá cada escenario.

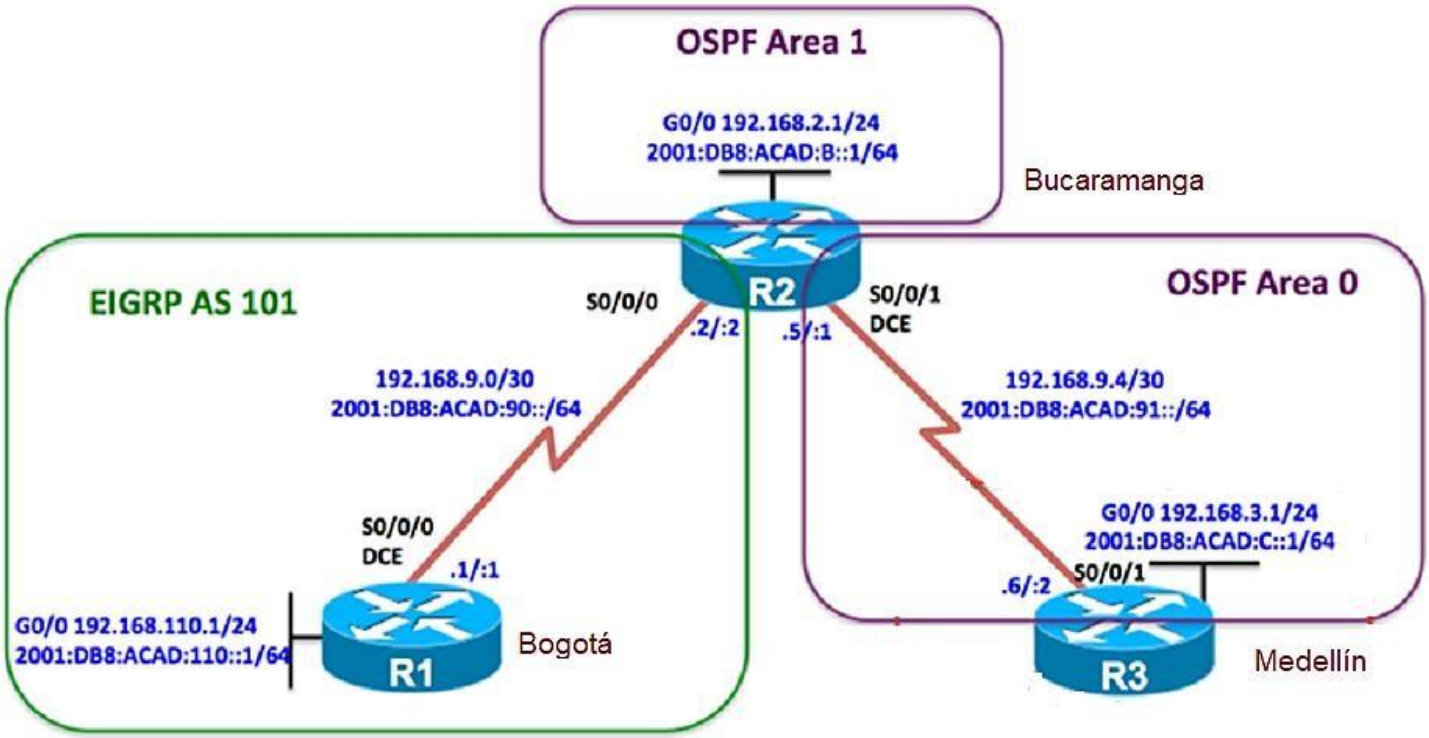
Finalmente, el informe deberá cumplir con las normas ICONTEC para la presentación de trabajos escritos, teniendo en cuenta que este documento deberá ser entregado al final del curso en el Repositorio Institucional, acorde con los lineamientos institucionales para grado. Proceso que les será socializado al finalizar el curso.

Es muy importante mencionar que esta actividad es de carácter INDIVIDUAL. El informe deberá estar acompañado de las respectivas evidencias de configuración de los dispositivos, las cuales generarán veracidad al trabajo realizado. El informe deberá ser entregado en el espacio creado para tal fin en el Campus Virtual de la UNAD.

Descripción de escenarios propuestos para la prueba de habilidades

Escenario 1: Una empresa de confecciones posee tres sucursales distribuidas en las ciudades de Bogotá, Medellín y Bucaramanga, en donde el estudiante será el administrador de la red, el cual deberá configurar e interconectar entre sí cada uno de los dispositivos que forman parte del escenario, acorde con los lineamientos

Establecidos para el direccionamiento IP, protocolos de enrutamiento y demás aspectos que forman parte de la topología de red.
Topología de red



Configurar la topología de red, de acuerdo con las siguientes especificaciones.

Parte 1: Configuración del escenario propuesto

1. Configurar las interfaces con las direcciones IPv4 e IPv6 que se muestran en la topología de red.
2. Ajustar el ancho de banda a 128 kbps sobre cada uno de los enlaces seriales ubicados en R1, R2, y R3 y ajustar la velocidad de reloj de las conexiones de DCE según sea apropiado.
3. En R2 y R3 configurar las familias de direcciones OSPFv3 para IPv4 e IPv6. Utilice el identificador de enrutamiento 2.2.2.2 en R2 y 3.3.3.3 en R3 para ambas familias de direcciones.

4. En R2, configurar la interfaz F0/0 en el área 1 de OSPF y la conexión serial entre R2 y R3 en OSPF área 0.
5. En R3, configurar la interfaz F0/0 y la conexión serial entre R2 y R3 en OSPF área 0.
6. Configurar el área 1 como un área totalmente Stubby.
7. Propagar rutas por defecto de IPv4 y IPv6 en R3 al interior del dominio OSPFv3. Nota: Es importante tener en cuenta que una ruta por defecto es diferente a la definición de rutas estáticas.
8. Realizar la configuración del protocolo EIGRP para IPv4 como IPv6. Configurar la interfaz F0/0 de R1 y la conexión entre R1 y R2 para EIGRP con el sistema autónomo 101. Asegúrese de que el resumen automático está desactivado.
9. Configurar las interfaces pasivas para EIGRP según sea apropiado.
10. En R2, configurar la redistribución mutua entre OSPF y EIGRP para IPv4 e IPv6. Asignar métricas apropiadas cuando sea necesario.
11. En R2, de hacer publicidad de la ruta 192.168.3.0/24 a R1 mediante una lista de distribución y ACL.

