Universidad Continental

Conmutación y enrutamiento

Guía de Trabajo

VISIÓN

Ser la mejor organización de educación superior posible para unir personas e ideas que buscan hacer realidad sueños y aspiraciones de prosperidad en un entorno incierto

MISIÓN

Somos una organización de educación superior que conecta personas e ideas para impulsar la innovación y el bienestar integral a través de una cultura de pensamiento y acción emprendedora.

Presentación

Bienvenido al segundo curso: Conmutación y enrutamiento. Este es el segundo de los tres cursos que están alineados con el examen de certificación CCNA. Contiene 16 capítulos, cada uno con una serie de temas.

Conmutación y enrutamiento mejora su conocimiento del funcionamiento de enrutadores y conmutadores en redes pequeñas. Este curso le presentará los conceptos de redes de área local inalámbricas (WLAN) y seguridad de red.

Al finalizar la asignatura, el estudiante será capaz de configurar router, switches (L2, L3) y APs dando solución a problemas de conmutación y enrutamiento, empleando enrutamiento estático, VLAN, routing entre VLAN, STP, Etherchannel, FHRP, DHCP y WLAN con WLC en redes IPv4 e IPv6

Se les recomienda leer bastante todos los conceptos que se les ofrece a través del material que está en la Academia de Cisco Netacad (www.netacad.com), así como resolución de sus evaluaciones por cada tema. También se les recomienda resolver todas las prácticas haciendo uso de los softwares simuladores de redes "Packet tracer" y GNS3

Giancarlo Condori Torres

ÍNDICE

Primera unidad

Semana 1

Configuración básica de routers Cisco

Sección:	Apellidos : .....
Docente : Giancarlo Condori Torres	Nombres : .....
Unidad : Unidad 1	Fecha: ...../...../..... Duración: 150 min

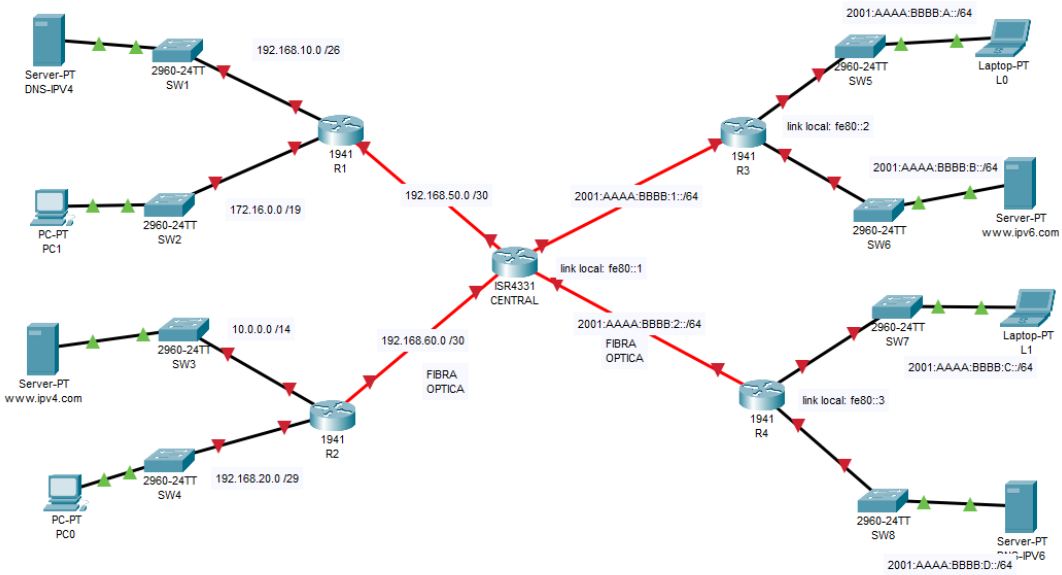
Instrucciones: A continuación de manera colaborativa configure los routers y switches con las siguientes instrucciones.

I. Propósito: El estudiante será capaz de configurar parámetros básicos de routers y switches, así como algunos servicios de red.

II. Descripción de la actividad a realizar (casos)

En esta actividad se va a configurar los routers y switches de manera muy básica con los protocolos IPv4 e IPv6, haciendo uso del software simulador Packet Tracer

III. Procedimientos



Parte 1: Configurar los dispositivos y verificar la conectividad

Configure las direcciones IPv4 e IPv6 en los routers y dispositivos finales

Parte 2: Configurar enrutamiento estático IPv4 e IPv6

Configure rutas estáticas tanto para IPv4 e IPv6, de tal manera que los equipos finales tengan conectividad con otros equipos de otras redes.

Parte 3: Configurar los servidores DNS y WEB

Configure los servidores DNS y WEB, de tal manera que los equipos puedan ingresar a los sitios web propuestos.

Parte 4: Configure el router CENTRAL

a) Asígnele el nombre “CENTRAL”
b) Deshabilite la búsqueda DNS para evitar que el router intente traducir los comandos introducidos de manera incorrecta como si fueran nombres de host.
c) Establezca el requisito de que todas las contraseñas tengan como mínimo 10 caracteres
d) Asigne **conti12345** como la contraseña cifrada del modo EXEC privilegiado.
e) Asigne **conti12345** como la contraseña de consola, establezca un tiempo de espera, habilite el inicio de sesión y agregue el comando **logging synchronous**. El comando **logging synchronous** sincroniza la depuración y el resultado del software IOS de Cisco, y evita que estos mensajes interrumpan la entrada del teclado.
f) Asigne **conti12345** como la contraseña de vty, establezca un tiempo de espera, habilite el inicio de sesión y agregue el comando **logging synchronous.**
g) Cifre las contraseñas de texto no cifrado.
h) Cree un aviso que advierta a todo el que acceda al dispositivo que el acceso no autorizado está prohibido.
i) Documente las 4 interfaces del router.
j) Configure la fecha y la hora actual en el router
k) Guarde la configuración en ejecución en el archivo de configuración de inicio
l) Pruebe el acceso por telnet desde cualquier equipo al router “CENTRAL”

Parte 5: Configure el router CENTRAL para acceso por SSH

a) Configure un dominio conti.com
b) Configure un usuario “juan” con el privilegio más alto una contraseña encriptada “conti12345”
c) Configurar SSH versión 2
d) Generar una encriptación de 1024 bits
e) Dentro de las líneas vty, configurar para que sólo permita el acceso por SSH.
f) Active el usuario local para que permita el acceso con juan y su contraseña.
g) Pruebe el acceso por SSH desde cualquier equipo al router “CENTRAL”, OJO: el intento de poder acceder por telnet debe ser fallido.

Parte 6: Configure interfaces loopback en el router “CENTRAL”

a) Configure la interface loopback 0 con el ip 192.168.100.1 /25
b) Configure la interface loopback 1 con el ip 2001:AAAA:BBBB:3::/64
c) En los demás routers configurar rutas estáticas de tal manera que hagan ping a las dos interfacs looback.

Parte 7: Mostrar información del router “CENTRAL”

a) Use el comando **show version** para responder preguntas sobre el router
    a. ¿Cuál es el nombre de la imagen de IOS que el router está ejecutando?
    b. ¿Cuánta memoria de acceso aleatorio no volátil (NVRAM) tiene el router?
    c. ¿Cuánta memoria flash tiene el router?
b) Mostrar la configuración de inicio
c) Mostrar la tabla de routing tanto para IPv4 e IPv6.

Mostrar una lista de resumen de interfaces para IPv4 e IPv6 del router.

Semana 2

Configuración de rutas estáticas y predeterminadas

Sección: ……..……..	Apellidos : ……..……..
Docente : Giancarlo Condori Torres	Nombres : ……..
Unidad : Unidad 1	Fecha: …../……/…… Duración: 140 min

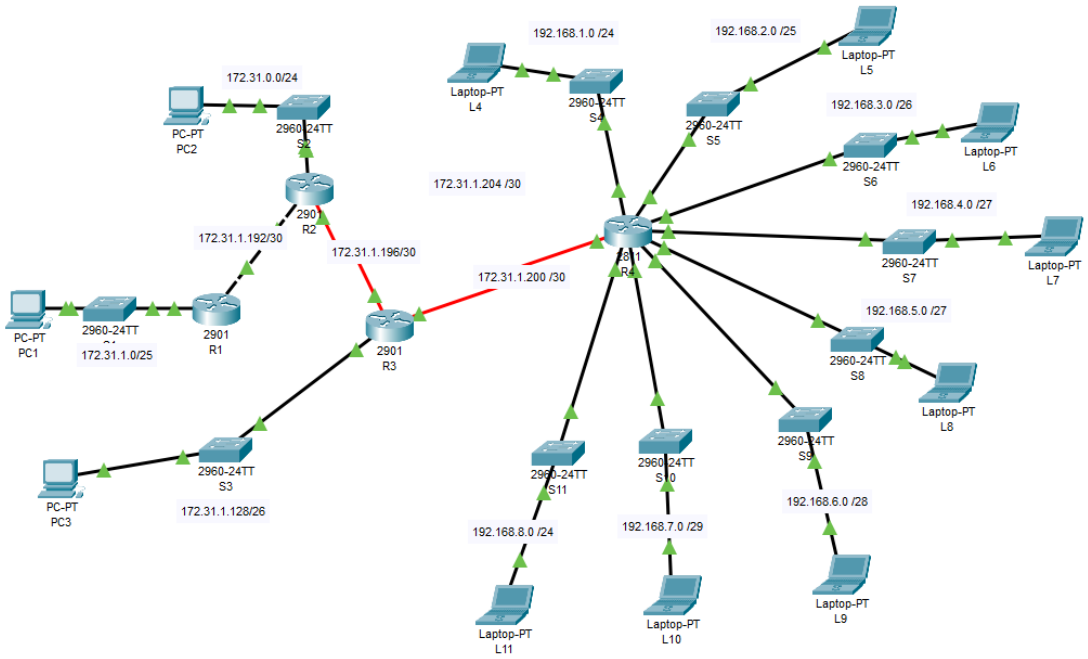
Instrucciones: A continuación de manera colaborativa configure los routers y switches con las siguientes instrucciones.

I. Propósito: El estudiante será capaz de configurar rutas estáticas recursivas, directamente conectadas y predeterminadas haciendo uso de IPv4 e IPv6.

II. Descripción de la actividad a realizar (casos)

En esta actividad configurará rutas estáticas, predeterminadas y resumidas. Una ruta estática es una ruta que el administrador de red introduce manualmente para crear una ruta confiable y segura. En esta actividad, se utilizan cinco rutas estáticas diferentes: una ruta estática recursiva, una ruta estática conectada directamente, una ruta estática completamente especificada, una ruta predeterminada y una ruta resumida.

III. Procedimientos



Parte 1: Configurar de rutas estáticas y predeterminadas

Paso 1: Configurar rutas estáticas recursivas en el R1

a. Configure una ruta estática recursiva a cada red que no esté conectada directamente al R1, incluidos los enlaces WAN entre el R2 y el R3 a excepción de las redes que empiecen con 192….

b. Pruebe la conectividad a la LAN del R2 y haga ping a las direcciones IP de la PC2 y la PC3.

¿Por qué no logró hacerlo?

_____

Paso 2: Configurar rutas estáticas conectadas directamente en el R2

a. Configure una ruta estática conectada directamente del R2 a cada red que no esté conectada directamente a excepción de las redes que empiecen con 192….

Paso 3: Configurar una ruta predeterminada en el R3

a. Configure una ruta predeterminada en el R3 de modo que se pueda llegar a cada red que no esté conectada directamente a excepción de las redes que empiecen con 192….

Parte 2: Verificar la conectividad

Hasta el momento todos los dispositivos de los routers R1, R2 y R3 deberían poder hacerse ping. Si no fuera así, revise la configuración de las rutas estáticas y predeterminadas.

Parte 3: Configurar de rutas predeterminadas y resumidas

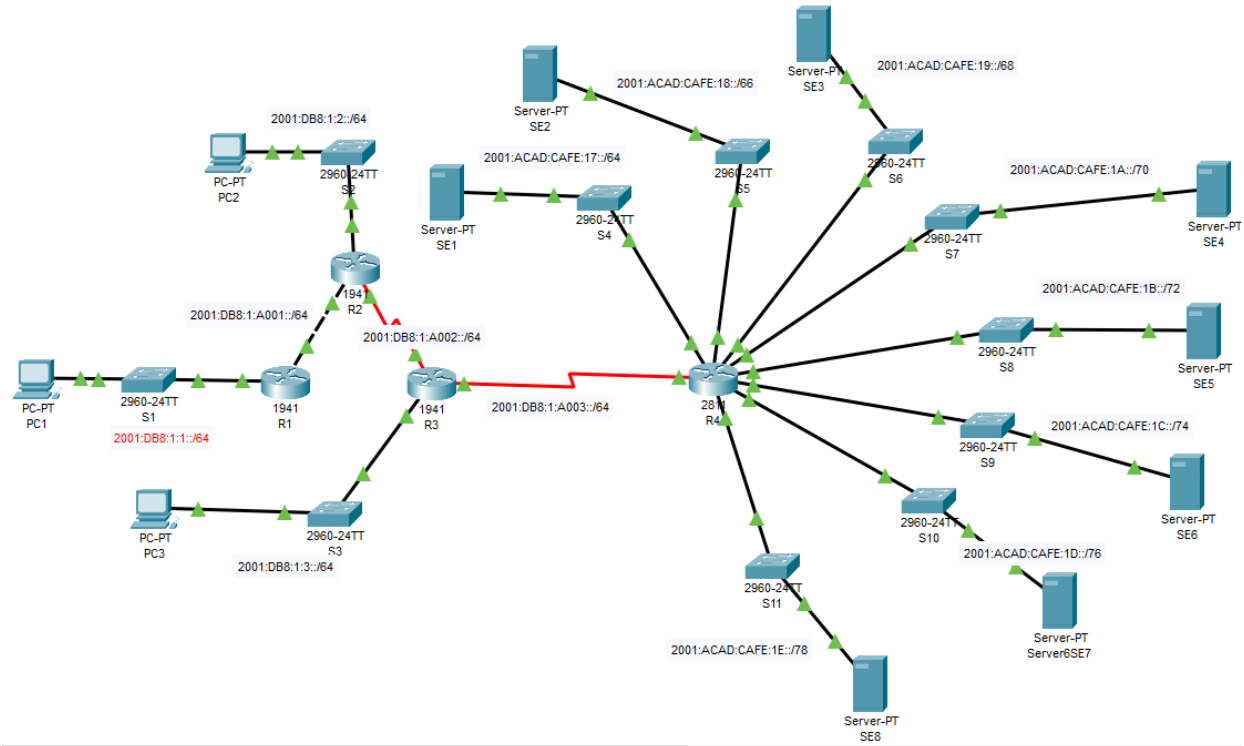
Paso 1: Configurar una ruta predeterminada en el R4

a. Configure una ruta predeterminada en el R4 de modo que se pueda llegar a cada red que no esté conectada directamente.

Paso 2: Configurar una ruta resumida en los routers R1, R2 y R3

a. Calcule y configure una sola ruta resumida en los routers R1, R2 y R3 hacia las redes que comiencen con 192….

Todos los equipos deben de tener conectividad.



Parte 1: Configurar rutas estáticas y predeterminadas IPv6

Paso 1: Habilitar el routing IPv6 en todos los routers

Antes de configurar rutas estáticas, se debe configurar el router para que reenvíe paquetes IPv6.

¿Qué comando permite lograr este resultado? _____

Introduzca este comando en cada router.

Paso 2: Configurar rutas estáticas recursivas en el R1

Configure una ruta estática IPv6 recursiva en cada red que no esté conectada directamente al R1 a excepción de las redes que empiecen con 2001:ACAD…..

Paso 3: Configurar una ruta estática conectada directamente y completamente especificada en el R2

a. Configure una ruta estática conectada directamente desde el R2 hasta la LAN del R1 y al enlace WAN entre R3 y R4

b. Configure una ruta **completamente especificada** desde el R2 hasta la LAN del R3.

Paso 4: Configurar una ruta predeterminada en el R3

Configure una ruta predeterminada recursiva en el R3 que llegue a todas las redes que no estén conectadas directamente a excepción de las redes que empiecen con 2001:ACAD…..

Parte 2: Verificar la conectividad de la red

Hasta el momento todos los dispositivos de los routers R1, R2 y R3 deberían poder hacerse ping. Si no fuera así, revise la configuración de las rutas estáticas y predeterminadas.

Parte 3: Configurar de rutas predeterminadas y resumidas

Paso 1: Configurar una ruta predeterminada en el R4

b. Configure una ruta predeterminada en el R4 de modo que se pueda llegar a cada red que no esté conectada directamente.

Paso 2: Configurar una ruta resumida en los routers R1, R2 y R3

b. Calcule y configure una sola ruta resumida en los routers R1, R2 y R3 hacia las redes que comiencen con 2001:ACAD….

Todos los equipos deben de tener conectividad.

Semana 3

Configuración de VLAN

Sección: ……..……..	Apellidos : ……..……..
Docente : Giancarlo Condori Torres	Nombres : ……..
Unidad : Unidad 1	Fecha: …../……/…… Duración: 240 min

Instrucciones: A continuación de manera colaborativa configure los routers y switches con las siguientes instrucciones.

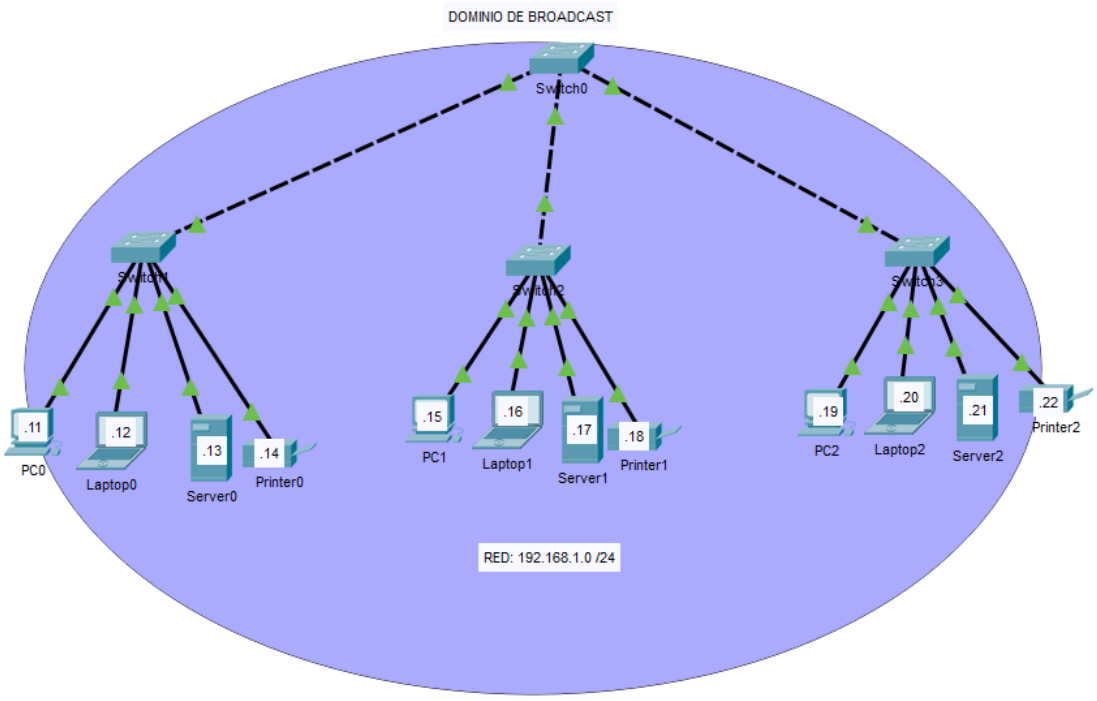
I. **Propósito**: El estudiante será capaz de configurar VLAN, routing de VLAN haciendo uso de switches de capa 2, capa 3 y routers

II. Descripción de la actividad a realizar (casos)

Las VLAN son útiles para la administración de grupos lógicos y permiten mover, cambiar o agregar fácilmente a los miembros de un grupo. Esta actividad se centra en la creación y la denominación de redes VLAN, así como en la asignación de puertos de acceso a VLAN específicas.