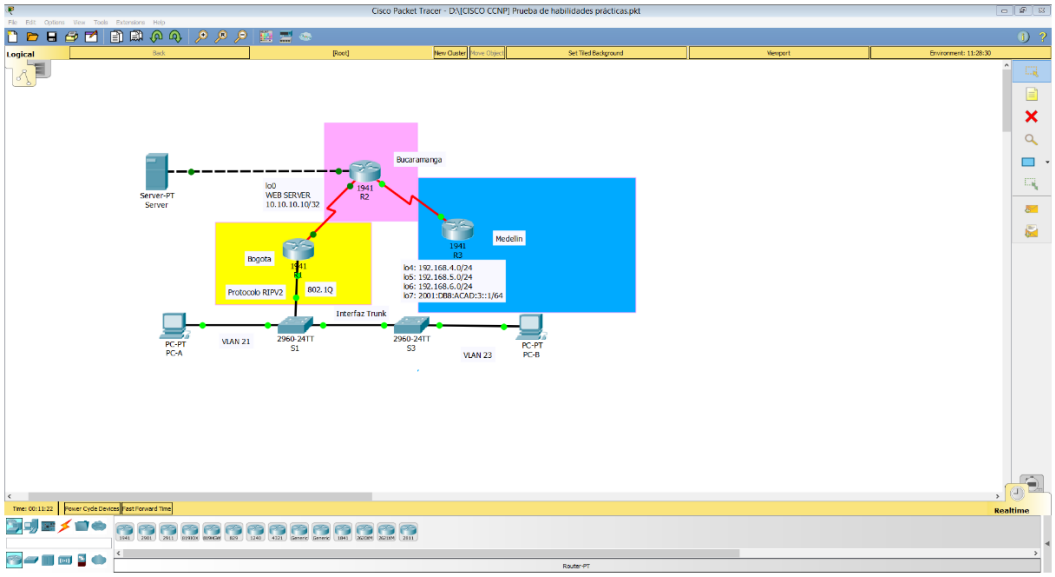
Parte 2: Verificar conectividad de red y control de la trayectoria.

a. Registrar las tablas de enrutamiento en cada uno de los routers, acorde con los parámetros de configuración establecidos en el escenario propuesto.
b. Verificar comunicación entre routers mediante el comando ping y traceroute
c. Verificar que las rutas filtradas no están presentes en las tablas de enrutamiento de los routers correctas.

Nota: Puede ser que Una o más direcciones no serán accesibles desde todos los routers después de la configuración final debido a la utilización de listas de distribución para filtrar rutas y el uso de IPv4 e IPv6 en la misma red.