III. Procedimientos

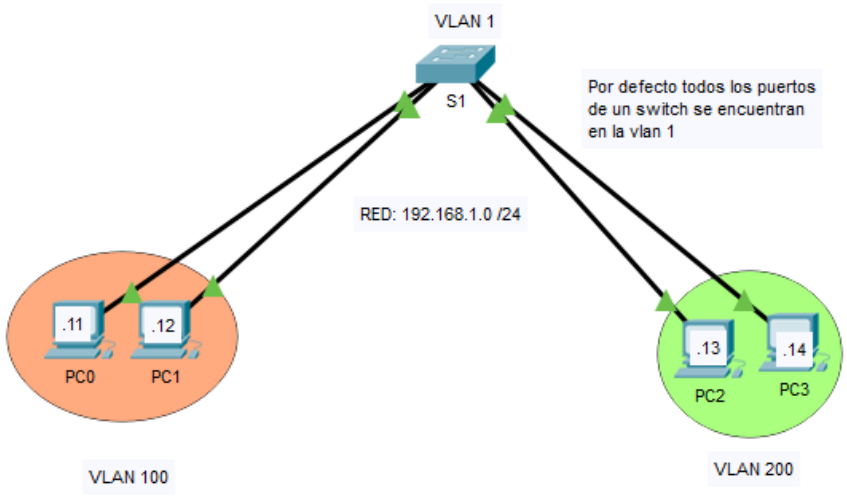
Parte 1: Tráfico Broadcast



c. Haciendo uso de la vista simulador del software packet tracer, haga ping al mismo tiempo en la PC0, Server1 y laptop2 a la dirección de broadcast.

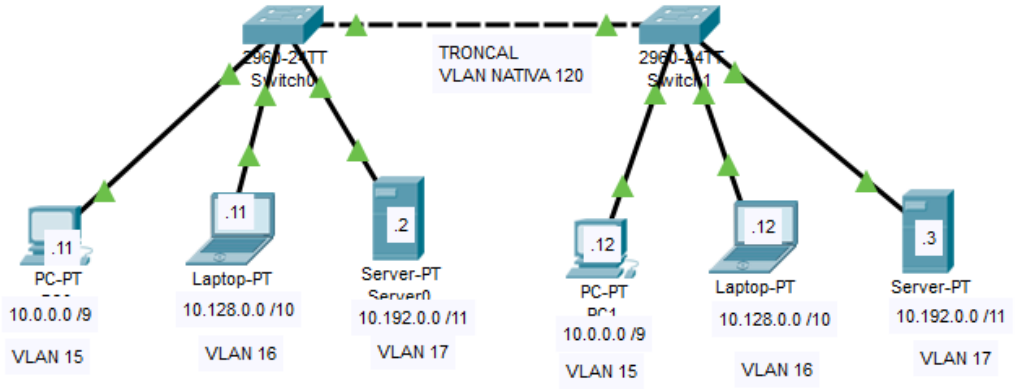
d. Observe el tráfico que se genera al hacer correr la animación con el simulador y analice el enorme problema que se genera cuando se tiene un solo dominio de broadcast.

Parte 2: VLAN predeterminada



a. A través de comandos IOS vea que todos los puertos del switch están en la VLAN 1
b. Por defecto los cuatro equipos se deben de hacer ping ya que están en la misma VLAN y en la misma red.
c. Cree las vlan 100 y 200 con sus respectivos nombres
d. Observe que las vlan estén creadas.
e. Ingrese a los puertos que están conectados a los equipos y configúrelo como acceso
f. Asocie los puertos a sus vlan respectivas según esquema.
g. Verifique con comandos que los puertos estén asignados a su vlan correcta
h. Haga ping de un equipo de la vlan 100 a otro equipo de la vlan 200. ¿El ping fue correcto? ¿porqué?
i. Desde cualquier PC haga ping al broadcast y verifique si ese tráfico afecta a las dos VLAN y saque sus conclusiones.

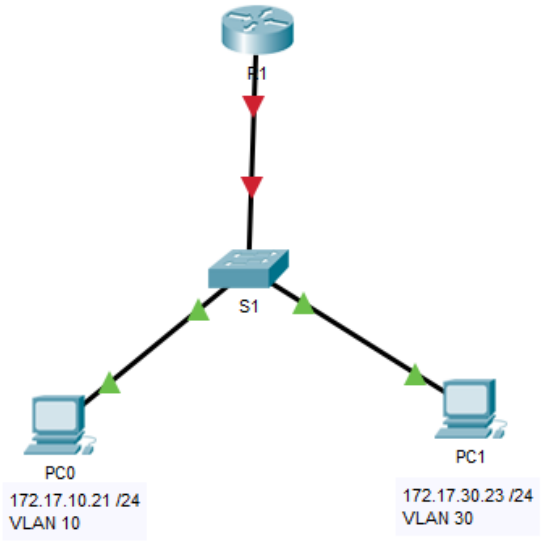
Parte 3: VLAN con troncales



a. En los dos switches cree las vlan 15, 16, 17 y 120
b. Observe que las vlan estén creadas.

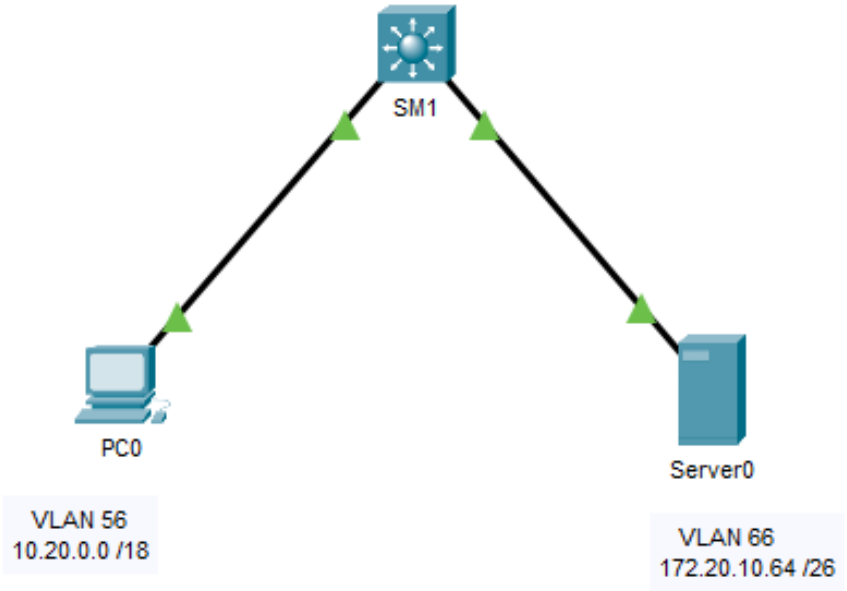
c. Ingrese a los puertos que están conectados a los equipos y configúrelo como acceso
d. Asocie los puertos a sus vlan respectivas según esquema.
e. Haga ping de la PC de la vlan 15 con la otra PC de la vlan 15 que está en el otro switch. ¿el ping fue exitoso? ¿porqué?
f. En el switcht0 configure la interfaz que conecta al otro switch como troncal y asóciela a la vlan nativa.
g. Verifique con comandos que la interfaz esté como troncal
h. Vaya al otro switch y vea que sale un mensaje de error de falta de concordancia de vlan. Explique porqué
i. Para solucionar el problema haga la misma configuración en el switch1 del paso "**f**".
j. La conectividad debe ser exitoso entre las mismas vlan.

Parte 4: Enrutamiento de VLAN con ROUTER ON STICK



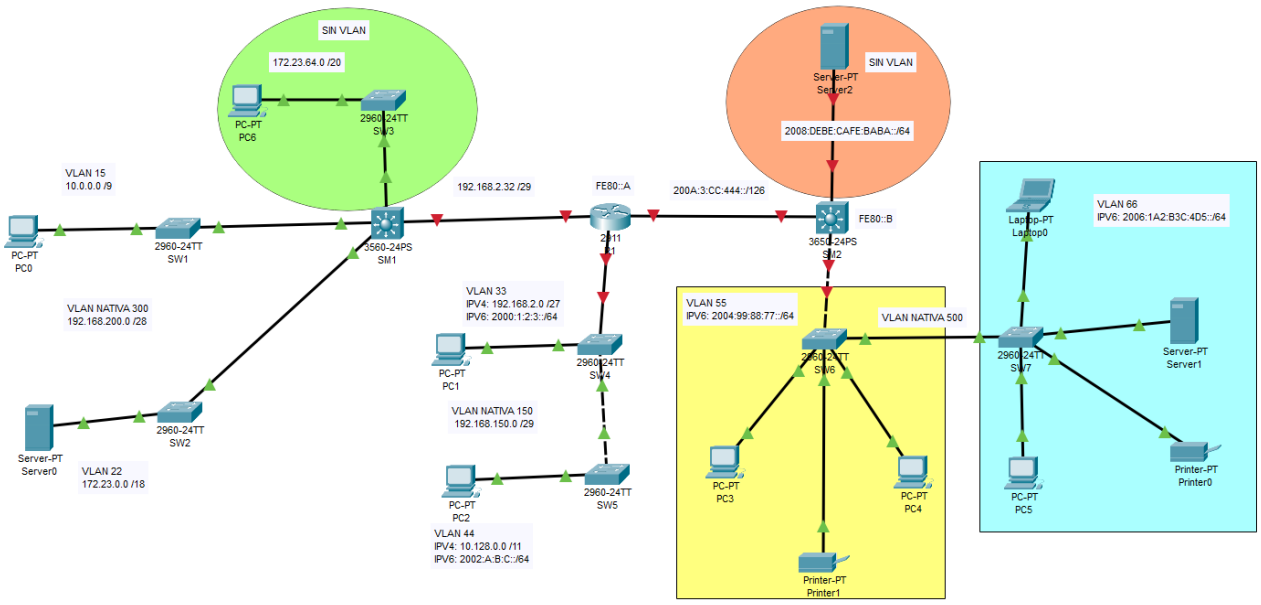
a. En el **S1** cree las VLAN y asocie los puertos como está en el esquema.
b. el ping de una PC a la otra PC el ping es fallido, esto es normal porque se encuentran en redes y en vlan distintas.
c. Para dar solución a esto configuremos el enrutamiento de vlan con el método **ROUTER-ON-STICK** en el **R1** como sigue a continuación
d. En R1 active la interfaz que está conectado al switch
e. En **R1** cree subinterfaces, encapsulamiento con el número de las vlan creadas en el **S1** y asigne el primer IP por cada red.
f. En las PCs debe de poner un Gateway que apunta a los IPs del router.
g. Haga prueba de conectividad entre las PCs. ¿el ping fue exitoso? ¿porqué?
h. En **S1** cree la vlan 200 para que sea la vlan nativa
i. En **S1** configure la interfaz que conecta al router como troncal y asóciela a la vlan nativa.
j. En el router cree la subinterfaz con el número de la vlan nativa y encapsúlele como nativa.
k. Los equipos ya se deben de hacer ping.

Parte 5: Enrutamiento de VLAN con Switch multicapa



a. En el **SM1** cree las VLAN y asocie los puertos como está en el esquema.
b. Configure las puertas de enlace de los equipos.
c. ¿Se pueden hacer ping los equipos??
d. Para que los equipos se hagan ping en el SM1 active el enrutamiento IPv4 con el comando **IP ROUTING** en el modo global.
e. Cree las interfaces como muestra el esquema, una vez dentro configure su direccionamiento IP.
f. Los equipos ya se deben de hacer ping.

Parte 6: Caso práctico



Todos los dispositivos finales ya tienen IPv4 e IPv6 según corresponda, a excepción del router y los switches de capa 3. Desarrolle lo siguiente:

a. Configure y enrute VLAN entre el SW1, SW2 y el SM1, de tal manera que las VLAN 15 y 22 se hagan ping, incluido los switches SW1 y SW2.

b. Configure VLAN entre el SW4, SW5 y el R1, de tal manera que las VLAN 33 y 34 se hagan ping a nivel IPv4 incluido los switches.

c. Configure VLAN entre el SW4, SW5 y el R1, de tal manera que las VLAN 33 y 34 se hagan ping a nivel IPv6. OJO: los switches 2960 en packet tracer no trabajan bien con IPv6.

d. Configure VLAN entre el SW6, SW7 y el SM2, de tal manera que las VLAN 55 y 66 se hagan ping a nivel IPv6.

e. Configure IPv4 entre SM1 y R1, de tal manera que se hagan ping.

f. Configure IPv6 entre SM2 y R1, de tal manera que se hagan ping.

g. Configure el SM1 con IPv4 para la zona verde, de tal manera que la PC6 le haga ping.

h. Configure el SM2 con IPv6 para la zona naranja, de tal manera que el servidor le haga ping.

i. Configure enrutamiento estático para IPv4 de la mejor forma posible entre el SM1 y R1, de tal manera que todos los equipos con IPv4 se hagan ping, incluido los switches con IPv4

Configure enrutamiento estático para IPv6 de la mejor forma posible entre el SM2 y R1, de tal manera que todos los equipos con IPv6 se hagan ping.

Semana 4

Práctica integrada

Sección: ……..……..	Apellidos : ……..……..
Docente : Giancarlo Condori Torres	Nombres : ……..
Unidad : Unidad 1	Fecha: …../……/…… Duración: 240 min

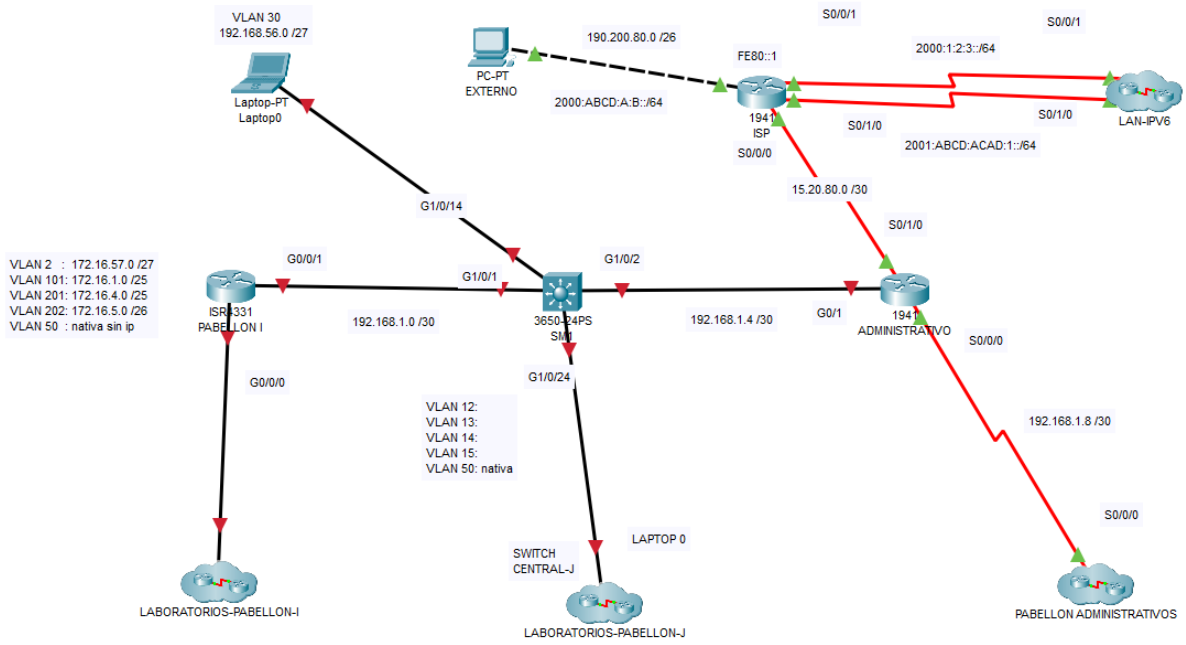
Instrucciones: A continuación de manera colaborativa configure los routers y switches con las siguientes instrucciones.

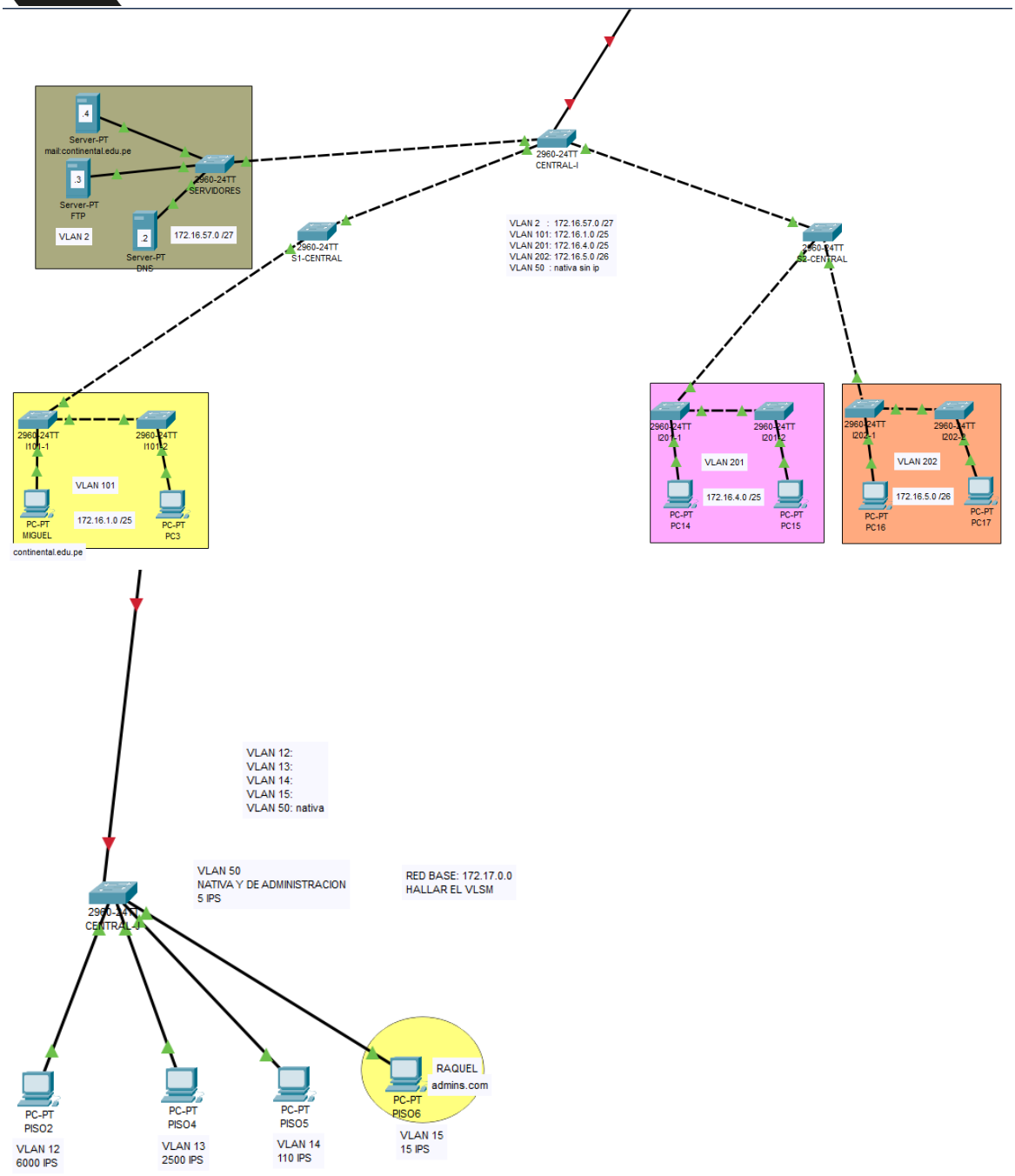
I. Propósito: El estudiante será capaz de integrar todos los servicios de red vistas hasta la fecha.