Evidencia escenario 1

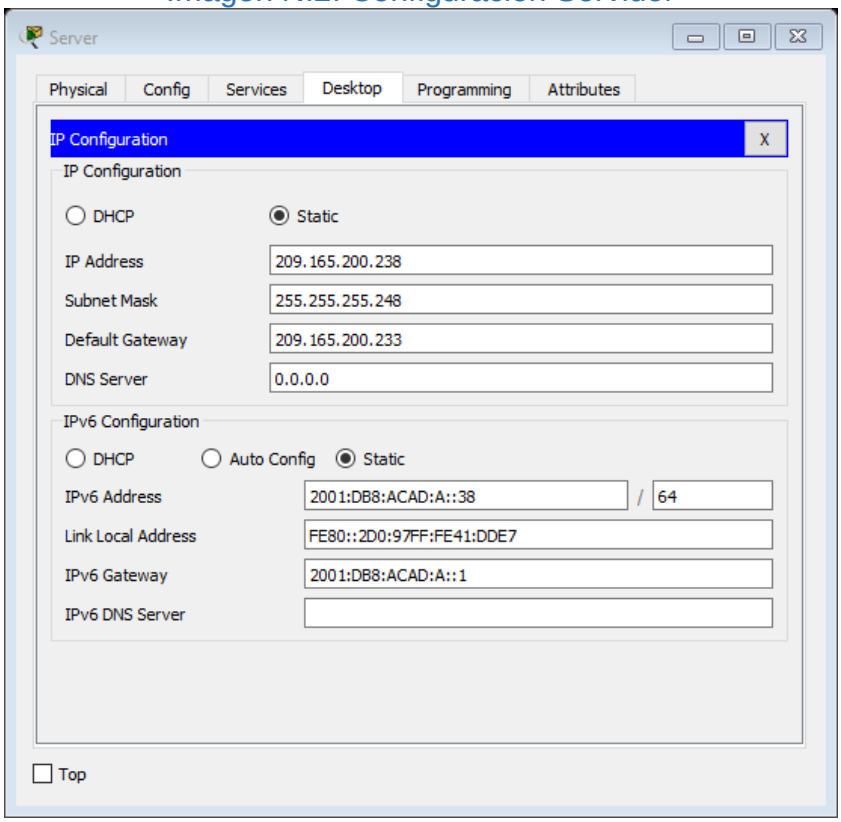
Imagen N.1: Escenario 1



Fuente: Packet Tracer

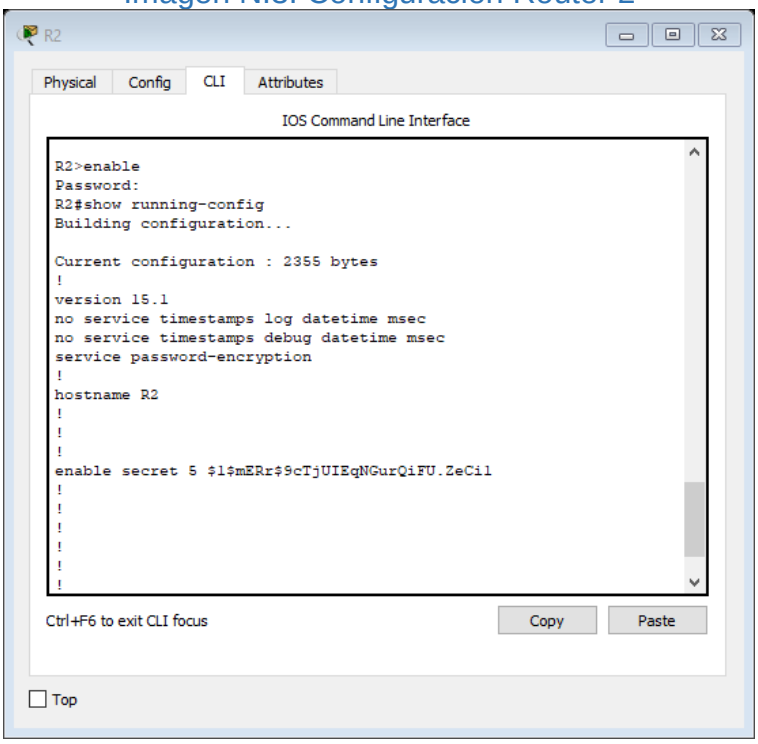
Se realiza la topología y conexión del escenario número 1, se realiza conexión entre los diferentes equipos, como se evidencia en la imagen anterior y de acuerdo a lo solicitado en el escenario.