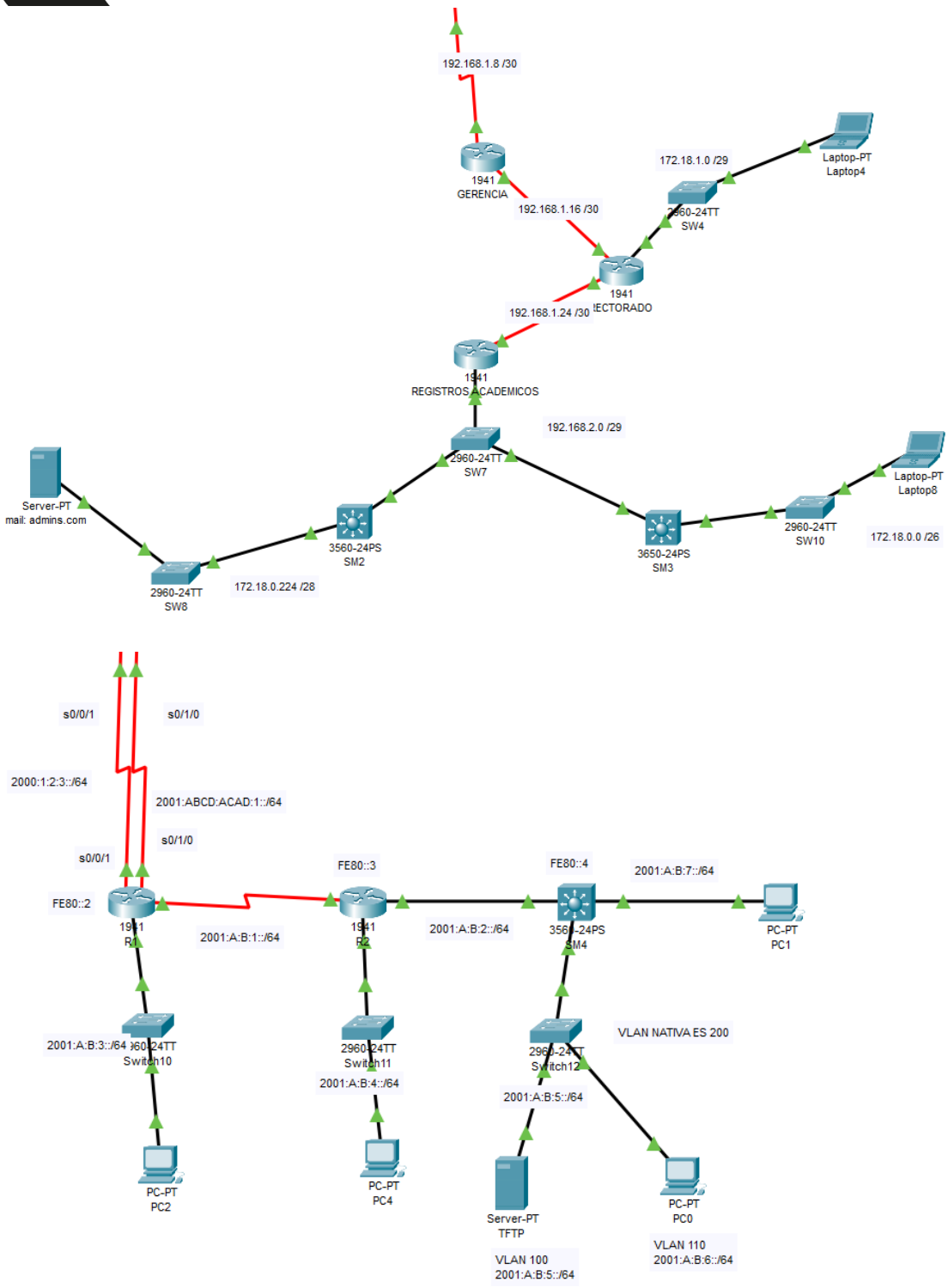
II. Descripción de la actividad a realizar (casos)

En esta actividad se va a integrar las VLAN, enrutamiento de VLAN, enrutamiento estático, cálculo de VLSM, configuración de servidores de red y el acceso remoto seguro a router y switches.

III. Procedimientos




Server-PT
mail:continental.edu.pe
Server-PT
FTP
2960-24TT
SERVIDORES
VLAN 2
Server-PT
DNS
172.16.57.0 /27
2960-24TT
CENTRAL-I
2960-24TT
S1-CENTRAL
VLAN 2 : 172.16.57.0 /27
VLAN 101: 172.16.1.0 /25
VLAN 201: 172.16.4.0 /25
VLAN 202: 172.16.5.0 /26
VLAN 50 : nativa sin ip
2960-24TT
S2-CENTRAL
2960-24TT
I101-1
2960-24TT
I101-2
VLAN 101
PC-PT
MIGUEL
172.16.1.0 /25
PC-PT
PC3
continental.edu.pe
2960-24TT
I201-1
2960-24TT
I201-2
VLAN 201
PC-PT
PC14
172.16.4.0 /25
PC-PT
PC15
2960-24TT
I202-1
2960-24TT
I202-2
VLAN 202
PC-PT
PC16
172.16.5.0 /26
PC-PT
PC17
VLAN 12:
VLAN 13:
VLAN 14:
VLAN 15:
VLAN 50: nativa
VLAN 50
NATIVA Y DE ADMINISTRACION
5 IPS
RED BASE: 172.17.0.0
HALLAR EL VLSM
2960-24TT
CENTRAL-I
PC-PT
PISO2
VLAN 12
6000 IPS
PC-PT
PISO4
VLAN 13
2500 IPS
PC-PT
PISO5
VLAN 14
110 IPS
RAQUEL
admins.com
PC-PT
PISO6
VLAN 15
15 IPS



Parte 1: Creación y configuración de VLAN

e. En la LAN “LABORATORIOS-PABELLON-I” crear y configurar las VLAN como se plantea en el esquema.

f. Configurar los puertos de acceso y troncales en base a su criterio

g. Todos los equipos de la misma VLAN se deben hacer ping.

Parte 2: Enrutamiento VLAN

a. En el router “PABELLON-I” configure el enrutamiento VLAN, de tal manera que todas las VLAN se puedan interconectar.

Parte 3: Cálculo de VLSM

a. En la LAN "LABORATORIOS-PABELLON-J", calcule el VLSM en base a la red planteada
b. Asigne los IPs calculados a los dispositivos
c. Cree y configure las VLAN 12, 13, 14, 15 Y 150 en el switch "central-J"
d. En el router "SM1" configure el enrutamiento de las VLAN, de tal manera que las anteriores VLAN se hagan ping.
e. En el router SM1 configure la VLAN 30 y asocie la laptop 0
f. Todos los equipos deben de tener conexión entre ellos, incluido el switch CENTRAL-J y la VLAN 30

Parte 4: Configurar enrutamiento estático

Paso 1: Configurar enrutamiento estático en los routers PABELLON-I, SM1, ADMINISTRATIVOS y todos los routers que pertenecen a la LAN "PABELLON-ADMINISTRATIVOS" con los siguientes parámetros:

j. En el router PABELLON I, configure enrutamiento estático predeterminado de manera recursiva para todas las redes
k. En el router SM1 configure una sóla ruta sumarizada recursiva hacia las redes del PABELLON I.
l. En el router SM1 configure una ruta predeterminada recursiva hacia el resto de redes.
m. En el router ADMINISTRATIVO configure 3 rutas estáticas: una para el pabellón I y J, otra para la VLAN 30, y otra para el pabellón administrativo de la mejor forma posible.
n. En la nube PABELLON ADMINISTRATIVO configure enrutamiento estático de la mejor forma posible, de tal manera que todos los equipos de esa nube se hagan ping.
o. Pruebe conectividad entre todas las redes LAN internas de todas las nubes, debería ser satisfactorio.

Parte 5: Configurar VLAN y enrutamiento estático para IPv6

c. En la nube LAN-IPV6, en el switch 12 y SM4 configure y enrute VLAN, de tal manera que las 2 VLAN se hagan ping.
d. En el SM4, configure su direccionamiento IPv6 en las interfaces que falta
e. Configure enrutamiento estático con IPv6 en todos los routers, de la manera más óptima, de tal manera que todos se hagan ping.

Parte 6: Configurar rutas estáticas predeterminadas, flotantes y resumidas

a. En el router **"ADMINISTRATIVO"**, crear una ruta predeterminada para internet.
b. En el router **"R1"**, de la LAN **"LAN-IPV6"** crear una ruta predeterminada para internet por la interfaz **s0/0/1** como primaria y por la **s0/1/0** como secundaria.
c. En el router **ISP** crear una sola ruta resumida para las redes LAN con IPv4 y otra ruta para la VLAN 30.
d. En el router **ISP** crear una sola ruta resumida para las redes LAN con IPv6 por la interfaz **s0/0/1** como primaria y por la **s0/1/0** como secundaria
e. Todos los equipos deben de hacer ping al host externo

Parte 7: Configurar servidores FTP, DNS, TFTP y CORREO

Paso 1 Configurar servidores CORREO y DNS.

a. Configurar los servidores de correo: **continental.edu.pe** del pabellón I, **admins.com** del pabellón administrativos y el servidor DNS del pabellón I, de tal manera que Miguel con su cuenta de continental.edu.pe pueda enviarle correos a RAQUEL con su cuenta admins.com.

b. Configurar el servidor FTP de la VLAN 2 con un usuario JUAN, password: 123 y con permisos de LECTURA Y LISTADO, de tal manera que cualquier equipo con IPv4 pueda acceder.

c. Configurar el servidor TFTP de la LAN-IPV6, de tal manera que el router R1 pueda guardar el contenido de memoria RAM o NVRAM

Parte 8: Configurar acceso remoto seguro

Paso 1 Configurar SSH versión 2 en el switch "CENTRAL-J" que está en la LAN "LABORATORIOS-PABELLON-J" con los siguientes parámetros.

a. Nombre de dominio: **conti.com**
b. Parámetros de par de claves RSA con encriptación de 2048.
c. Establecimiento de SSH versión 2, limitado a 3 intentos de autenticación y a un tiempo de espera de 40 segundos.
d. Usuario **admin** con contraseña secreta **class**.
e. Las líneas VTY aceptan todas las conexiones, tanto SSH y TELNET y utilizan el nombre de usuario local para la autenticación.
f. Contraseña encriptada para el modo privilegiado **"class"**

Todos los clientes con IPv4 deben de poder conectarse por SSH o TELNET.

Segunda unidad

Semana 5

Configuración de pvst+

Sección: ……..……..	Apellidos : ……..……..
Docente : Giancarlo Condori Torres	Nombres : ……
Unidad : Unidad 2	Fecha: ……/……/…… Duración: 70 min

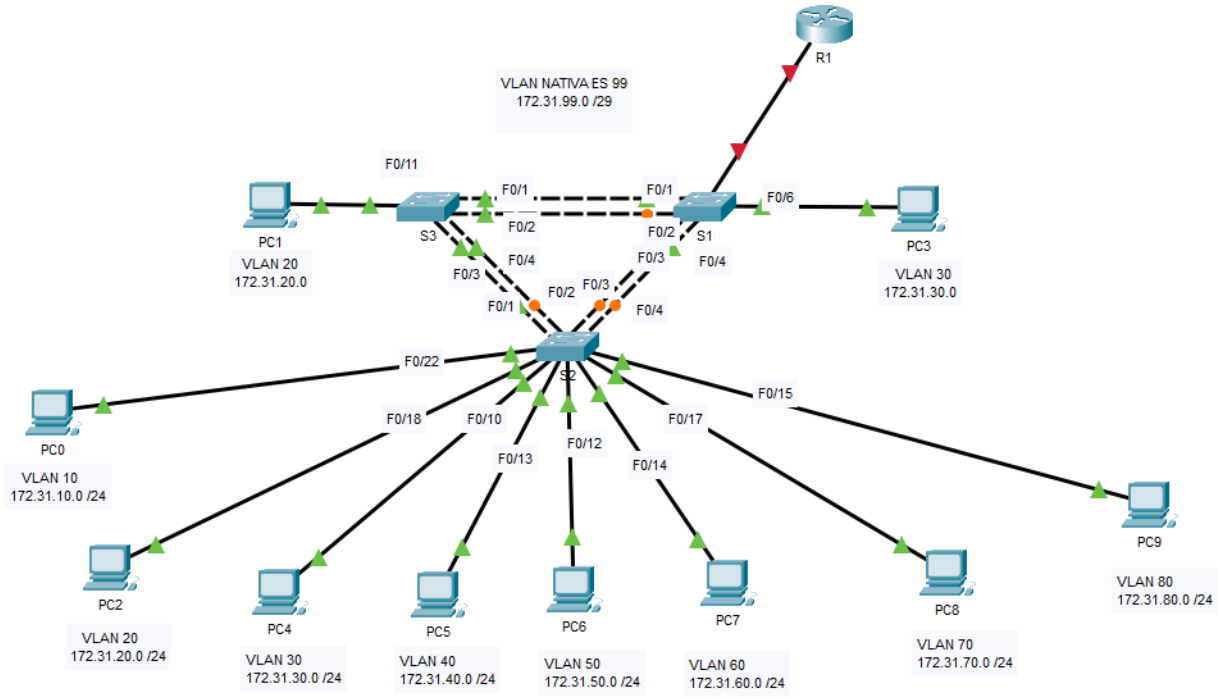
Instrucciones: A continuación de manera colaborativa resuelva el siguiente caso con las siguientes instrucciones.

I. Propósito: El estudiante será capaz de configurar STP haciendo uso del software simulador Packet tracer

II. Descripción de la actividad a realizar (casos)

En esta actividad, configurará redes VLAN y enlaces troncales, y examinará y configurará los puentes raíz principales y secundarios del protocolo de árbol de expansión. También optimizará la topología conmutada mediante PVST+, PortFast y la protección BPDU.

III. Procedimientos



Parte 1: Verificar la configuración de las VLAN

- Verificar que en los 3 switches se haya creado las VLAN: 10, 20, 30, 40, 50, 60, 70, 80 y 99 y las PCs estén asociados a sus respectivas VLAN según el esquema.
- Verificar que en los 3 switches se hayan creado las interfaces troncales asociados a la VLAN nativa 99.
- Los 3 switches ya tienen ip, por lo que se deberían hacer ping.
- Las Pcs de las mismas VLAN se deberían hacer ping.

Parte 2: Configurar el protocolo de árbol de expansión PVST+ y el balanceo de carga

Dado que hay una instancia separada del spanning-tree para cada VLAN activa, se efectúa una elección de raíz separada para cada instancia. Si las prioridades del switch establecidas de manera predeterminada se utilizan para seleccionar la raíz, se elige la misma raíz para cada instancia del árbol de expansión, como ya hemos visto. Esto podría ocasionar un diseño inferior. Algunas razones para controlar la selección del switch raíz incluyen:

- El switch raíz es el responsable de generar las BPDU para el STP 802.1D y es el centro del tráfico de control del árbol de expansión. El switch raíz debe ser capaz de manejar esta carga adicional.
- La ubicación de la raíz define las rutas conmutadas activas en la red. Es posible que la ubicación aleatoria produzca rutas por debajo de lo óptimo. Lo ideal es que la raíz se encuentre en la capa de distribución.
- Considere la topología que se utiliza en esta actividad. De los seis enlaces troncales configurados, sólo tres transportan tráfico. Si bien esto evita los bucles, es un desperdicio de recursos. Dado que la raíz puede definirse en función de la VLAN, es posible que algunos puertos estén bloqueando elementos para una VLAN y reenviando elementos a otra. Esto se demuestra a continuación.

Paso 1: Configurar el modo STP.

Utilice el comando **spanning-tree mode** para establecer que los switches utilicen PVST como el modo STP.

Paso 2: Configurar el balanceo de carga del protocolo de árbol de expansión PVST+.

a. Configure el **S1** para que sea la raíz principal para las VLAN 1, 10, 30, 50 y 70 y las otras vlan como secundarias. Configure el **S3** para que sea la raíz principal para las VLAN 20, 40, 60, 80 y 99 y las otras vlan como secundaria.

b. Verifique la configuración mediante el comando **show spanning-tree**.

Parte 3: Configurar PortFast y la protección BPDU

Paso 1: Configurar PortFast en los switches.

PortFast hace que un puerto ingrese al estado de reenvío casi de inmediato al disminuir drásticamente el tiempo de estados de escucha y aprendizaje. PortFast minimiza el tiempo que tarda en conectarse el servidor o la estación de trabajo. Configure PortFast en las interfaces del switch que están conectadas a las computadoras.

Paso 2: Configurar la protección BPDU en los switches.

La mejora en la Protección STP PortFast BPDU permite que los diseñadores de red apliquen las fronteras de dominio de STP y mantengan predecible la topología activa. Los dispositivos detrás de los puertos que tienen PortFast habilitado no pueden influir en la topología STP. Al recibir las BPDU, la función de protección BPDU deshabilita el puerto que tiene PortFast configurado. La protección BPDU lleva a cabo la transición del puerto al estado err-disabled, y aparece un mensaje en la consola. Configure la protección BPDU en las interfaces del switch que están conectadas a las computadoras.

Paso 3: Verificar la configuración.

Utilice el comando **show running-configuration** para verificar la configuración.

Parte 4: Enrutamiento VLAN

Paso 1: enrutamiento VLAN router-on-stick

Configure el R1 y el S1 para que todas las VLAN estén enrutadas haciendo uso del método routers on stick

Paso 2: pruebe conectividad

Todos los equipos que pertenecen a distintas VLAN deben poder tener conectividad entre ellos, inclusive con los switches.

Semana 6

ETHERCHANNEL y DHCPv4

Sección: ……..……..	Apellidos : ……..……
Docente : Giancarlo Condori Torres	Nombres : ……
Unidad : Unidad 2	Fecha: ...../……/2021 Duración: 270 min

Instrucciones: A continuación de manera colaborativa resuelva el siguiente caso con las siguientes instrucciones.

I. Propósito: El estudiante será capaz de configurar Etherchannel y DHCPv4 haciendo uso del software simulador Packet tracer

II. Descripción de la actividad a realizar (casos)

ETHERCHANNEL

El diseño de la red incluye switches y enlaces redundantes. Usted tiene alguna versión de STP configurada para evitar bucles de Capa 2. Pero ahora usted, como la mayoría de los administradores de red, se da cuenta de que podría usar más ancho de banda y redundancia en su red. ¡Nada de qué preocuparse, EtherChannel está aquí para ayudarle! EtherChannel agrega enlaces entre dispositivos en paquetes. Estos paquetes incluyen enlaces redundantes. STP puede bloquear uno de esos enlaces, pero no los bloqueará todos. ¡Con EtherChannel su red puede tener redundancia, prevención de bucles y mayor ancho de banda!

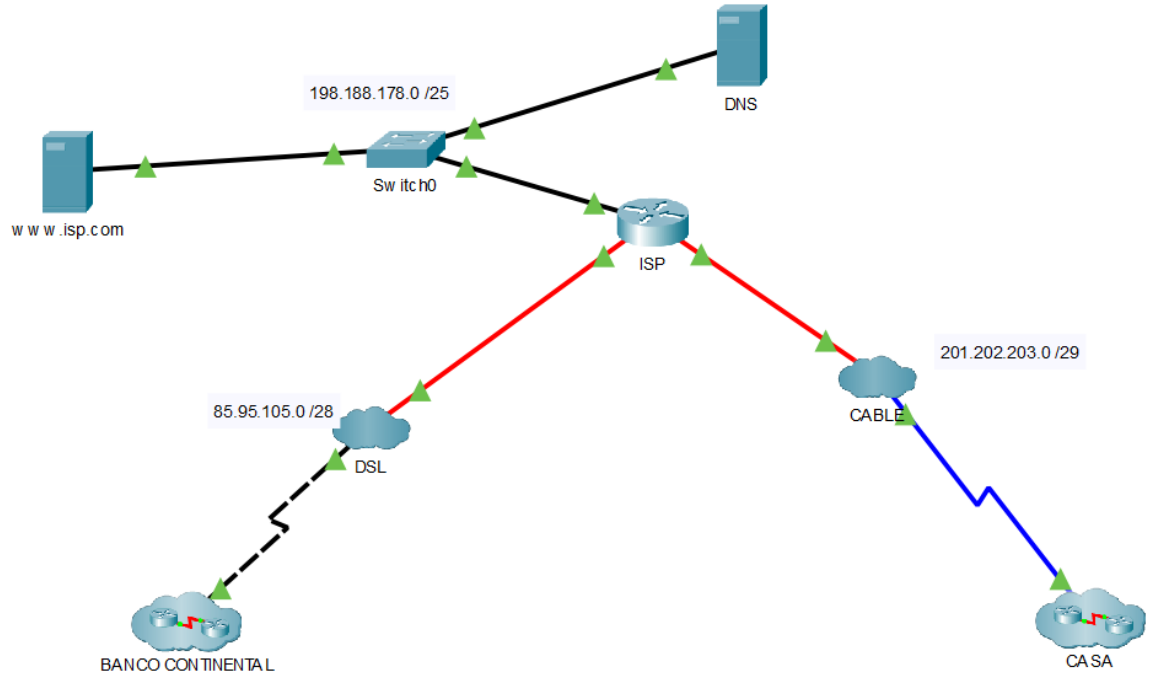
Hay dos protocolos, PAgP y LACP. Este módulo explica ambos y también muestra cómo configurarlos, verificarlos y solucionarlos.

DHCPv4

El protocolo de configuración dinámica de host (DHCP) se utiliza para asignar direcciones IPv4 dinámicamente a hosts de red. DHCPv4 es para una red IPv4. Esto significa que usted, el administrador de la red, no tiene que pasar el día configurando direcciones IP para cada dispositivo de la red. En una pequeña casa u oficina, eso no sería muy difícil, pero cualquier red grande podría tener cientos, o incluso miles de dispositivos.

En esta práctica, aprenderá a configurar un router Cisco IOS para que sea un servidor DHCPv4, así como cliente DHCPv4.

III. Procedimientos



Parte 1: Configurar VLAN y su enrutamiento

- En la nube Continental configurar y enrutar VLAN entre los switches SW1, SW2, SW3, SW6 y SM1, de tal manera que todos los equipos de esas VLAN se hagan ping, incluido los switches de la VLAN 33.

Parte 2: Configurar STP.

- En la nube Continental configure PVST rápido en los switches SW1, SW2, SW3, SW6 y SM1
- Configure los puentes raíces primarios o secundarios como sigue:

Dispositivo	Prioridad de VLAN 2 y 3	Prioridad de VLAN 4 y 33
SW6	Primario	16384
SW3	Secundario	12288

Parte 3: Configurar Etherchannel de capa 2

- En la nube Continental configure Etherchannel de capa 2 entre los switches SW1, SW2, SW3, SW6 y SM1 según muestra el esquema.
- Configurar los canales lógicos como troncales y asociados a la VLAN nativa.
- Verificar el incremento de ancho de banda en los switches y con ayuda de la vista simulador verificar el balanceo de carga que se da. OJO: el incremento de ancho de banda sólo se puede comprobar en switches multicapa y routers con el comando “sh int port-channel [nro de canal]”, en los switches de capa 2 no funciona porque packet tracer no lo soporta.
- Configurar el balanceo de carga de etherchannel de manera manual entre el SW1 y SW6 y verificar que funciona.

Parte 4: Configurar Etherchannel de capa 3

- En la nube Continental, configure Etherchannel de capa 3 entre los routers SM1 con R1, R2 con SM2, SM2 con SM3, SM2 con SW4 y SM3 con SW5 según el como muestra el esquema.
- Configurar el balanceo de carga de etherchannel de manera manual entre el SW5 y SM3 y verificar que funciona.

Parte 5: Enrutamiento Estático

- En la nube Continental configure enrutamiento estático de la forma más óptima de tal manera que todos los equipos de esa nube se hagan ping. OJO: en el R1 todavía no configure la interfaz hacia internet, ni tampoco ninguna ruta predeterminada.
- Configurar el balanceo de carga de etherchannel de manera manual entre el SM2 y SM3 y verificar que funciona.

Parte 6: DHCPv4 en un equipo servidor

- En la nube Continental en el servidor DHCP de la VLAN 4 configure un pool de IPs para la misma VLAN excluyendo los 50 primeros IPs, de tal manera que brinde IPs y DNS que está en el internet de forma dinámica a la PC6.

Parte 7: Configurar Porfast y su protección BPDU

- En la nube Continental, en el SW2 apague y prenda las interfaces que conecta al servidor DHCP y la PC6. En el momento que las interfaces están cargando (color ambar), en la PC6 intente recibir IP de manera automática, este tendrá problemas en recibir los IPs, hasta que las interfaces carguen por completo.

- Para evitar estos problemas en el SW2 en las interfaces que conecta al servidor DHCP y la PC6 configure porfast y su protección BPDU. Haga las pruebas de la mejora.

Parte 8: Agente reenviador DHCPv4

- En la nube Continental en el servidor DHCP de la VLAN 4 configure otro pool de IPs para la red 10.1.0.0 /17 excluyendo los 30 primeros IPs. **¿Funcionó?**
- Para que esto funcione, es necesario la configuración de un agente reenviador que sería en el router que está más cerca a los clientes DHCP, es decir en el SM2.
- Con esto los clientes de la red 10.1.0.0 /17 debería recibir Ips por DHCP.

Parte 9: DHCPv4 en un router como servidor con agente reenviador.

- En la nube Continental en el R1 configure DHCP como servidor para la red 10.2.0.0 /18 excluyendo los 20 primeros IPs con su respectivo agente reenviador, de tal manera que los equipos de la red 10.2.0.0/18 reciban IPs de manera dinámica.

Parte 9: DHCPv4 en un switch multicapa como servidor con agente reenviador.

- En la nube Continental en el SM3 configure DHCP como servidor para la VLAN 2 excluyendo los 10 primeros IPs con su respectivo agente reenviador, de tal manera que los equipos de la VLAN 2 reciban IPs de manera dinámica.

Parte 10: DHCPv4 como cliente en switches de capa 2

- En la nube Continental en el SM3 configure DHCP como servidor para la VLAN 33 excluyendo sólo el 1er IP con su respectivo agente reenviador, de tal manera que los switches SW1, SW2 y SW3 reciban IPs.

Parte 11: DHCPv4 como cliente en un router.

- En el internet en el router ISP configure un pool de IPs en la red 85.95.105.0 /28 excluyendo el primer IP.
- En el internet configure la nube DSL para que conmute la fibra óptica con la línea telefónica.
- En la nube Continental, configure el R1 como cliente DHCP de tal manera que reciba Ips de forma dinámica.

Parte 12: Salida a internet.

- En la nube Continental en el R1 configure una ruta predeterminada recursiva para internet.
- En el router ISP configure 2 rutas sumarizadas, de tal manera que todos los equipos de la nube CONTINENTAL salguen a internet.

Parte 13: DHCP en router doméstico

- En el internet en el router ISP configure un pool de IPs en la red 201.202.203.0 /29 excluyendo el primer IP.
- En el internet configure la nube CABLE para que conmute el cable serial con la línea por cable (cable coaxial).
- En la nube CASA, configure el MODEM ROUTER como cliente DHCP de tal manera que reciba Ips de forma dinámica.

- En el modem router también configure su direccionamiento IP privado en la red: 192.168.100.0 /24 y su servicio DHCP como servidor, de tal manera que todos los equipos reciban IPs de manera dinámica.

Parte 14: DNS Y WEB

En el internet configure los servidores DNS y WEB, de tal manera que todos los equipos naveguen a www.isp.com.

Semana 7

Práctica integrada

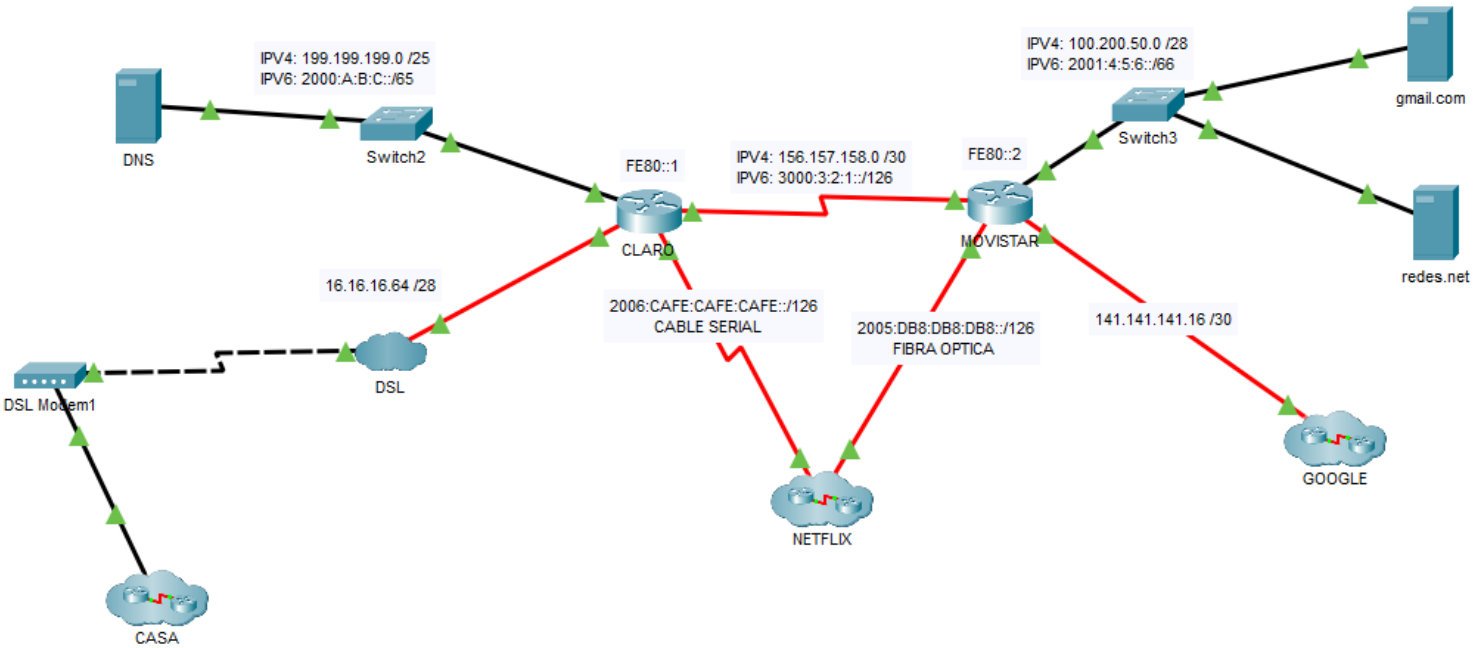
Sección:	Apellidos : .....
Docente : Giancarlo Condori Torres	Nombres : .....
Unidad : Unidad 2	Fecha: ...../...../..... Duración: 270 min

Instrucciones: A continuación de manera colaborativa resuelva el siguiente caso con las siguientes instrucciones.

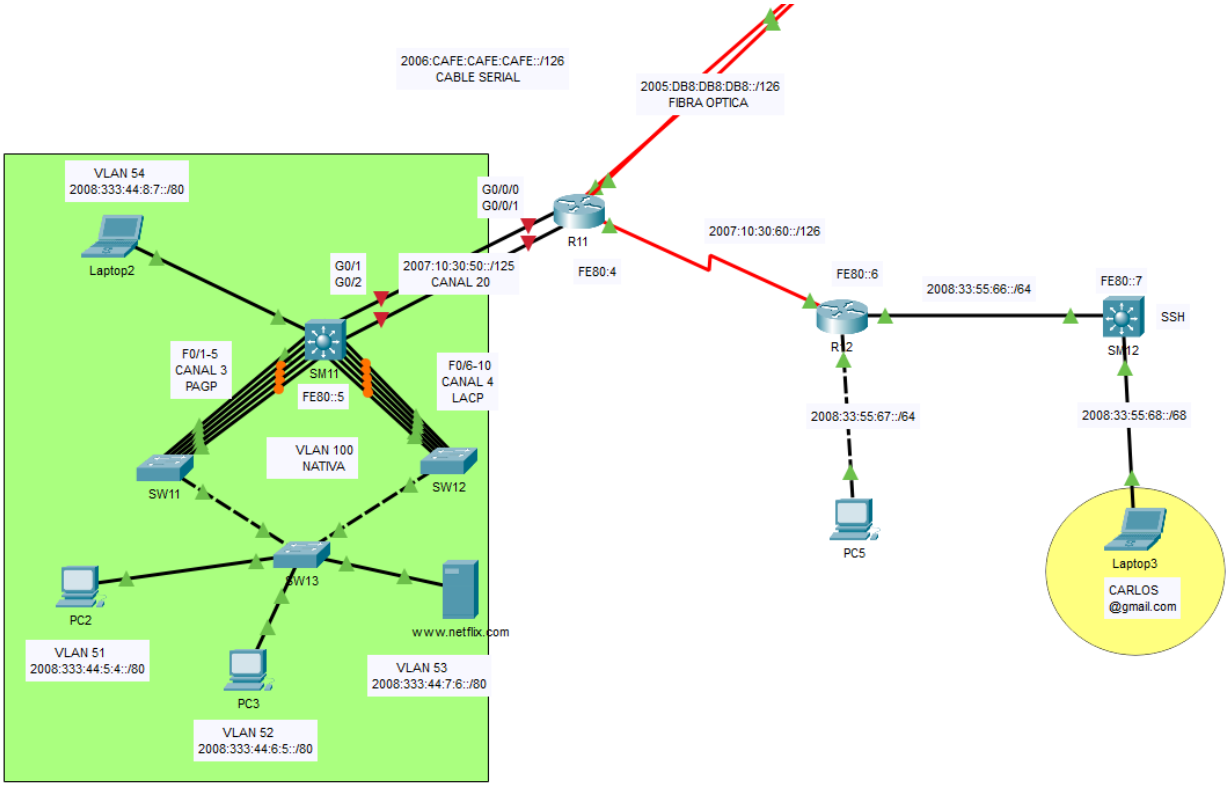
I. **Propósito:** El estudiante será capaz de integrar todos los servicios de red vistos hasta la fecha, de tal manera que esté preparado para su examen parcial.

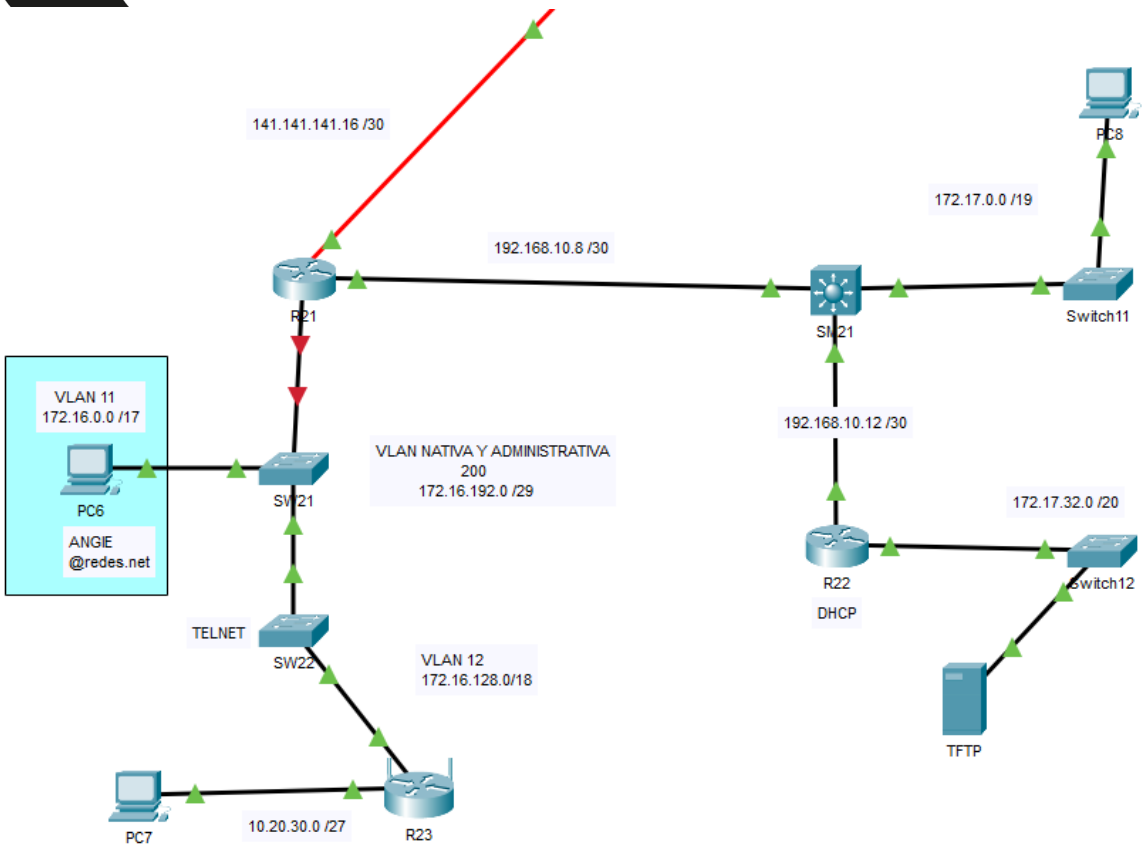
II. **Descripción de la actividad a realizar (casos)**
En esta actividad se configurará Enrutamiento estático, con IPv4 e IPv6, nube DSL y router LINKSYS, DHCP como cliente y servidor, agente reenviador de DHCP, etherchannel de capa 2 y 3, STP, VLAN y servidores de red.