Imagen N.2: Configuración Servidor



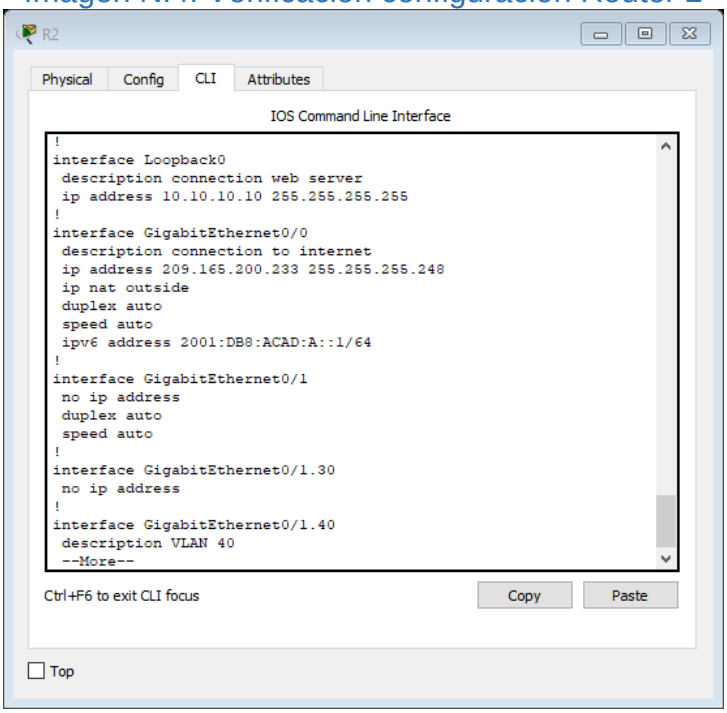
Fuente: Packet Tracer

Imagen N.3: Configuración Router 2



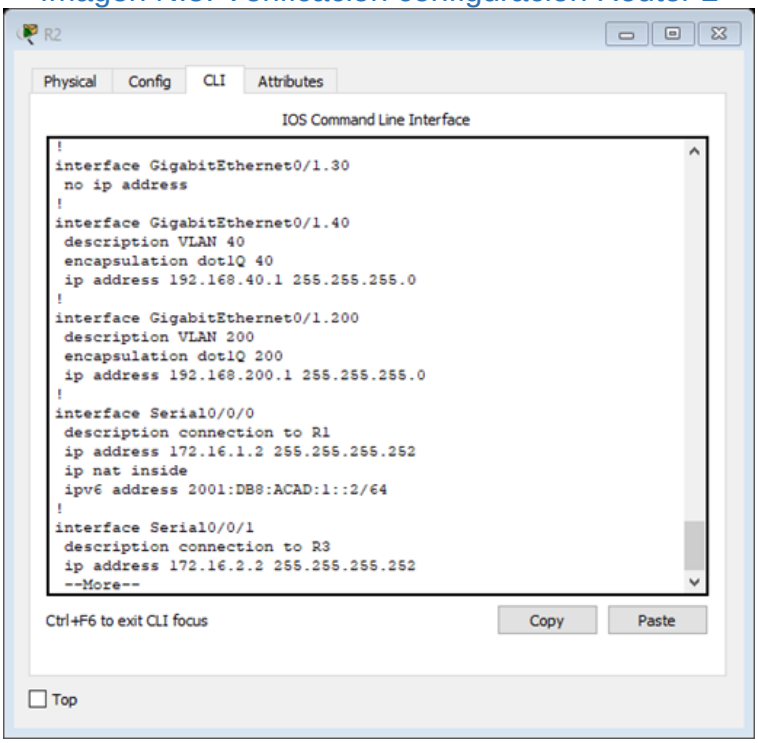
Fuente: Packet Tracer

Imagen N.4: Verificación configuración Router 2



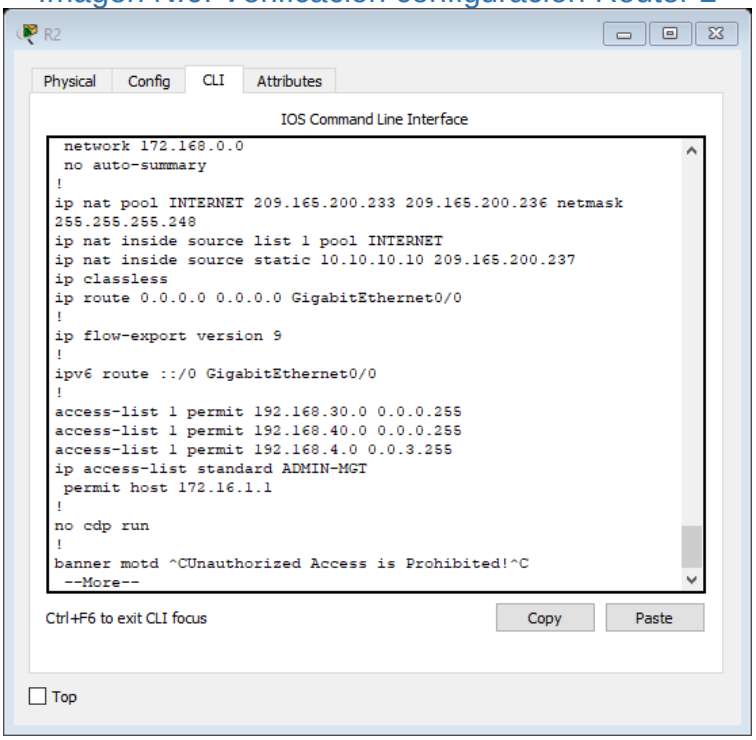
Fuente: Packet Tracer

Imagen N.5: Verificación configuración Router 2



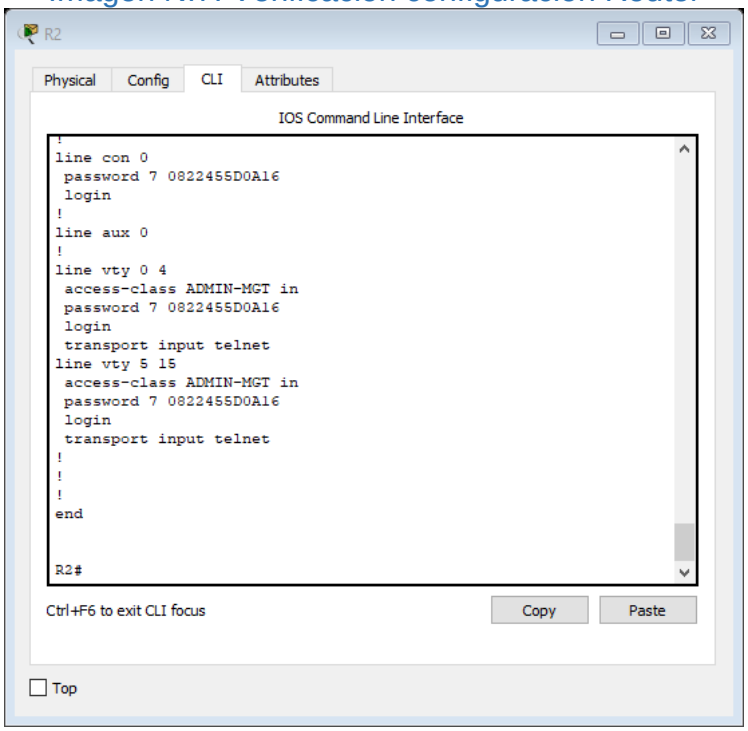
Fuente: Packet Tracer

Imagen N.6: Verificación configuración Router 2



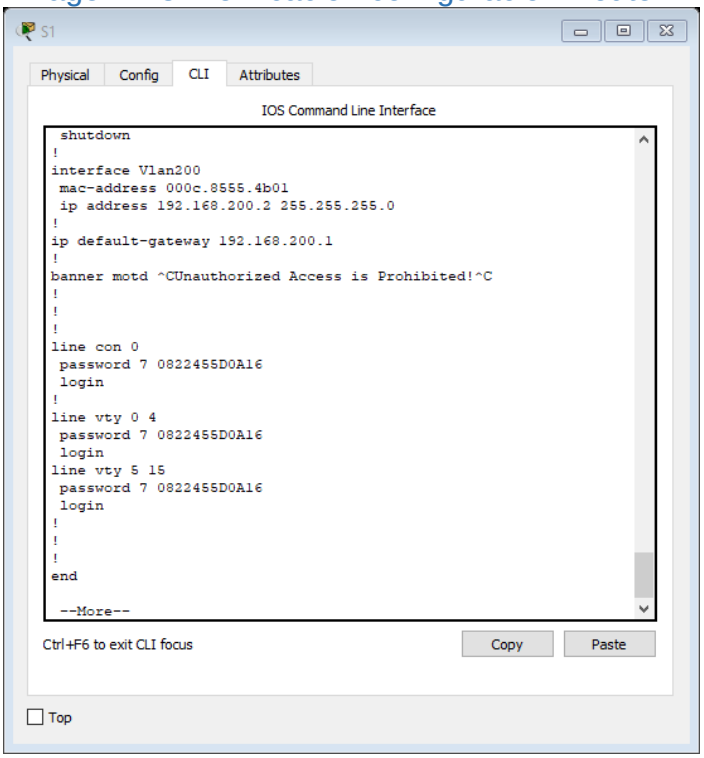
Fuente: Packet Tracer

Imagen N.7: Verificación configuración Router



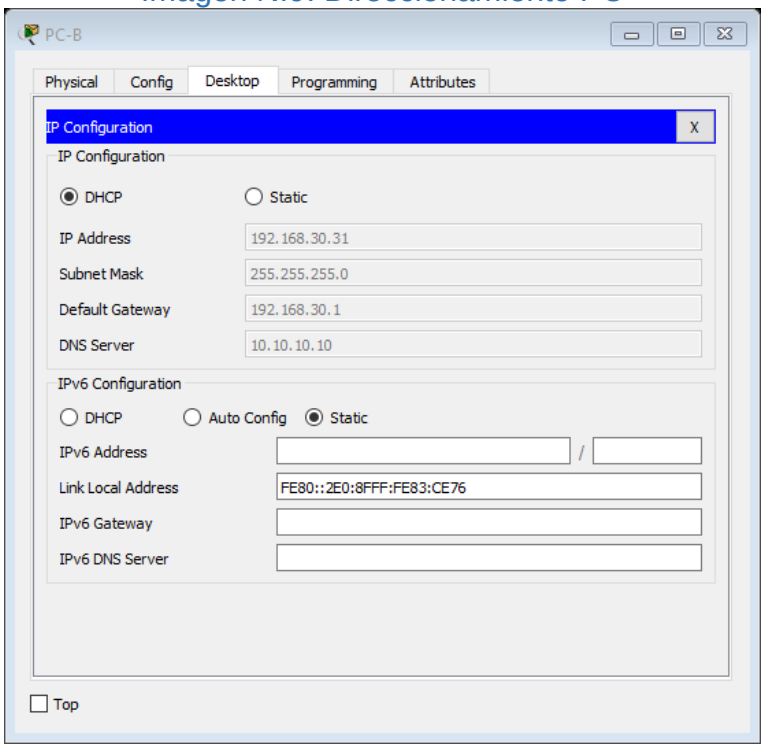
Fuente: Packet Tracer