III. **Procedimientos**




SW2
MODEM-ROUTER
192.168.20.128 /25
Laptop1
Printer0


2006:CAFE:CAFE:CAFE::/126
CABLE SERIAL
2005:DB8:DB8:DB8::/126
FIBRA OPTICA
VLAN 54
2008:333:44:8:7::/80
Laptop2
G0/0/0
G0/0/1
R11
G0/1
G0/2
2007:10:30:50::/125
CANAL 20
FE80:4
2007:10:30:60::/126
FE80::6
2008:33:55:66::/64
FE80::7
SSH
R12
SW12
F0/1-5
CANAL 3
PAGP
SW11
FE80::5
F0/6-10
CANAL 4
LACP
VLAN 100
NATIVA
SW11
SW12
SW13
2008:33:55:67::/64
2008:33:55:68::/68
PC5
Laptop3
CARLOS
@gmail.com
PC2
www.netflix.com
VLAN 51
2008:333:44:5:4::/80
PC3
VLAN 53
2008:333:44:7:6::/80
VLAN 52
2008:333:44:6:5::/80



Parte 1: Enrutamiento estático con IPv4 e IPv6

- En el internet configure Enrutamiento estático para IPv4 e Ipv6, de tal manera que los equipos de internet se hagan ping.

Parte 2: DHCP, nube ADSL y router LINKSYS

- En el internet, en el router CLARO, configure DHCP como servidor de tal manera que brinde IPs al router LINKSYS de la nube CASA.
- Al mismo tiempo en la nube CASA configure el router LINKSYS como servidor DHCP, de tal manera que los equipos clientes de esa nube reciban IPs

Parte 3: Salida a internet

- Hasta el momento todos los equipos de la nube CASA, deben hacerle ping al servidor DNS.
- Para que los equipos de la nube CASA tengan conectividad con los equipos internos de MOVISTAR en el el router de MOVISTAR se tiene que hacer una ruta estática hacia el enlace entre CLARO y la nube DSL.
- Todos los equipos de la nube CASA deben de salir a internet

Parte 4: VLAN y enrutamiento

- En la nube NETFLIX, configure y enrute VLAN en la zona verde, de tal manera que todas las VLAN se hagan ping.

Parte 5: Protocolo de árbol de expansión PVST no rápido

- En la nube NETFLIX, configure el modo de árbol de expansión no rápido por VLAN para los switches del SW11, SW12 y SW13.
- Configure el SW11 para que sea la raíz principal en la vlan 51 y 52 y secundario para la VLAN 53.

- Configure el SW12 para que sea la raíz principal en la vlan 53 y secundario para la VLAN 51 y 52.

Parte 6: PortFast y protección BPDU

- En la nube NETFLIX, configurar portfast y su protección BPDU en el SW13 en la interfaz que conecta al servidor WEB.

Parte 7: EtherChannel de capa 2 y 3.

- En la nube NETFLIX, entre el **SW11, SW12 y SM11** configure etherchannel de capa 2, según muestra el esquema con su respectivo balanceo de carga. OJO: las VLAN se deben de seguir haciendo ping.
- Entre el **SM11** y el **R11** configure etherchannel de capa 3 con su respectivo balanceo de carga, de tal manera que el SM11 y R11 se hagan ping.

Parte 8: Enrutamiento estático

- En la nube NETFLIX configure enrutamiento estático de la forma más óptima, de tal manera que todos los equipos de esa nube se hagan ping. OJO: en el R11 todavía no haga la ruta hacia internet, mas adelante se le pedirá.

Parte 9: SSH

- En la nube NETFLIX configure en el SM12 el servicio de SSH con los siguientes parámetros:
  - Nombre de dominio: **netflix.com**
  - Parámetros de par de claves RSA con encriptación de 1024.
  - Establecimiento de SSH versión 2, limitado a 2 intentos de autenticación y a un tiempo de espera de 30 segundos.
  - Usuario admin con contraseña secreta **class**.
  - Las líneas VTY aceptan sólo las conexiones SSH y utilizan el nombre de usuario local para la autenticación.
  - Contraseña encriptada para el modo privilegiado **"class"**
- Todos los clientes de esa nube deben de poder hacer SSH al SW11.

Parte 10: SALIDA A INTERNET

- En la nube NETFLIX en el R11 cree dos rutas estáticas predeterminadas flotantes directamente conectada o recursiva, según el tipo de cable. La salida principal hacia internet va a ser por MOVISTAR y la secundaria por CLARO.
- En el internet, en los routers MOVISTAR y CLARO crear una sola ruta estática sumarizada hacia la nube NETFLIX. De tal manera que todos los equipos de esa nube deben de salir a internet.

Parte 11: Servidores DNS y WEB

- Configurar el servidor web: netflix.com de la nube NETFLIX y el servidor DNS que está en el internet, de tal manera que cualquier equipo con IPv6 navegue a www.netflix.com

Parte 12: VLAN

- En la nube GOOGLE configure el router LINKSYS con su direccionamiento IP
- En la nube GOOGLE configure y enrute VLAN entre el R21, SW21 y SW22, de tal manera que los equipos de las VLAN se hagan ping.

Parte 13: Enrutamiento Estático

- En la nube GOOGLE, configure enrutamiento estático de la forma más óptima, de tal manera que todos los equipos de esa nube se hagan ping.

PARTE 14: DHCP

- En la nube GOOGLE configure DHCP en el R22 para que brinde IPs a la VLAN 200.
- Configure los switches SW21 y 22 para que reciban IPs de forma automática

PARTE 15: TELNET

- En la nube GOOGLE, configure en el SW22 el servicio de TELNET, de tal manera que cualquier equipo pueda ingresar al SW22 por TELNET.

PARTE 16: SERVIDOR TFTP

- En la nube GOOGLE, en el R21 cree una copia de su RAM y NVRAM hacia el servidor TFTP.
- Verifique que la copia esté guardada en el servidor TFTP.

PARTE 17: SALIDA A INTERNET

- En la nube GOOGLE e internet, configure enrutamiento estático con rutas predeterminadas y sumarizadas, de tal manera que todos los equipos de GOOGLE salgan a internet.

PARTE 18: Servidores DNS y CORREO

- En el INTERNET configure el servidor de correo: gmail.com con un usuario CARLOS que está en la nube NETFLIX.
- En el INTERNET configure el servidor de correo: redes.net con un usuario ANGIE que está en la nube NETFLIX.
- Registre los dos servidores de correo en el servidor DNS de internet.
- Los dos usuarios se deben de enviar correos.

Tercera unidad

Semana 9

Configurar DHCPv6

Sección: ……..……..	Apellidos : ……..……..
Docente : Giancarlo Condori Torres	Nombres : ……..
Unidad : Unidad 3	Fecha: …../……/…... Duración: 240 min

Instrucciones: Haciendo uso de los softwares packet tracer y GNS 3 resuelva los siguientes casos.

I. **Propósito:** El estudiante será capaz de configurar los diferentes tipos de DHCPv6 haciendo uso de packet tracer y GNS3.

II. Descripción de la actividad a realizar (casos)

La asignación dinámica de direcciones IPv6 de unidifusión global se puede configurar de tres maneras:

• Configuración automática de direcciones independiente del estado (SLAAC)

• Mediante el protocolo de configuración dinámica de host sin estado para IPv6 (DHCPv6)

• Mediante DHCPv6 con estado

Cuando se utiliza SLACC para asignar direcciones IPv6 a hosts, no se utiliza un servidor DHCPv6. Dado que no se utiliza un servidor DHCPv6 al implementar SLACC, los hosts no pueden recibir información adicional de red crítica, incluida una dirección de servidor de nombres de dominio (DNS) y un nombre de dominio.

Cuando se utiliza DHCPv6 sin estado para asignar direcciones IPv6 al host, se utiliza un servidor DHCPv6 para asignar la información de red crítica adicional, sin embargo, la dirección IPv6 se asigna mediante SLACC.

Cuando se implementa DHCPv6 con estado, el servidor de DHCP asigna toda la información, incluida la dirección host IPv6.

La determinación de cómo los hosts obtienen la información de direccionamiento dinámico IPv6 depende de la configuración de indicadores incluida en los mensajes de anuncio de router (RA).

En esta situación, la empresa creció en tamaño, y los administradores de red ya no pueden asignar direcciones IP a los dispositivos de forma manual. Su tarea es configurar el router R2 para asignar direcciones IPv6 en dos subredes diferentes conectadas al router R1

III. Procedimientos

Topología

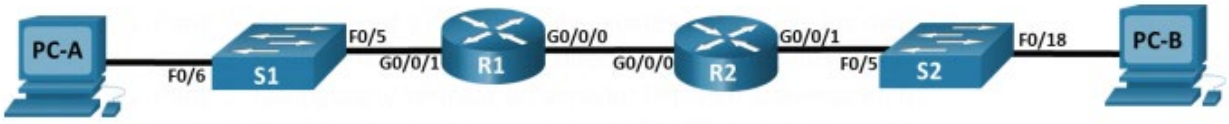


Tabla de asignación de direcciones

Dispositivo	Interfaz	Dirección IPv6
R1	G0/0/0	2001:db8:acad:2: :1 /64
		fe80::1
	G0/0/1	2001:db8:acad:1: :1/64
		fe80::1
R2	G0/0/0	2001:db8:acad:2: :2/64
		fe80::2
	G0/0/1	2001:db8:acad:3: :1 /64
		fe80::1
PC-A	NIC	DHCP
PC-B	NIC	DHCP

Parte 1: Armar la red y configurar los ajustes básicos de los dispositivos

En la parte 1, establecerá la topología de la red y configurará los parámetros básicos en los equipos host y los switches.

Paso 1: Realizar el cableado de red como se muestra en la topología

Conecte los dispositivos como se muestra en la topología y realizar el cableado necesario.

Paso 2: Configurar los parámetros básicos para cada switch (Opcional)

a. Asigne un nombre de dispositivo al switch.

b. Inhabilite la búsqueda DNS para evitar que el router intente traducir los comandos mal introducidos como si fueran nombres de host.

c. Asigne class como la contraseña cifrada del modo EXEC privilegiado.

d. Asigne cisco como la contraseña de la consola y habilite el inicio de sesión.

e. Asigne cisco como la contraseña de VTY y habilite el inicio de sesión.

f. Cifre las contraseñas de texto sin formato.

g. Cree un aviso que advierta a todo el que acceda al dispositivo que el acceso no autorizado está prohibido.

h. Apagar todos los puertos sin usar

i. Guardar la configuración en ejecución en el archivo de configuración de inicio

Paso 3: Configure los parámetros básicos para cada router.

a. Asigne un nombre de dispositivo al router.
b. Inhabilite la búsqueda DNS para evitar que el router intente traducir los comandos mal introducidos como si fueran nombres de host.
c. Asigne **class** como la contraseña cifrada del modo EXEC privilegiado.
d. Asigne **cisco** como la contraseña de la consola y habilite el inicio de sesión.
e. Asigne **cisco** como la contraseña de VTY y habilite el inicio de sesión.
f. Cifre las contraseñas de texto sin formato.
g. Cree un aviso que advierta a todo el que acceda al dispositivo que el acceso no autorizado está prohibido.
h. Habilitar el routing IPv6
i. Guardar la configuración en ejecución en el archivo de configuración de inicio

Paso 4: Configure las interfaces y el enrutamiento para ambos routers.

a. Configure las interfaces G0/0/0 y G0/0/1 en R1 y R2 con las direcciones IPv6 especificadas en la tabla anterior.
b. Configure una ruta predeterminada en cada enrutador que apunte a la dirección IP de G0/0/0 en el otro enrutador.
c. Verifique que el enrutamiento funcione haciendo ping a la dirección G0/0/1 de R2 desde R1
d. Guarde la configuración en ejecución en el archivo de configuración de inicio.

Parte 2: Verifique la asignación de direcciones SLAAC desde R1

En la Parte 2, comprobará que el host PC-A recibe una dirección IPv6 mediante el método SLAAC. Encienda el PC-A y asegúrese de que la NIC está configurada para la configuración automática IPv6.

Después de unos momentos, los resultados del comando ipconfig deberían mostrar que PC-A se ha asignado una dirección de la red 2001:db 8:1: :/64.

¿De dónde vino la porción de ID de host de la dirección?

Parte 3: Configurar y verificar un servidor DHCPv6 en R1

En la Parte 3, configurará y verificará un servidor DHCP sin estado en R1. El objetivo es proporcionar a PC-A información de servidor DNS y dominio.

Paso 1: Examine la configuración de PC-A con más detalle.

a. Ejecute el comando **ipconfig /all** en PC-A y eche un vistazo a la salida.
b. Observe que no hay sufijo DNS principal. Tenga en cuenta también que las direcciones del servidor DNS proporcionadas son direcciones de «transmisión local del sitio», y no direcciones de unidifusión, como cabría esperar.

Paso 2: Configure R1 para proporcionar DHCPv6 sin estado para PC-A.

a. Cree un grupo DHCP IPv6 en R1 denominado R1-ASTAPT. Como parte de ese grupo, asigne la dirección del servidor DNS como 2001:db8:acad: :1 y el nombre del dominio como stateless.com.

b. Configure la interfaz G0/0/1 en R1 para proporcionar el indicador de configuración Other a la LAN R1 y especifique el grupo DHCP que acaba de crear como recurso DHCP para esta interfaz.
c. Guarde la configuración en ejecución en el archivo de configuración de inicio.
d. Reinicie PC-A.
e. Examine la salida de **ipconfig /all** y observe los cambios.
f. Pruebe la conectividad haciendo ping a la dirección IP de la interfaz G0/0/1 de R2.

Parte 4: Configurar un servidor DHCPv6 con estado en R1

En la Parte 4, configurará R1 para que responda a las solicitudes DHCPv6 desde la LAN en R2.

a. Cree un grupo DHCPv6 en R1 para la red 2001:db8:acad:3:aaaa: :/80. Esto proporcionará direcciones a la LAN conectada a la interfaz G0/0/1 en R2. Como parte del grupo, establezca el servidor DNS en 2001:db8:acad: :254 y establezca el nombre de dominio en Stateful.com.
b. Asigne el grupo DHCPv6 que acaba de crear a la interfaz g0/0/0 en R1.

Parte 5: Configure y verifique la retransmisión DHCPv6 en R2.

En la Parte 5, configurará y verificará la retransmisión DHCPv6 en R2, permitiendo que PC-B reciba una dirección IPv6.

Paso 1: Encienda el PC-B y examine la dirección SLAAC que genera.

Observe en la salida que el prefijo utilizado es 2001:db8:acad:3::

Paso 2: Configure R2 como un agente de retransmisión DHCP para la LAN en G0/0/1.

a. Configure el comando **ipv6 dhcp relay** en la interfaz R2 G0/0/1, especificando la dirección de destino de la interfaz G0/0/0 en R1. Configure también el comando **managed-config-flag.**
b. Guarde su configuración.

Paso 3: Intentar adquirir una dirección IPv6 de DHCPv6 en PC-B.

a. Reinicie PC-B.
b. Abra un símbolo del sistema en PC-B y ejecute el comando **ipconfig /all** y examine la salida para ver los resultados de la operación de retransmisión DHCPv6.
c. Pruebe la conectividad haciendo ping a la dirección IP de la interfaz G0/0/1 de R1.

Semana 10

Configurarión de HSRP

Sección: ……..……..	Apellidos : ……..……
Docente : Giancarlo Condori Torres	Nombres : ……
Unidad : Unidad 3	Fecha: …../……/..... Duración: 150 min

Instrucciones: Haciendo uso de los softwares packet tracer y GNS 3 resuelva los siguientes casos.

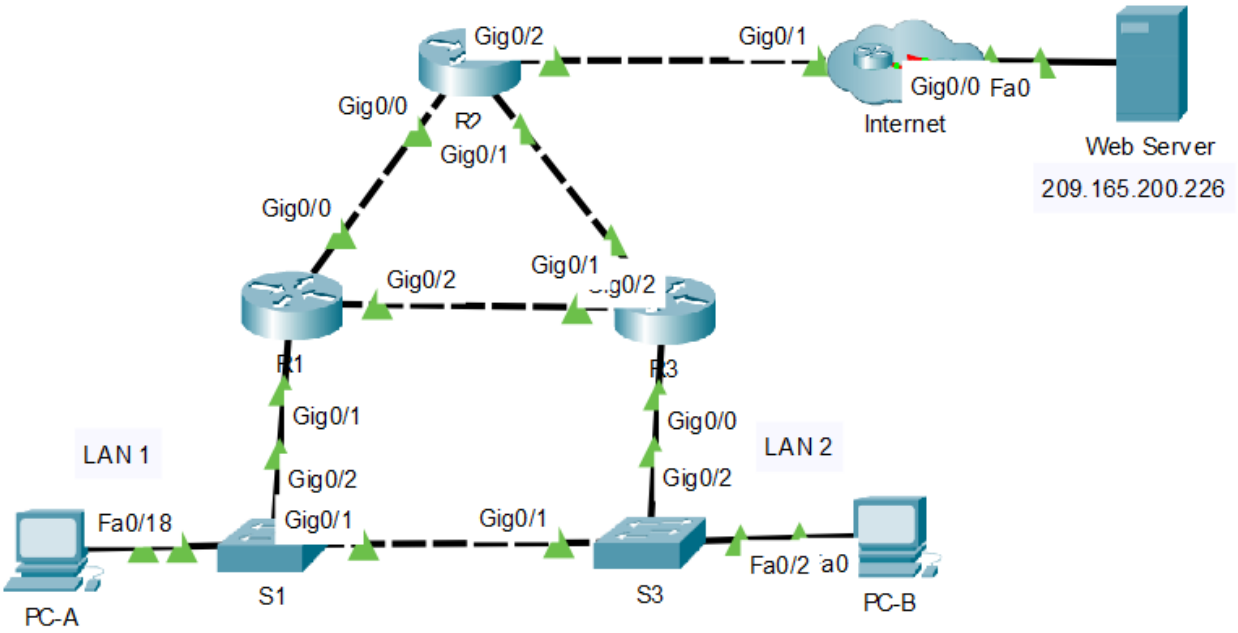
I. Propósito: El estudiante será capaz de configurar Hot Standby Router Protocol (HSRP) para proporcionar dispositivos de puerta de enlace predeterminados redundantes a hosts en LAN.

II. Descripción de la actividad a realizar (casos)

El protocolo Spanning Tree proporciona redundancia sin bucles entre conmutadores dentro de una LAN. Sin embargo, no proporciona puertas de enlace predeterminadas redundantes para dispositivos de usuario final dentro de la red si falla un router de puerta de enlace. Los protocolos de redundancia de primer salto (FHRP) proporcionan puertas de enlace predeterminadas redundantes para dispositivos finales sin necesidad de configuración adicional del usuario final. Al usar un FHRP, dos o más routers pueden compartir la misma dirección IP virtual y dirección MAC y pueden actuar como un solo router virtual. Los hosts de la red se configuran con una dirección IP compartida como puerta de enlace predeterminada. En esta actividad Packet Tracer, configurará el Protocolo de router de espera caliente (HSRP) de Cisco, que es un FHRP.

Configurará HSRP en los routers R1 y R3, que sirven como puertas de enlace predeterminadas para los hosts en LAN 1 y LAN 2. Al configurar HSRP, creará una puerta de enlace virtual que utilice la misma dirección de puerta de enlace predeterminada para los hosts de ambas LAN. Si un router de puerta de enlace deja de estar disponible, el segundo router se hará cargo con la misma dirección de puerta de enlace predeterminada que utilizó el primer router. Dado que los hosts de las LAN están configurados con la dirección IP de la puerta de enlace virtual como puerta de enlace predeterminada, los hosts recuperarán la conectividad a las redes remotas después de que HSRP active el router restante.

Procedimientos



Parte 1: Verificar la conectividad

Paso 1: Rastree la ruta al servidor web desde la PC-A.

a. Vaya al escritorio de PC-A y abra un símbolo del sistema.

b. Rastree la ruta de acceso desde PC-A al servidor web ejecutando el comando **tracert 209.165.200.226**.

¿Qué dispositivos están en la ruta de acceso desde PC-A al servidor Web? Utilice la tabla de direcciones para determinar los nombres de dispositivos.

Paso 2: Trace la ruta al servidor web desde la PC-B.

Repita el proceso en el paso 1 desde PC-B.

¿Qué dispositivos están en la ruta de acceso desde PC-B al servidor Web?

Paso 3: Observe el comportamiento de la red cuando R3 deja de estar disponible.

a. Seleccione la herramienta de eliminación de la barra de herramientas Packet Tracer y elimine el vínculo entre **R3** y **S3** .

b. Abra un símbolo del sistema en PC-B. Ejecute el comando **tracert** con el servidor Web como destino.

c. Compare la salida actual con la salida del comando del paso 2.

¿Cuáles son los resultados?

d. Haga clic en el icono **Conexiones** en la esquina inferior izquierda de la ventana PT. Localice y seleccione el icono **Cobre Strait-Through** en la paleta de tipos de conexión.

e. Haga clic en **S3** y seleccione el puerto **Gigbitethernet0/2** . Haga clic en **R3** y seleccione el puerto GigabiteThernet0/0 .

f. Después de que las luces de vínculo en la conexión estén verdes, pruebe la conexión haciendo ping al

servidor Web. El ping debería realizarse correctamente.

Parte 2: Configurar routers HSRP activos y en espera

Paso 1: Configure HSRP en el R1.

a. Configure HSRP en la interfaz LAN G0/1 de R1.

```
R1(config)# interface g0/1
```

b. Especifique el número de versión del protocolo HSRP. La versión más reciente es la versión **2**. **Nota**:

La versión en espera 1 solo admite direccionamiento IPv4.

```
R1(config-if)# standby version 2
```

c. Configure la dirección IP de la puerta de enlace virtual predeterminada. Esta dirección debe configurarse en cualquier host que requiera los servicios de la puerta de enlace predeterminada. Reemplaza la dirección de interfaz física del router que se ha configurado previamente en los hosts.

Se pueden configurar varias instancias de HSRP en un router. Debe especificar el número de grupo HSRP para identificar la interfaz virtual entre routers de un grupo HSRP. Este número debe ser coherente entre los routers del grupo. El número de grupo para esta configuración es 1.

```
R1(config-if)# standby 1 ip 192.168.1.254
```

d. Designe el router activo para el grupo HSRP. Es el router que se utilizará como dispositivo de puerta de enlace a menos que falle o que la ruta de acceso se vuelva inactiva o inutilizable. Especifique la prioridad para la interfaz del router. El valor predeterminado es 100. Un valor más alto determinará qué router es el router activo. Si las prioridades de los routers en el grupo HSRP son las mismas, entonces el router con la dirección IP configurada más alta se convertirá en el router activo.

```
R1(config-if)# standby 1 priority 150
```

R1 funcionará como el router activo y el tráfico de las dos LAN lo usará como la puerta de enlace predeterminada.

e. Si es deseable que el router activo reanude ese rol cuando vuelva a estar disponible, configúrelo para que prefiera el servicio del router en espera. El router activo se hará cargo de la función de puerta de enlace cuando vuelva a funcionar.

```
R1(config-if)# standby 1 preempt
```

¿Cuál será la prioridad HSRP de R3 cuando se agregue al grupo HSRP 1?

Paso 2: Configurar el protocolo HSRP en R3.

Configure R3 como el router en espera.

a. Configure la interfaz R3 que está conectada a LAN 2.

b. Repita solo los pasos 1b y 1c anteriores.

Paso 3: Verifique la configuración de HSRP

a. Verifique HSRP emitiendo el comando **show standby** en R1 y R3. Compruebe los valores del rol HSRP, grupo, dirección IP virtual de la puerta de enlace, preferencia y prioridad. Tenga en cuenta que HSRP también identifica las direcciones IP del router activo y en espera para el grupo.

```
R1# show standby

GigabitEthernet0/1 - Group 1
  (version 2) State is Active

    4 state changes, last state
  change 0:00:30 Virtual IP address
  is 192.168.1.254

  Active virtual MAC address is 0000.0C9F.F001

    Local virtual MAC address is 0000.0C9F.F001 (v2
  default) Hello time 3 sec, hold time 10 sec

    Next hello sent in
  1.696 secs Preemption
  enabled

  Active router is local

  El router en espera es
  192.168.1.3 Priority 150
  (configured 150)

  Group name is "hsrp-Gi0/1-1" (default)


R3# show standby

GigabitEthernet0/0 - Group 1
  (version 2) State is Standby

    4 state changes, last state
  change 0:02:29 Virtual IP address
  is 192.168.1.254

  Active virtual MAC address is 0000.0C9F.F001

    Local virtual MAC address is 0000.0C9F.F001
  (v2 default) Hello time 3 sec, hold time 10 sec

    Next hello sent in
  0.720 secs Preemption
  disabled

  El router activo es
    192.168.1.1 MAC
    address is
    d48c.b5ce.a0c1
```

```
  Standby router
  is local
  Priority 100
  (default 100)

  Group name is "hsrp-Gi0/0-1" (default)
```

Utilice el resultado que se muestra más arriba para responder las siguientes preguntas.

¿Qué router es el router activo?

¿Cuál es la dirección MAC para la dirección IP virtual?

¿Cuál es la dirección IP y la prioridad del router de reserva?

b. Utilice el comando **show standby brief** en el R1 y el R3 para ver un resumen del estado de HSRP. A continuación, se muestra un ejemplo de resultado.

```
R1# show standby brief

                     P indicates configured to preempt.

                     |

Interface Grp Pri P State Active Standby
Virtual IP Gi0/1 1 150 P Active local
192.168.1.3 192.168.1.254


R3# show standby brief

                     P indicates configured to preempt.

                     |

Interface Grp Pri P State Active Standby
Virtual IP Gi0/0 1 100 Standby
192.168.1.1 local 192.168.1.254
```

c. Cambie la dirección de gateway predeterminado para la PC-A, la PC-C, el S1 y el S3.

¿Qué dirección debería utilizar?

Verifique la nueva configuración. Ejecute un ping desde PC-A y PC-C al servidor Web. ¿Los pings son exitosos?

Parte 3: Observar la operación HSRP

Paso 1: Haga que el router activo deje de estar disponible.

Abra un símbolo del sistema en **PC-B** e introduzca el comando **tracert 209.165.200.226** .

¿La ruta difiere de la ruta utilizada antes de configurar HSRP?

Paso 2: Rompe el enlace a R1.

a. Seleccione la herramienta de eliminación de la barra de herramientas Rastreador de paquetes y elimine el cable que conecta R1 a S1.

b. Vuelva inmediatamente a PC-B y ejecute nuevamente el comando **tracert 209.165.200.226** . Observe

la salida del comando hasta que el comando complete la ejecución. Es posible que tenga que repetir el seguimiento para ver la ruta completa.

¿En qué se diferenció este rastro del anterior?

HSRP se somete a un proceso para determinar qué router debe hacerse cargo cuando el router activo deje de estar disponible. Este proceso lleva tiempo. Una vez finalizado el proceso, el router en espera R3 se activa y se utiliza como puerta de enlace predeterminada para los hosts de LAN 1 y LAN 2.

Paso 3: Restaure el enlace a R1.

a. Vuelva a conectar R1 a S1 con un cable directo de cobre.

b. Ejecute un seguimiento desde la PC-B al servidor web. Es posible que tenga que repetir el seguimiento para ver la ruta completa.

¿Qué ruta se utiliza para llegar al servidor web?

Si el comando preempt no se configuró para el grupo HSRP en R1, ¿los resultados habrían sido los mismos?

Semana 11

Cambiar configuración de seguridad

Sección:	Apellidos : .....
Docente : Giancarlo Condori Torres	Nombres : .....
Unidad : Unidad 3	Fecha: ...../...../..... Duración: 240 min

Instrucciones: Haciendo uso de los softwares packet tracer y GNS 3 resuelva los siguientes casos.

I. Propósito: El estudiante será capaz de configurar diferentes formas de darle seguridad a los switches.

II. Descripción de la actividad a realizar (casos)

Está mejorando la seguridad en dos switches de acceso en una red configurada parcialmente. Implementará el rango de medidas de seguridad cubiertas en este módulo de acuerdo con los requisitos a continuación.

Tenga en cuenta que el router se ha configurado en esta red, por lo que la conectividad entre hosts en diferentes VLAN debería funcionar cuando se complete.

III. Procedimientos

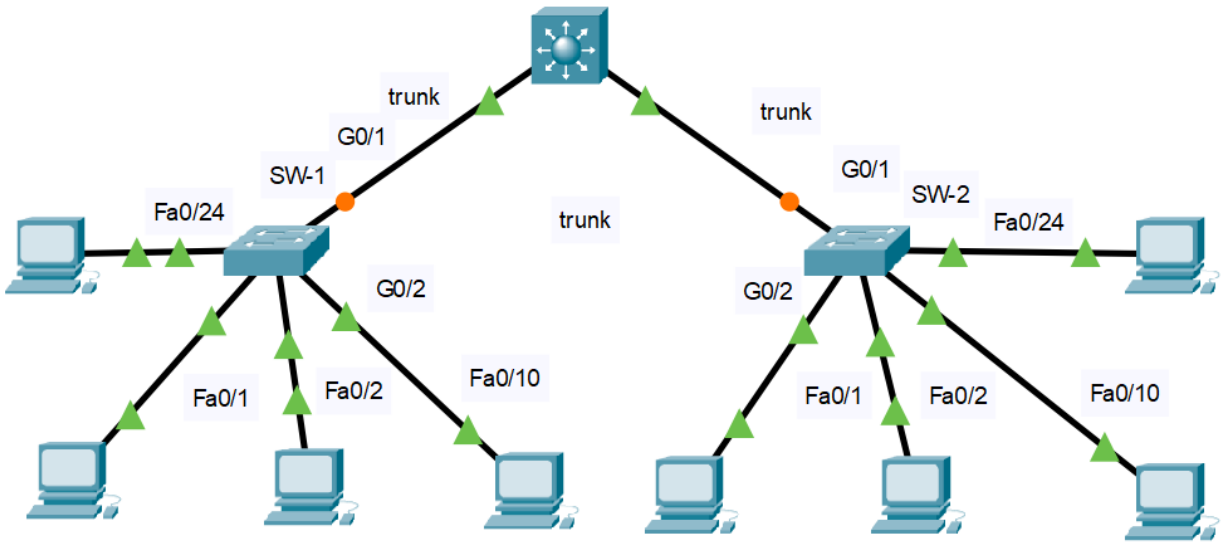


Tabla de VLAN

Switch	Número de VLAN	Nombre de la VLAN	Asociación de puertos	Red
SW-1	10	Administrador	F0/1, F0/2	192.168.10.0/24
	20	Ventas	F0/10	192.168.20.0/24
	99	Administración	F0/24	192.168.99.0/24
	100	Nativo	G0/1, G0/2	No
	999	BlackHole	Todos sin usar	Ninguna
SW-2	10	Administrador	F0/1, F0/22	192.168.10.0/24
	20	Ventas	F0/10	192.168.20.0/24
	99	Administración	F0/24	192.168.99.0/24
	100	Nativo	Ninguna	Ninguna
	999	BlackHole	Todos sin usar	Ninguna

Paso 1: Crear un troncal seguro (Secure Trunk).

a. Conecte los puertos G0/2 de los dos switches de capa de acceso.

b. Configure los puertos G0/1 y G0/2 como troncales estáticos en ambos switches.

c. Deshabilite la negociación DTP en ambos lados del enlace.

d. Cree VLAN 100 y asígnele el nombre Nativo en ambos switches

e. Configure todos los puertos troncales en ambos switches para usar la VLAN 100 como la VLAN nativa.

Paso 2: Asegure los puertos del switch no utilizados.

a. Apague todos los puertos del switch no utilizados en SW-1.

b. En SW-1, cree una VLAN 999 y asígnele el nombre Agujero Negro. El nombre configurado debe coincidir exactamente con el requisito.

c. Mueva todos los puertos de switch no utilizados a la VLAN Agujero Negro.

Paso 3: Implemente seguridad en los puertos.

a. Active la seguridad del puerto en todos los puertos de acceso activos en el switch SW-1.

b. Configure los puertos activos para permitir que se aprenda un máximo de 4 direcciones MAC en los puertos.

c. Para los puertos F0 / 1 en SW-1, configure estáticamente la dirección MAC de la PC utilizando la seguridad del puerto.

d. Configure cada puerto de acceso activo para que agregue automáticamente las direcciones MAC aprendidas en el puerto a la configuración en ejecución.

e. Configure el modo de violación de seguridad del puerto para descartar paquetes de direcciones MAC que excedan el máximo, generar una entrada de Syslog, pero no deshabilitar los puertos.

Paso 4: Configure la detección DHCP.

a. Configure los puertos troncales en SW-1 como puertos confiables.

b. Limite los puertos no confiables en SW-1 a cinco paquetes DHCP por segundo.

c. En SW-2, habilite la inspección DHCP globalmente y para las VLAN 10, 20 y 99.

Nota: La configuración de indagación DHCP puede no puntuar correctamente en Packet Tracer.

Paso 5: Configure PortFast y BPDU Guard.

a. Habilite Puerto rápido (PortFast) en todos los puertos de acceso que están en uso en SW-1.

b. Habilite BPDU Guard en todos los puertos de acceso que están en uso en SW-1.

Configure SW-2 para que todos los puertos de acceso usen PortFast de manera predeterminada.

Semana 12

Práctica integrada

Sección: ……..……..	Apellidos : ……..……
Docente : Giancarlo Condori Torres	Nombres : ……
Unidad : Unidad 3	Fecha: …../……/..... Duración: 200 min

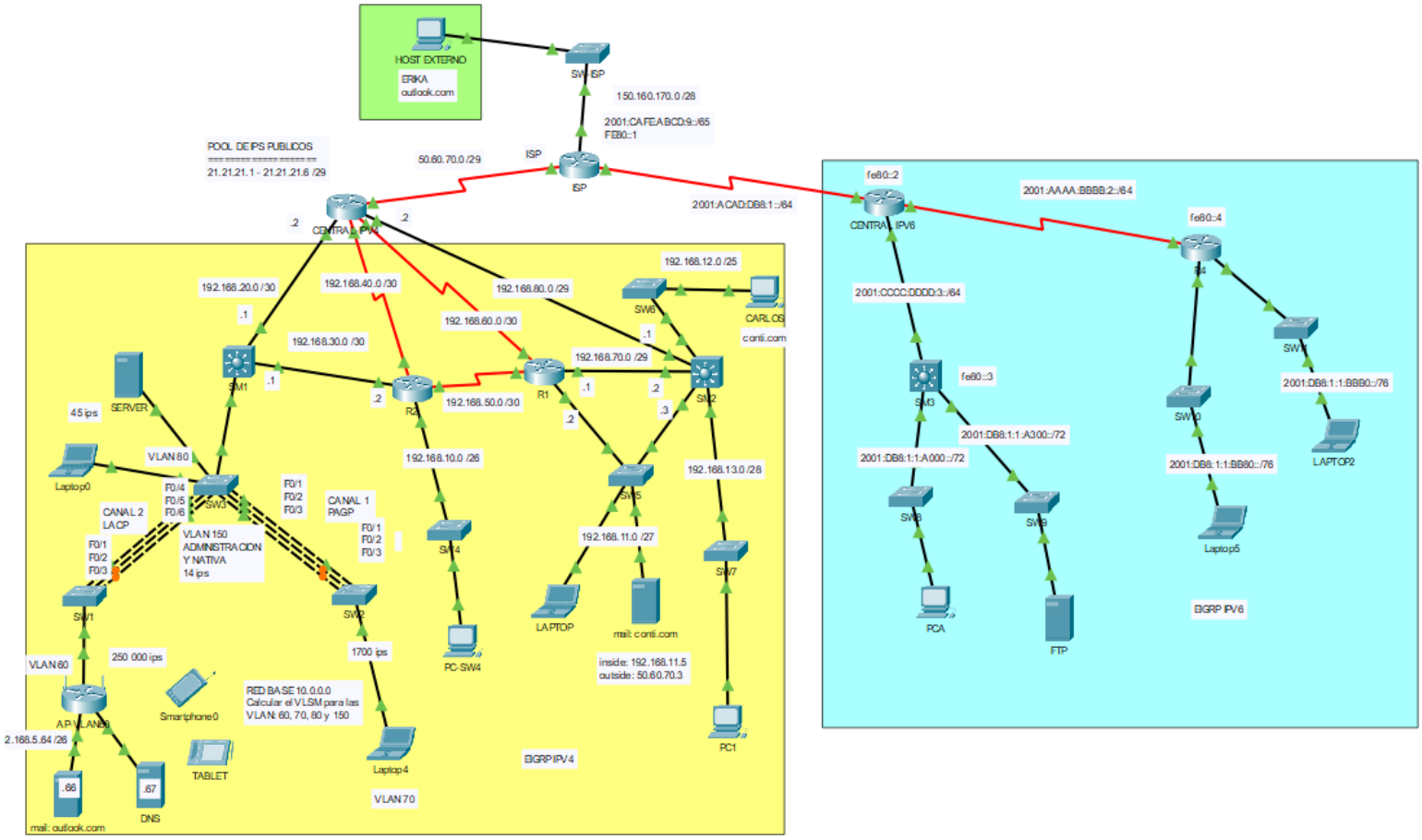
Instrucciones: Haciendo uso de los softwares packet tracer y GNS 3 resuelva los siguientes casos.

I. Propósito: El estudiante será capaz de configurar los diferentes servicios de red de manera integrada aprendidos hasta la fecha.

II. Descripción de la actividad a realizar (casos)

En esta actividad, configurará varios servicios como VLSM, vlan, enrutamiento, PVST, seguridad de puertos, etherchannel, HSRP, y servidores de red de manera integrada.

III. Procedimientos



Parte 1: Cálculo VLSM

- En base a la red 10.0.0.0 calcule el VLSM para las VLAN 60,70,80 y 150.
- Asigne el direccionamiento IP calculado a los equipos correspondientes.

Parte 2: Punto de acceso

- Configure el AP que pertenecen a la VLAN 60 con un IP de forma estática y las siguientes configuraciones
  - El SSID para el AP es “REPASO”
  - El AP debe trabajar en el estándar “N”
  - El modo de seguridad del AP debe ser “WPA2 PERSONAL” con encriptación “AES”
  - La clave de seguridad del AP debe ser “PRACTICA12345”
- Cada cliente inalámbrico debe de conectarse al AP y recibir un IP, máscara, Gateway y DNS. Los servidores hacerlos manualmente.

Parte 3: VLAN con VTP

- A través de VTP cree las VLAN 60,70,80 y 150. El switch servidor va a ser el SW3 y los otros dos, son los clientes. Los parámetros de VTP son:
  - Dominio: **practica.com**
  - Password: **class**

Puertos	Asignaciones
F0/1-f0/6 G0/1-G0/2	TRONCALES VLAN 150
F0/7-F0/10	VLAN 60
F0/11-F0/15	VLAN 70
F0/16-F0/20	VLAN 80

- Configure como puertos troncales en los tres switches según la tabla. Asegúrese que los switches clientes ya reciban las VLAN creadas en el switch servidor.

- Configure como puerto de acceso y asocie a su VLAN respectiva en los tres switches según la tabla**.**

Parte 4: Routing entre VLAN en switch multicapa

- Cree en este switch las VLAN 60,70,80 y 150

- Configure el switch multicapa SM1 para que interconecte todas las VLAN

- Es normal que los clientes inalámbricos hagan ping a los otros equipos de fuera, pero que los equipos de fuera no les hagan ping a los clientes inalámbricos. Esto es porque el AP protege a su red interna

Parte 5: Protocolo de árbol de expansión PVST + rápido

- Configure el modo de árbol de expansión rápido por VLAN para los switches del SW1, SW2, SW3 Y SM1.