Imagen N.8: Verificación configuración Router 1



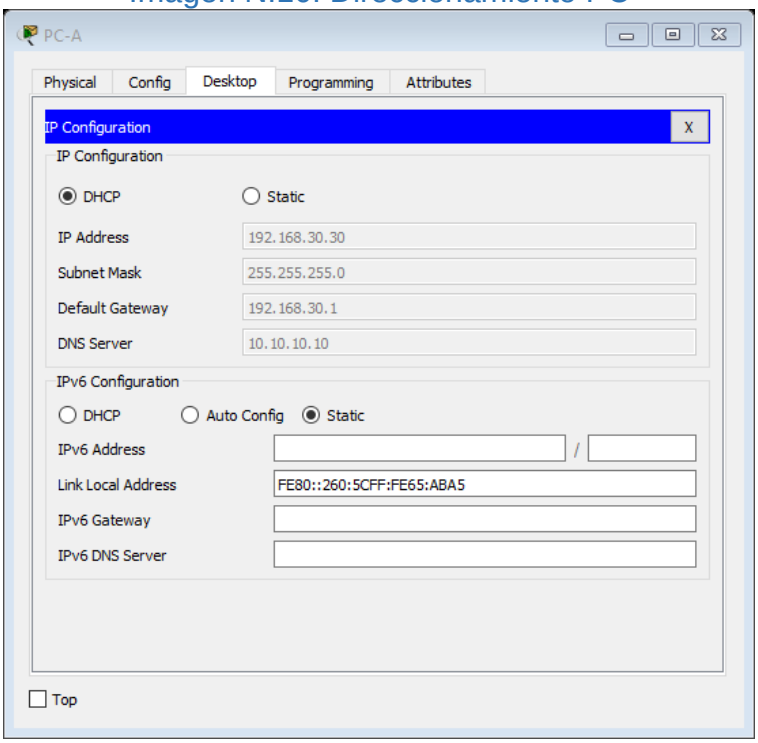
Fuente: Packet Tracer

Imagen N.9: Direccionamiento PC



Fuente: Packet Tracer

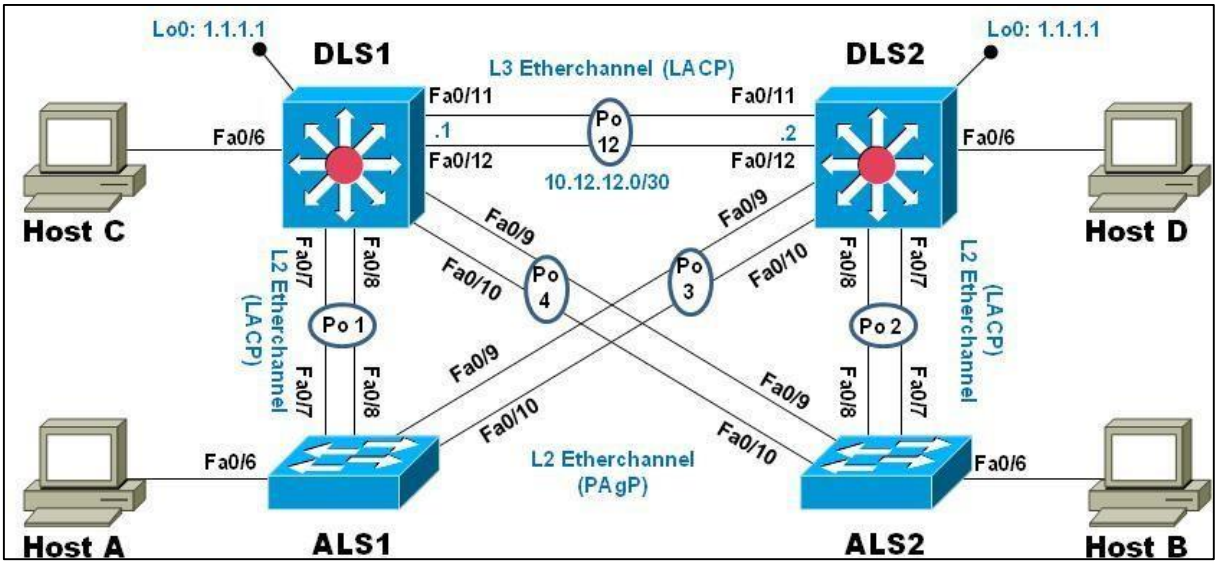
Imagen N.10: Direccionamiento PC



Fuente: Packet Tracer

Escenario 2: Una empresa de comunicaciones presenta una estructura Core acorde a la topología de red, en donde el estudiante será el administrador de la red, el cual deberá configurar e interconectar entre sí cada uno de los dispositivos que forman parte del escenario, acorde con los lineamientos establecidos para el direccionamiento IP, etherchannels, VLANs y demás aspectos que forman parte del escenario propuesto.