- Configure el SW3 para que sea la raíz principal en la vlan 80 y 150. Configure el SW2 para que sea la raíz principal en la vlan 70, el SW1 para que sea la raíz principal en la vlan 60. El SW1 debe ser la raíz secundaria en las 3 vlans (70, 80 y 150)

Parte 6: PortFast, protección BPDU y seguridad de puertos

- Configurar portfast y su protección BPDU en el switch SW3 en las interfaces que están conectadas a los equipos finales.

- Habilitar la seguridad de puertos en el switch SW2 que conecta a la laptop con los siguientes parámetros:

- Que permita sólo dos hosts por puerto.
- Registre la dirección MAC en la configuración en ejecución.
- Si ocurre un acceso indebido al puerto, este debe de desactivarse.

Parte 7: EtherChannel

- Entre el **SW3** y el **SW2** configure etherchannel en modo PAGP con el canal 1, también configurar su interface del canal 1 en modo trunk y la vlan nativa 150.

- Entre el **SW1** y el **SW3** configure etherchannel en modo LACP con el canal 2, también configurar su interface del canal 2 en modo trunk y la vlan nativa 150.

- Verifique su resultado y que todos los equipos se deberían seguir haciendo ping.

Parte 8: Protocolo de redundancia de primer salto (HSRP)

- Configure **HSRP** en el **R1** y el **SM2** para la red 192.168.11.0 /27 con los siguientes parámetros:
  - El **R1** debe tener el 2do IP
  - El **SM2** debe tener el 3er IP
  - Para ambos equipos crear un router virtual con el grupo nro 1 y con IP virtual HSRP con el primer IP.
  - El router de reenvío o router principal va a ser **R1**
  - El router de reserva o router secundario va a ser **SM2**

- La laptop y el servidor de correo, deben de poder salir a otras redes por el router de reenvío y si falla éste, deben de salir por el router de reserva, hacer las pruebas.

Parte 9: EIGRP para IPv4

- Realizar enrutamiento EIGRP con IPv4 en la zona amarilla entre los routers que corresponda, de tal manera que todos los equipos de la zona amarilla se hagan ping. OJO: tener en cuenta las siguientes indicaciones:
  - EIGRP debe de trabajar con el número de sistema autónomo 1
  - Deshabilitar la sumarización automática
  - Todos los routers deben de tener un router id diferente a los demás
  - Anunciar las redes respectivas por routers (se recomienda sumarizar)
  - Declarar las interfaces pasivas donde corresponda.
  - Configure una ruta predeterminada conectada directamente en CENTRAL-IPV4 y propáguela en las actualizaciones de EIGRP.

Parte 10: NAT dinámico con sobrecarga

- En el router “CENTRAL-IPv4” configurar NAT dinámico con sobrecarga de tal manera que deje salir a internet a todos los equipos de la empresa. Seguir las siguientes indicaciones:
  - Crear una lista de acceso estándar que permita dar salida a todos los IP privados de la empresa hacia internet.
  - Crear un pool de ips públicos según el esquema.

  - Configurar las interfaces del router “CENTRAL-IPv4” con ip nat inside o ip nat outside según corresponda
- Al final todos los equipos deben de hacerles ping al host externo de internet
- OJO: es normal que todos los equipos de la empresa le hagan ping al host externo, pero que el host externo que se encuentran en internet no les haga ping a los equipos de la empresa.

Parte 11: Servidores DNS y CORREO con NAT estático y redireccionamiento de puertos

- Configurar el servidor de correo: conti.com con un usuario: Carlos
- Configurar el servidor de correo: outlook.com con un usuario: Erika
- Configurar la PC de Carlos como cliente del correo conti.com
- Configurar el HOST EXTERNO de Erika como cliente de correo de Outlook.com (para esto se requiere NAT estático)
- Configurar el servidor DNS para que registre los dos servidores de correo.
- Los equipos de Carlos, Erika y los servidores de correo deben de tener DNS configurado (para esto se requiere NAT estático)
- Carlos y Erika se deben de enviar correos.

Parte 12: EIGRP para IPv6

- Realizar enrutamiento EIGRP con IPV6 en la zona celeste entre los routers de R3, R4 Y CENTRAL-IPV6 de tal manera que todos los equipos de la zona celeste se hagan ping. OJO: tener en cuenta las siguientes indicaciones:
  - EIGRP debe de trabajar con el número de sistema autónomo 1
  - Todos los routers deben de tener un router id diferente a los demás
  - Configurar las interfaces pasivas donde corresponda.
  - Active EIGRP IPv6 en todas las interfaces que se requiera
  - Configure una ruta predeterminada conectada directamente en CENTRAL-IPV6 y propáguela en las actualizaciones de EIGRP.
- Verifique que todos los equipos de la zona celeste se hagan ping

Parte 13: Acceso a internet

- En el router ISP configurar rutas estáticas para IPv6 para toda la zona celestes, de tal manera que todos los equipos de la LAN de IPv6 puedan hacer ping al host externo y viceversa. De preferencia sumarizar las rutas para que sólo haiga una sola ruta estática en el router ISP

PARTE 14: Servidor FTP

- Configurar el servidor FTP con un usuario Axel, contraseña 123 y con permisos de lectura y escritura, de tal manera que cualquier equipo con IPv6 pueda acceder.

Cuarta unidad

Semana 13

Configuración de una red inalámbrica

Sección: ……..……..	Apellidos : ……..……
Docente : Giancarlo Condori Torres	Nombres : ……
Unidad : Unidad 4	Fecha: …../……/..... Duración: 70 min

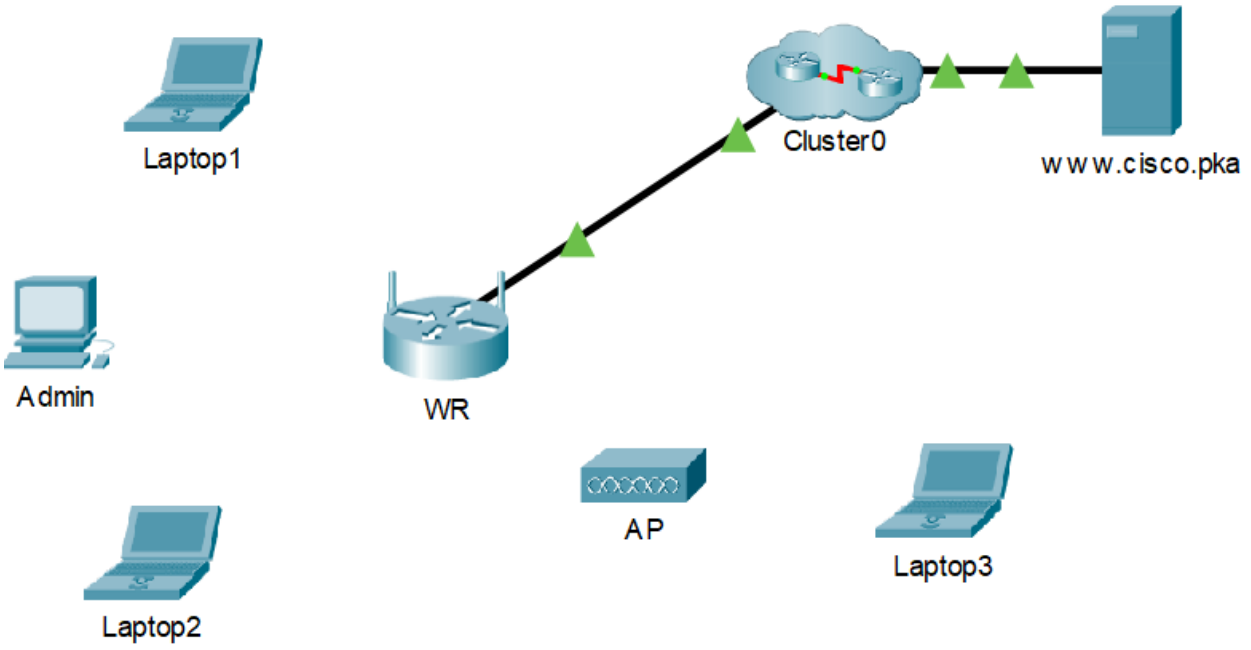
Instrucciones: Haciendo uso del software packet tracer resuelva los siguientes casos

I. Propósito: El estudiante será capaz de configurar una pequeña red inalámbrica con el software Packet tracer

II. Descripción de la actividad a realizar (casos)

Durante esta actividad, configurará un router inalámbrico y un punto de acceso para que admitan clientes inalámbricos y enruten los paquetes IP. Además, también actualizará algunas de las configuraciones predeterminadas.

III. Procedimientos



Parte 1: Conectarse a un router inalámbrico

Paso 1: Conectar el administrador a WR

a. Conecte el **administrador** a **WR** con un cable Ethernet directo a través de los puertos Ethernet. Seleccione **Conexiones** (Connections), que se representa con un rayo de tormenta y se encuentra en la parte inferior izquierda de Packet Tracer. Haga clic en **Cobre de conexión directa** (Copper Straight-Through), que se representa con una línea negra continua.

b. Cuando el cursor cambie al modo de conexión, haga clic en **Admin** y seleccione **FastEthernet0**. Haga clic en **WR** y elija un puerto Ethernet disponible para conectar el otro extremo del cable.

WR actuará como switch de los dispositivos conectados a la LAN y como router a Internet. **Admin** ahora está conectado a la LAN (**GigabitEthernet 1**). Cuando en Packet Tracer aparezcan triángulos verdes a ambos lados de la conexión entre **Admin** y **WR**, continúe con el paso siguiente.

Nota: Si no se muestran triángulos verdes, asegúrese de activar la función **Mostrar luces de enlace** (Show Link Lights) en **Opciones > Preferencias** (Options > Preferences). También puede hacer clic en **Adelantar el tiempo** (Fast Forward Time), que se encuentra arriba del cuadro de selección **Conexiones** (Connections) en la barra amarilla.

Paso 2: Configurar Admin para que use DHCP

Para acceder a la página de administración de **WR**, **Admin** debe comunicarse en la red. Generalmente, un router inalámbrico incluye un servidor DHCP y este suele estar activado de forma predeterminada en la LAN. **Admin** recibirá información de la dirección IP del servidor DHCP en **WR**.

a. Haga clic en **Admin** y seleccione la pestaña **Escritorio** (Desktop).

b. Haga clic en **Configuración IP** (IP Configuration) y seleccione **DHCP**.

¿Cuál es la dirección IP de la computadora?

¿Cuál es la máscara de subred de la computadora?

¿Cuál es la puerta de enlace predeterminada de la computadora?

c. Cierre la ventana **IP Configuration** (Configuración IP).

Nota: Los valores pueden variar dentro del intervalo de la red debido al funcionamiento normal de DHCP.

Paso 3: Conectarse a la interfaz web de WR

a. En la pestaña **Escritorio** (Desktop) en **Admin**, seleccione **Navegador web** (Web Browser).

b. Ingrese **192.168.0.1** en el campo URL para abrir la página web de configuración del router inalámbrico.

c. Use **admin** para el nombre de usuario y la contraseña.

d. En el encabezado Configuración de red (Network Setup) de la página **Configuración básica** (Basic Setup), observe el intervalo de direcciones IP para el servidor DHCP.

¿La dirección IP para el **administrador** está dentro de este rango? ¿Se espera que lo esté? Explique su respuesta.

Paso 4: Configurar el puerto Internet de WR

En este paso, **WR** está configurado para enrutar los paquetes desde los clientes inalámbricos hacia Internet. Configurará el puerto**Internet** en **WR** para conectarse a Internet.

a. En **Configuración de Internet** (Internet Setup), que se encuentra en la parte superior de la página **Configuración básica** (Basic Setup), cambie el método de dirección IP de Internet de **Configuración automática: DHCP** (Automatic Configuration - DHCP) a **IP estática** (Static IP).

b. Escriba la dirección IP que se asignará a la interfaz de Internet de la siguiente manera:

Dirección IP de Internet: 209.165.200.225

Máscara de subred: 255.255.255.252

Puerta de enlace Predeterminado: 209.165.200.226

Servidor DNS: 209.165.201.1

c. Desplácese hacia abajo en la página y haga clic en **Guardar configuración** (Save Settings).

Nota: Si recibe un mensaje de **Solicitar tiempo de espera** (Request Timeout), cierre la ventana del administrador y espere a que las luces naranjas se conviertan en triángulos verdes. Haga clic en el botón de avance rápido para acelerar el proceso. Luego , vuelva a conectarse a **WR** desde el **navegador del administrador** mediante el proceso explicado en el paso 3.

d. Para verificar la conectividad, abra un nuevo navegador web y navegue hasta el servidor **www.cisco.pka** .

Nota: La red puede demorar unos segundos en converger. Haga clic en **Adelantar el tiempo**(Fast Forward Time) o **Alt+D** para acelerar el proceso.

Parte 2: Configurar los parámetros inalámbricos

En esta actividad, usted solo configurará los parámetros inalámbricos para 2,4 GHz.

Paso 1: Configurar el SSID de WR

a. Diríjase a la interfaz GUI de **WR** en **192.168.0.1** en un navegador web en **Admin**.

b. Navegue a **Inalámbrica > Configuración inalámbrica básica** (Wireless > Basic Wireless Settings).

c. Cambie el **nombre de la red (SSID)** a **aCompany** solo para 2,4 GHz. Tenga en cuenta que los SSID distinguen entre mayúsculas y minúsculas.

d. Cambie el **canal estándar** a **6 - 2,437 GHz**.

e. Para esta actividad, desactive ambas frecuencias de 5 GHz. El resto de las configuraciones queda igual.

f. Desplácese hacia la parte inferior de la ventana y haga clic en **Guardar configuración** (Save Settings).

Paso 2: Configurar los ajustes de seguridad inalámbrica

En este paso, usted configurará las opciones de seguridad inalámbrica con el modo de seguridad WPA2 con cifrado y palabra clave.

a. Navegue a **Inalámbrica > Seguridad inalámbrica** (Wireless > Wireless Security).

b. En el encabezado 2,4 GHz, seleccione **WPA2 Personal** para el modo de seguridad.

c. Para el campo Encryption (Cifrado), deje las configuraciones **AES** predeterminadas.

d. En el campo Palabra clave (Passphrase), escriba **Cisco123!** como palabra clave.

e. Haga clic en **Guardar configuración** (Save Settings).

f. Verifique que la configuración de las páginas **Configuración inalámbrica básica**(Basic Wireless Settings) y **Seguridad inalámbrica** (Wireless Security) sean correctas y se guarden.

Paso 3: Conectar los clientes inalámbricos

a. Abra **Laptop1**. Seleccione la pestaña **Escritorio** (Desktop). Haga clic en **PC inalámbrica** (PC Wireless).

b. Seleccione la pestaña **Conectar** (Connect). Haga clic en **Actualizar** (Refresh) según sea necesario. Seleccione el nombre de red inalámbrica **aCompany**.

c. Ingrese la palabra clave configurada en el paso anterior. Escriba **Cisco123!** en el campo Clave precompartida (Pre-shared key) y haga clic en **Conectar** (Connect). Cierre la ventana PC inalámbrica (PC Wireless).

d. Abra un navegador web y verifique que pueda navegar al servidor **www.cisco.pka** .

e. Repita los pasos anteriores para conectar **Laptop2** a la red inalámbrica.

Parte 3: Conectar clientes inalámbricos a un punto de acceso

Un punto de acceso (AP) es un dispositivo que extiende la red de área local inalámbrica. Un punto de acceso se conecta a un router cableado mediante un cable Ethernet para proyectar la señal en una ubicación deseada.

Paso 1: Configurar el punto de acceso

a. Conecte **el puerto 0** del **AP** a un puerto Ethernet disponible de **WR** con un cable Ethernet directo.

b. Haga clic en **AP**. Seleccione la pestaña **Config**.

c. En el encabezado INTERFAZ (INTERFACE), seleccione **Puerto 1** (Port 1).

d. En el campo SSID, ingrese **aCompany**.

e. Seleccione **WPA2-PSK**. Escriba la palabra clave **Cisco123!**. En el campo Palabra clave (Pass Phrase).

f. Deje **AES** como el tipo de cifrado predeterminado.

Paso 2: Conectar los clientes inalámbricos

a. Abra **Laptop3**. Seleccione la pestaña **Escritorio** (Desktop). Haga clic en **PC inalámbrica** (PC Wireless).

b. Seleccione la pestaña **Conectar** (Connect). Haga clic en **Actualizar** (Refresh) según sea necesario. Seleccione el nombre de red inalámbrica **aCompany** con la señal más fuerte (canal 1) y haga clic en **Conectar** (Connect).

c. Abra un navegador web y verifique que pueda navegar al servidor **www.cisco.pka** .

Parte 4: Otras tareas

administrativas Paso 1: Cambiar la contraseña de acceso de WR

a. En **Admin**, navegue a la interfaz GUI de WR en **192.168.0.1**.

b. Navegue a **Administración > Gestión** (Administration > Management) y cambie la **contraseña del router** actual a **cisco**.

c. Desplácese hacia la parte inferior de la ventana y haga clic en **Guardar configuración** (Save Settings).

d. Use el nombre de usuario **admin** y la nueva contraseña **cisco** cuando se le indique que debe iniciar sesión en el router inalámbrico. Haga clic en **OK** (Aceptar) para continuar.

e. Haga clic en **Continuar** (Continue) y pase al siguiente paso.

Paso 7: Cambiar el intervalo de dirección de DHCP en WR

En este paso, cambiará la dirección de red interna de 192.168.0.0/24 a 192.168.50.0/24. Cuando la dirección de red LAN cambia, se deben renovar las direcciones IP de los dispositivos en las redes LAN y WLAN para que puedan recibir las direcciones IP nuevas antes de que expire la licencia.

a. Navegue a **Configuración > Configuración básica** (Setup > Basic Setup).

b. Desplácese hacia abajo en la página a **Configuración de la red** (Network Setup).

c. La dirección IP asignada a **IP del router** (Router IP) es 192.168.0.1. Cámbiela a 192.168.50.1. Verifique que la dirección IP siga iniciando a las .100 y que haya 50 direcciones IP disponibles en el pool de DHCP.

d. Agregue **209.165.201.1** como servidor DNS con la configuración de DHCP.

e. Desplácese hacia la parte inferior de la ventana y haga clic en **Guardar configuración** (Save Settings).

f. Tenga en cuenta que el intervalo de direcciones de DHCP se actualizó automáticamente para que refleje el cambio en la dirección IP de la interfaz. En el navegador web aparecerá el mensaje **Request Timeout** (Solicitud de tiempo de espera) poco tiempo después.

¿Por qué?

g. Cierre el navegador web **Admin** .

h. En la pestaña **Escritorio de Admin** (Admin Desktop), haga clic en **Petición de ingreso de comando** (Command Prompt).

i. Escriba **ipconfig /renew** para forzar a **Admin** a que vuelva a adquirir su información de IP mediante DHCP.

¿Cuál es la nueva información de dirección IP para el **administrador**?

j. Verifique que aún puede navegar al servidor **www.cisco.pka**.

k. Renueve la dirección IP de otras computadoras portátiles para verificar que aún puede navegar al servidor **www.cisco.pka**.

l. Observe que **Laptop1** se conectó al **AP** en lugar de **WR**.