Topología de red



Parte 1: Configurar la red de acuerdo con las especificaciones.

a. Apagar todas las interfaces en cada switch.
b. Asignar un nombre a cada switch acorde al escenario establecido.
c. Configurar los puertos troncales y Port-channels tal como se muestra en el diagrama.
    1) La conexión entre DLS1 y DLS2 será un EtherChannel capa-3 utilizando LACP. Para DLS1 se utilizará la dirección IP 10.12.12.1/30 y para DLS2 utilizará 10.12.12.2/30.
    2) Los Port-channels en las interfaces Fa0/7 y Fa0/8 utilizarán LACP.
    3) Los Port-channels en las interfaces F0/9 y fa0/10 utilizará PAgP.
    4) Todos los puertos troncales serán asignados a la VLAN 800 como la VLAN nativa.
d. Configurar DLS1, ALS1, y ALS2 para utilizar VTP versión 3
    1) Utilizar el nombre de dominio UNAD con la contraseña cisco123
    2) Configurar DLS1 como servidor principal para las VLAN.
    3) Configurar ALS1 y ALS2 como clientes VTP.
e. Configurar en el servidor principal las siguientes VLAN:

Número de VLAN	Nombre de VLAN	Número de VLAN	Nombre de VLAN
800	NATIVA	434	ESTACIONAMIENTO
12	EJECUTIVOS	123	MANTENIMIENTO
234	HUESPEDES	1010	VOZ
1111	VIDEONET	3456	ADMINISTRACIÓN

f. En DLS1, suspender la VLAN 434.
g. Configurar DLS2 en modo VTP transparente VTP utilizando VTP versión 2, y configurar en DLS2 las mismas VLAN que en DLS1.
h. Suspender VLAN 434 en DLS2.
i. En DLS2, crear VLAN 567 con el nombre de CONTABILIDAD. La VLAN de CONTABILIDAD no podrá estar disponible en cualquier otro Switch de la red.
j. Configurar DLS1 como Spanning tree root para las VLAN 1, 12, 434, 800, 1010, 1111 y 3456 y como raíz secundaria para las VLAN 123 y 234.
k. Configurar DLS2 como Spanning tree root para las VLAN 123 y 234 y como una raíz secundaria para las VLAN 12, 434, 800, 1010, 1111 y 3456.
l. Configurar todos los puertos como troncales de tal forma que solamente las VLAN que se han creado se les permitirá circular a través de éstos puertos.
m. Configurar las siguientes interfaces como puertos de acceso, asignados a las VLAN de la siguiente manera:

Interfaz	DLS1	DLS2	ALS1	ALS2
Interfaz Fa0/6	3456	12 , 1010	123, 1010	234
Interfaz Fa0/15	1111	1111	1111	1111
Interfaces F0 /16-18		567		

n. Todas las interfaces que no sean utilizadas o asignadas a alguna VLAN deberán ser apagadas.

o. Configurar SVI en DLS1 y DLS2 como soporte de todas las VLAN y de enrutamiento entre las VLAN. Utilice la siguiente tabla para las asignaciones de subred:

VLAN	Nombre de VLAN	subred	VLAN	Nombre de VLAN	subred
12	EJECUTIVOS	10.0.12.0/24	123	MANTENIMIENTO	10.0.123.0/24
234	HUESPEDES	10.0.234.0/24	1010	VOZ	10.10.10.0/24
1111	VIDEONET	10.11.11.0/24	3456	ADMINISTRACIÓN	10.34.56.0/24

- DLS1 siempre utilizará la dirección .252 y DLS2 siempre utilizará la dirección .253 para las direcciones IPv4.
- La VLAN 567 en DLS2 no podrá ser soportada para enrutamiento.

p. Configurar una interfaz Loopback 0 en DLS1 y DLS2. Esta interfaz será configurada con la dirección IP 1.1.1.1/32 en ambos Switch.

q. Configurar HSRP con interfaz tracking para las VLAN 12, 123, 234, 1010, y 1111
   1) Utilizar HSRP versión 2
   2) Crear dos grupos HSRP, alineando VLAN 12, 1010, 1111, y 3456 para el primer grupo y las VLAN 123 y 234 para el segundo grupo.
   3) DLS1 será el Switch principal de las VLAN 12, 1010, 1111, y 3456 y DLS2 será el Switch principal para las VLAN 123 y 234.
   4) Utilizar la dirección virtual .254 como la dirección de Standby de todas las VLAN

r. Configurar DLS1 como un servidor DHCP para las VLAN 12, 123 y 234
   1) Excluir las direcciones desde .251 hasta .254 en cada subred
   2) Establecer el servidor DNS a 1.1.1.1 para los tres Pool.
   3) Establecer como default-router las direcciones virtuales HSRP para cada VLAN

s. Obtener direcciones IPv4 en los host A, B, y D a través de la configuración por DHCP que fue realizada.

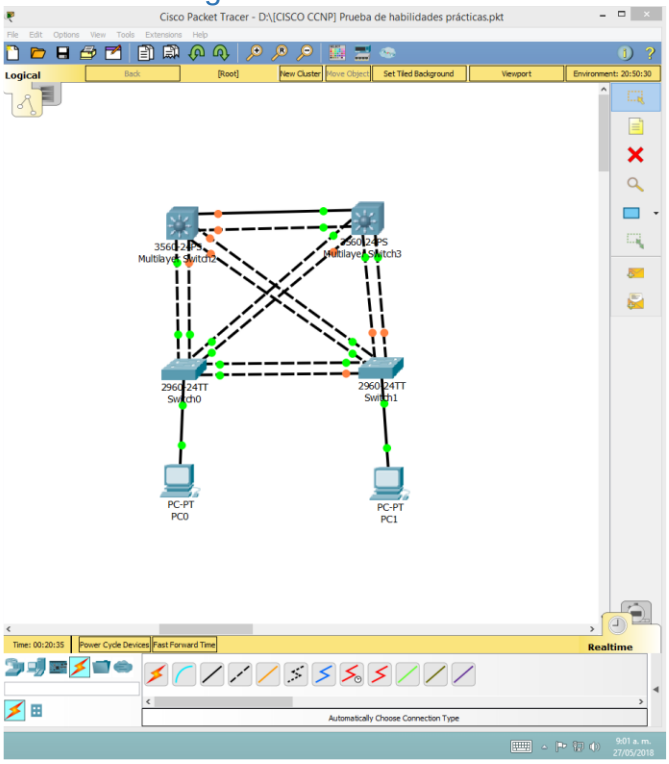
Part 2: conectividad de red de prueba y las opciones configuradas.

a. Verificar la existencia de las VLAN correctas en todos los switches y la asignación de puertos troncales y de acceso

b. Verificar que el EtherChannel entre DLS1 y ALS1 está configurado correctamente
c. Verificar la configuración de Spanning tree entre DLS1 o DLS2 para cada VLAN.
d. Verificar configuraciones HSRP mediante comandos Show

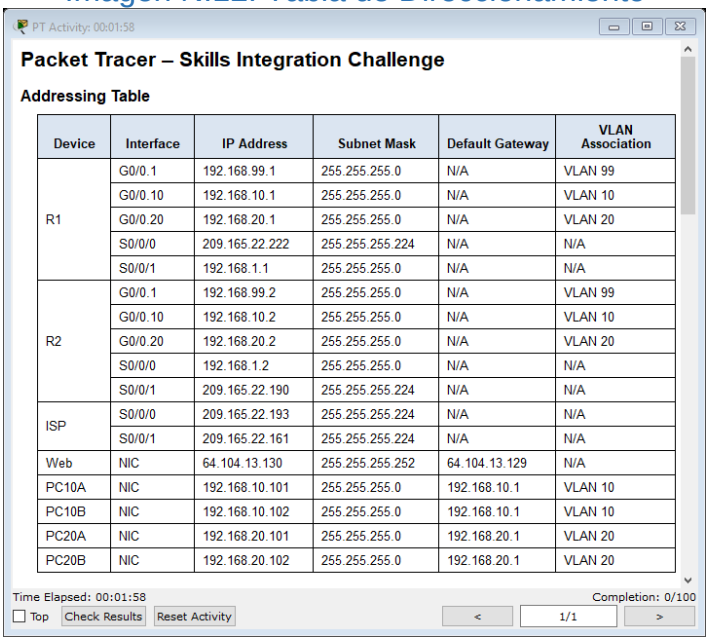
Evidencia escenario 2

Imagen N.11: Escenario 2



Fuente: Packet Tracer

Imagen N.12: Tabla de Direccionamiento



Packet Tracer – Skills Integration Challenge

Addressing Table

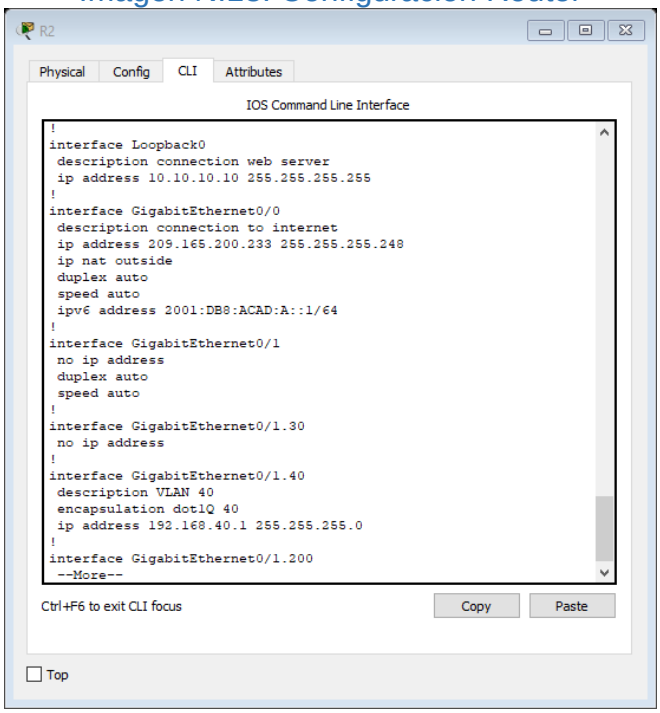
Device	Interface	IP Address	Subnet Mask	Default Gateway	VLAN Association
R1	G0/0.1	192.168.99.1	255.255.255.0	N/A	VLAN 99
	G0/0.10	192.168.10.1	255.255.255.0	N/A	VLAN 10
	G0/0.20	192.168.20.1	255.255.255.0	N/A	VLAN 20
	S0/0/0	209.165.22.222	255.255.255.224	N/A	N/A
	S0/0/1	192.168.1.1	255.255.255.0	N/A	N/A
R2	G0/0.1	192.168.99.2	255.255.255.0	N/A	VLAN 99
	G0/0.10	192.168.10.2	255.255.255.0	N/A	VLAN 10
	G0/0.20	192.168.20.2	255.255.255.0	N/A	VLAN 20
	S0/0/0	192.168.1.2	255.255.255.0	N/A	N/A
	S0/0/1	209.165.22.190	255.255.255.224	N/A	N/A
ISP	S0/0/0	209.165.22.193	255.255.255.224	N/A	N/A
	S0/0/1	209.165.22.161	255.255.255.224	N/A	N/A
Web	NIC	64.104.13.130	255.255.255.252	64.104.13.129	N/A
PC10A	NIC	192.168.10.101	255.255.255.0	192.168.10.1	VLAN 10
PC10B	NIC	192.168.10.102	255.255.255.0	192.168.10.1	VLAN 10
PC20A	NIC	192.168.20.101	255.255.255.0	192.168.20.1	VLAN 20
PC20B	NIC	192.168.20.102	255.255.255.0	192.168.20.1	VLAN 20

Time Elapsed: 00:01:58 Completion: 0/100

Top Check Results Reset Activity < 1/1 >

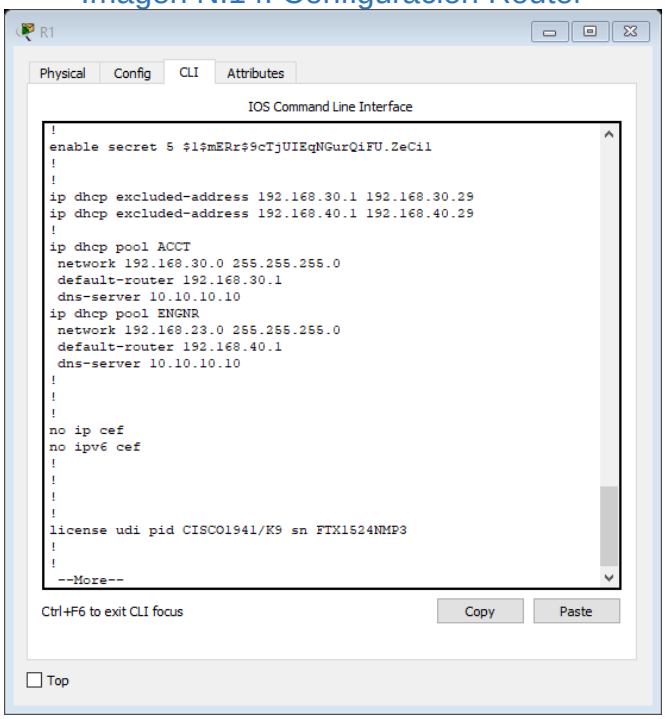
Fuente: Packet Tracer

Imagen N.13: Configuración Router



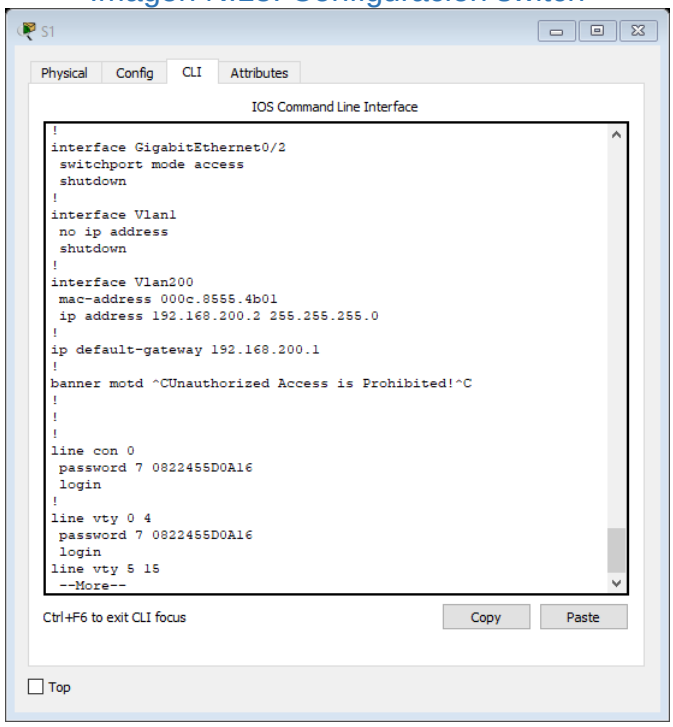
Fuente: Packet Tracer

Imagen N.14: Configuración Router



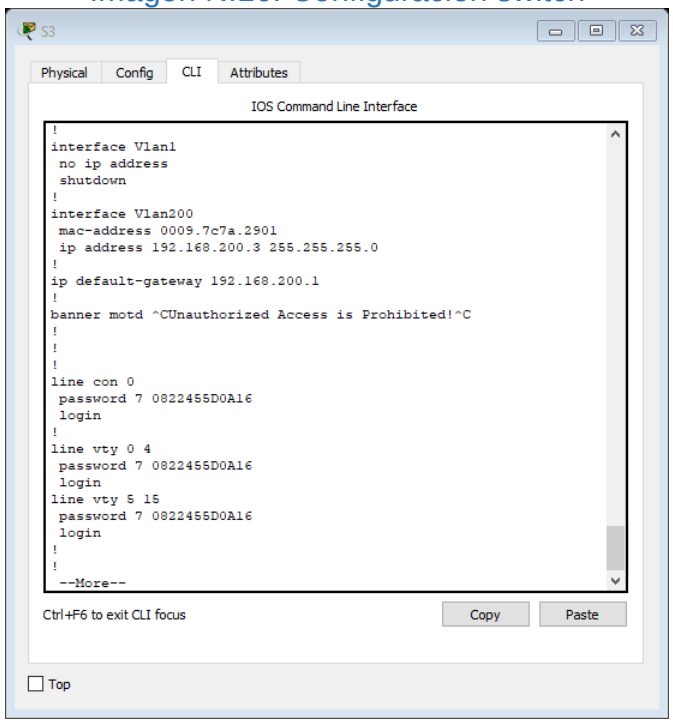
Fuente: Packet Tracer

Imagen N.15: Configuración switch



Fuente: Packet Tracer

Imagen N.16: Configuración switch



Fuente: Packet Tracer

CONCLUSIONES

- la división de las redes planas de Capa 2 en múltiples grupos lógicos de trabajo reduce el tráfico innecesario en la red y potencia el rendimiento, lo cual nos permite mejor rendimiento.

  La administración de aplicación o de proyectos más simples nos permite que las VLAN agregan dispositivos de red y usuarios para admitir los requerimientos geográficos o comerciales.

- La división de una red en las VLAN reduce el número de dispositivos que pueden participar en una tormenta de broadcast.

- las VLAN facilitan el manejo de la red debido a que los usuarios con requerimientos similares de red comparten la misma VLAN. Esto nos lleva a mayor eficiencia del personal de TI.

- Se obtiene reducción de costos; ya que el ahorro en el costo resulta de la poca necesidad de actualizaciones de red caras y usos más eficientes de enlaces y ancho de banda existente.

- Mejora o mayor seguridad a los grupos que tienen datos sensibles se les separa del resto de la red, disminuyendo las posibilidades de que ocurran violaciones de información confidencial.

Referencias

CISCO. (2018). *CCNP Routing and Switching*. Obtenido de https://www.cisco.com/c/en/us/training-events/training-certifications/certifications/professional/ccnp-routing-switching.html

S.C., N. I. (2018). *Fundamentos de IPv6*. Obtenido de http://www.ipv6.mx/index.php/informacion/fundamentos/ipv6