¿Por qué?

Semana 14

Configuración de WLAN con WLC

Sección:	Apellidos : .....
Docente : Giancarlo Condori Torres	Nombres : .....
Unidad : Unidad 4	Fecha: ...../...../..... Duración: 70 min

Instrucciones: Haciendo uso del software packet tracer resuelva los siguientes casos

I. Propósito: El estudiante será capaz de configurar un router doméstico inalámbrico y una red basada en WLC. Implemente tanto la seguridad WPA2-PSK como la WPA2-Enterprise.

II. Descripción de la actividad a realizar (casos)

En esta actividad aplicará sus habilidades y conocimientos de WLAN configurando un router inalámbrico doméstico y un WLC empresarial. Va a implementar seguridad tanto WPA2-PSK como WPA2-Enterprise. Finalmente, conecte los hosts a cada WLAN y verifique la conectividad.

III. Procedimientos

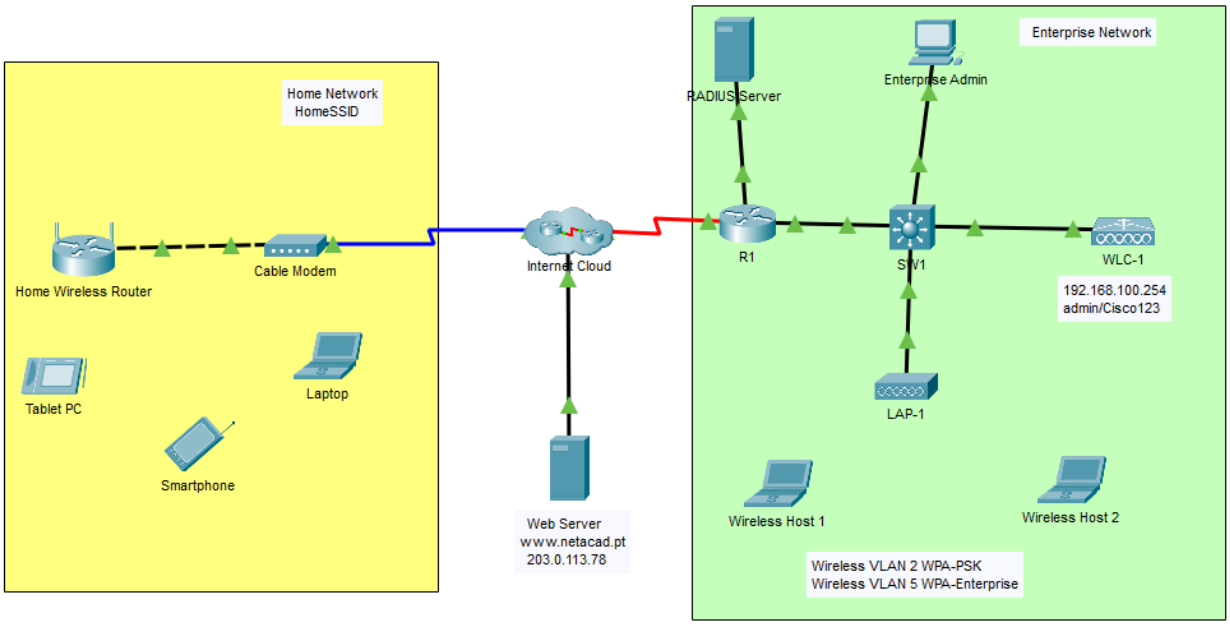


Tabla de asignación de direcciones

Dispositivo	Interfaz	Dirección IP
Router doméstico inalámbrico	Protocolo	DHCP
	LAN	192.168.6.1/27
RTR-1	G0/0/0.2	192.168.2.1/24
	G0/0/0.5	192.168.5.1/24
	G0/0/0.100	192.168.100.1/24
	G0/0/1	10.6.0.1/24
SW1	VLAN 200	192.168.100.100/24
LAB-1	G0	DHCP
WLC-1	Administración	192.168.100.254/24
Servidor RADIUS	NIC	10.6.0.254/24
Administrador de inicio	NIC	DHCP
Administrador de empresa	NIC	192.168.100.200/24
Servidor web	NIC	203.0.113.78/24
Servidor DNS	NIC	10.100.100.252
Computadora portátil	NIC	DHCP
Tablet PC	Wireless0	DHCP
Smartphone	Wireless0	DHCP
Wireless Host 1	Wireless0	DHCP
Wireless Host 2	Wireless0	DHCP

Información de la WLAN

WLAN	SSID	Servidor	Usuario	contraseña
Red doméstica	HomeSSID	WPA2-Personal	N/D	Cisco123
WLAN VLAN 2	SSID-2	WPA-2 Personal	N/D	Cisco123
WLAN VLAN 5	SSID-5	WPA-2 Enterprise	userWLAN5	userW5pass

Parte 1: Configurar un router inalámbrico doméstico.

Está instalando un nuevo router inalámbrico para la casa de un amigo. Deberá cambiar la configuración del router para mejorar la seguridad y cumplir con los requisitos de su amigo.

Paso 1: Cambiar la configuración de DHCP.

a. Abra la GUI del router inalámbrico doméstico y cambie la configuración de IP y DHCP del router según la información de la tabla de direccionamiento.

b. Permita que el router emita un máximo de **20** direcciones.

c. Configure el servidor DHCP para comenzar con la dirección IP.**3** de la red LAN.

d. Configure la interfaz de Internet del router para recibir su dirección IP a través de DHCP.

Verifica la dirección. ¿Qué dirección recibió?

e. Configure el servidor DNS estático para la dirección en la tabla de direccionamiento.

Paso 2: Configurar la LAN inalámbrica.

a. La red utilizará la interfaz LAN inalámbrica de 2.4GHz. Configure la interfaz con el SSID que se muestra en la tabla de información de LAN inalámbrica.

b. Use el **canal 6**.

c. Asegúrese de que todos los hosts inalámbricos en el hogar puedan ver el SSID.

Paso 3: Configurar la seguridad.

a. Configure la seguridad de LAN inalámbrica. Use WPA2 Personal y la frase de contraseña que se muestra en la tabla de información de LAN inalámbrica.

b. Asegure el enrutador cambiando la contraseña predeterminada al valor que se muestra en la tabla de información de LAN inalámbrica.

Paso 4: Conectar clientes a la red.

a. Abra la aplicación PC Wireless en el escritorio de la computadora portátil y configure el cliente para conectarse a la red.

b. Abra la pestaña Configuración en la Tablet PC y el teléfono inteligente y configure las interfaces inalámbricas para conectarse a la red inalámbrica.

c. Verifique la conectividad. Los hosts deberían poder hacer ping entre sí y al servidor web. También deberían poder llegar a la URL del servidor web.

Parte 2: Configurar una red de controlador WLC

Configure el controlador de LAN inalámbrica con dos WLAN. Una WLAN usará la autenticación WPA2-PSK. La otra WLAN utilizará la autenticación WPA2-Enterprise. También configurará el WLC para usar un servidor SNMP y configurará un alcance DHCP que será utilizado por la red de administración inalámbrica.

Paso 1: Configurar las interfaces VLAN.

a. Desde Enterprise Admin, navegue a la interfaz de administración WLC-1 a través de un navegador web. Para iniciar sesión en WLC-1, use **admin** como nombre de usuario y **Cisco123** como contraseña.

b. Configure una interfaz para la primera WLAN.

Name: **WLAN 2**

VLAN Identifier: **2**

Port Number: **1**

Interface IP Address: **192.168.2.254**

Máscara de Red **255.255.255.0**

Gateway: **RTR-1 G0/0/0.2 address**

Primary DHCP Server: **Gateway address**

c. Configure una interfaz para la segunda WLAN.

Nombre: **WLAN 5**

VLAN Identifier: **5**

Port Number: **1**

Interface IP Address: **192.168.5.254**

Máscara de Red **255.255.255.0**

Gateway: **RTR-1 interface G0/0/0.5 address**

Primary DHCP Server: **Gateway address**

Paso 2: Configurar un alcance DHCP para la red de administración inalámbrica.

Configure y habilite un ámbito DHCP interno de la siguiente manera:

Scope Name: **management**

Dirección de Inicio en el grupo **192.168.100.235**

Dirección Final en el grupo:**192.168.100.245**

Network: **192.168.100.0**

Máscara de Red **255.255.255.0**

Default Routers: **192.168.100.1**

Paso 3: Configurar el WLC con direcciones de servidor externo.

a. Configure la información del servidor RADIUS de la siguiente manera:

Sever Index: **1**

Sever Address: **10.6.0.254**

Shared Secret: **RadiusPW**

b. Configure el WLC para enviar información de registros a un servidor SNMP.

Nombre de la comunidad: **WLAN**

Dirección IP: **10.6.0.254**

Paso 4: Crear las WLAN.

a. Cree la primera WLAN:

Profile Name: **Wireless VLAN 2**

WLAN SSID: **SSID-2**

ID: **2**

Interface: **WLAN 2**

Security: **WPA2-PSK**

Passphrase: **Cisco123**

En la pestaña Avanzado, vaya a la sección FlexConnect. Enable **FlexConnect Local Switching** y **FlexConnect Local Auth**.

b. Cree la segunda WLAN:

Profile Name: **Wireless VLAN 5**

WLAN SSID: **SSID-5**

Interfaz: **WLAN 5**

ID: **5**

Security: **802.1x - WPA2-Enterprise**

Configure la WLAN para usar el servidor RADIUS para la autenticación.

Realice la configuración de**FlexConnect** como se hizo en el Paso 4a.

Paso 5: Configurar los hosts para conectarse a las WLAN.

Use la aplicación inalámbrica de PC de escritorio para configurar los hosts de la siguiente manera:

a. El host inalámbrico 1 debe conectarse a la VLAN inalámbrica 2.

b. Wireless Host 2 debe conectarse a Wireless VLAN 5 usando las credenciales en la tabla de información de WLAN.

Paso 6: Probar de conectividad.

Pruebe la conectividad entre los hosts inalámbricos y el servidor web mediante ping y URL.

Semana 15

Practica integrada

Sección: ……..……..	Apellidos : ……..……
Docente : Giancarlo Condori Torres	Nombres : ……
Unidad : Unidad 4	Fecha: …../……/..... Duración: 240 min

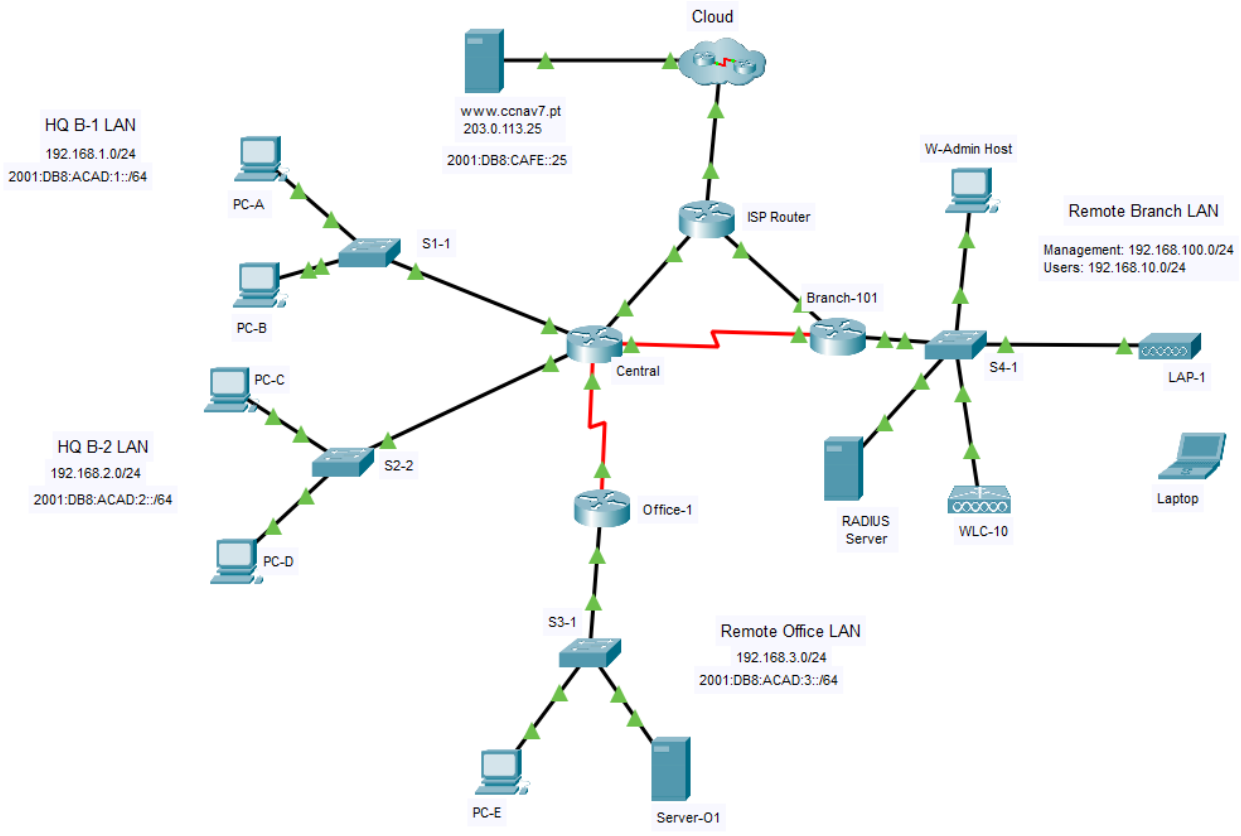
Instrucciones: Haciendo uso del software packet tracer resuelva los siguientes casos

I. Propósito: El estudiante será capaz de configurar los diferentes servicios de red de manera integrada aprendidos hasta la fecha.

II. Descripción de la actividad a realizar (casos)

En esta actividad se configurará los servicios de red: enrutamiento estático, VLAN, Switches de capa 2 y 3, FHRP, Etherchannel, PVST, DHCPv4 y DHCPv6, WLAN básico y con WLC aprendidos en todo el curso .

III. Procedimientos



Parte 1: Configurar la seguridad del conmutador

En esta parte de la evaluación configurará el conmutador **S1-1** con funciones de seguridad del conmutador. Los puertos del switch FastEthernet0/1 a FastEthernet0/5 son los puertos del switch activo. El puerto GigabitEthernet0/1 es un enlace dedicado al router Central. El resto de los puertos deben ser asegurados.

Paso 1: Configurar VLAN

un. Configure el VLA N 10 con **los usuarios de nombre.**

B. Configure el VLA N 999 con el nombre **inusitado.**

Paso 2: Configurar los puertos del conmutador activo.

En los puertos del switch activo, configure lo siguiente:

un. Configure FastEthernet 0/1 a 0/5 y GigabitEthernet 0/1 como puertos de acceso estático en el VLA N 10.

B. Active la Seguridad de puerto en los puertos.

1) Configure los puertos activos para que acepten un máximo de **4** direcciones MAC.

2) Si ocurre una violación, configure los puertos para caer las tramas de la dirección MAC desautorizada, para registrarla, y para enviar una alerta.

3) Las direcciones MAC deben estar presentes en la tabla de direcciones MAC durante un máximo de 10 minutos antes de que se eliminen.

4) Los puertos deben agregar las direcciones MAC aprendidas a la configuración corriente.

5) Configure la dirección MAC de **PC-A** como dirección estática en el puerto FastEthernet0/1.

c. Proteja contra el espionaje del DHCP.

Nota: En esta red simulada, el snooping del DHCP puede no actuar correctamente en el trazador de paquetes. Configúrelo como lo haría normalmente. Recibirá crédito completo por una configuración que cumpla con los requisitos a continuación.

1) Activar DHCP husmeando globalmente.

2) Active el snooping del DHCP para los dos VLA N que usted configuró.

3) Configure los puertos para limitar la tarifa a 5 paquetes DHCP por segundo.

4) Configure el puerto que se vincula al router como de confianza.

d. Protección contra ataques ARP mediante la implementación de DAI.

1) Activar DAI globalmente.

2) Active el DAI en los dos VLA N.

3) Configure el puerto que se vincula al router como de confianza.

E. Mitigue los ataques STP configurando el BPDUguard y PortFast en los puertos activos.

Paso 3: Asegure los puertos del conmutador no utilizados.

un. Mueva **todos los** puertos del switch no utilizados al VLA N 999.

B. Configure todos los puertos del switch no utilizados como puertos de acceso estáticos.

c. Desactive todos los puertos del conmutador no utilizados.

Parte 2: Configurar el direccionamiento y DHCP

Configurará el DHCP y el direccionamiento de la interfaz en el router Branch-101 para prepararse para implementar la red del regulador del Wireless LAN.

Paso 1: Configure y dirija una subinterfaz para la red de usuario wlan.

un. Configure la subinterfaz 10 en la interfaz del router que está conectada con el Switch S4-1.

B. El router debe proporcionar el encaminamiento del router-en-un-palillo al VLA N 10.

c. Configure la subinterfaz con el direccionamiento de la tabla de direccionamiento.

Paso 2: Configure a un pool dhcp para la red de usuario de la red inalámbrica (WLAN).

un. Excluya la dirección de la interfaz del router y la dirección de administración del WLC.

B. Configure a un pool del DHCP que sea utilizado por los hosts que están conectando con la red inalámbrica (WLAN).

1) Nombre los **WLAN-anfitriones de**lapiscina.

2) Configure el grupo para utilizar direcciones en la red 192.168.10.0/24.

3) El grupo también debe proporcionar la puerta de enlace predeterminada y las direcciones del servidor DNS.

Paso 3: Configurar una interfaz como cliente DHCP.

En branch-101, configure la interfaz que está conectada con el router ISP para recibir su dirección sobre el DHCP.

Parte 3: Configurar rutas estáticas

En esta parte de la evaluación, configurará rutas estáticas, predeterminadas, estáticas flotantes y de host tanto en IPv4 como en I Pv6. Usted configurará el Central y el Routers Branch-101. Netacad PLC

ha decidido que quiere utilizar el enrutamiento estático entre todas sus redes. Además, la compañía quiere utilizar los links Ethernet entre el Routers para la mayoría del tráfico de datos y reservar el link serial entre central y Branch-101 para los propósitos de backup en caso de que uno de los links de Ethernet llegue a ser inasequible. Configurará rutas estáticas y predeterminadas flotantes.

Paso 1: Configure las Static rutas en central.

un. Configure las rutas predeterminadas del IPv4 a la nube usando el link de Ethernet como el link preferido y el link serial como el respaldo flotante. Utilice una distancia administrativa de **10** para la ruta de reserva. Estas rutas se deben configurar como rutas directamente conectadas. Â

Nota: Las interfaces Ethernet darán una advertencia cuando están configuradas sin un direccionamiento del next-hop. Â En esta configuración, la interfaz es punto a punto, así que la advertencia puede ser ignorada.

B. Configure las Static rutas del IPv4 a la red de usuario de la red inalámbrica (WLAN) lan de la rama remota siguiendo las mismas guías de consulta que arriba para el tipo de ruta y la distancia administrativa.

c. Configure una ruta de host IPv4 en Central al Servidor-O1 en la LAN de oficina remota. Cree una ruta conectada directamente.

Nota: Con el fin de esta evaluación, introduzca por favor las Static rutas del IPv4 en la orden siguiente:

1) Ruta predeterminada de IPv4

2) Ruta predeterminada flotante IPv4

3) Ruta del host IPv4

4) Static ruta del IPv4 a la lan de la rama remota

5) Static ruta flotante del IPv4 a la LAN de la rama remota

d. Asegúrese de que el dispositivo esté configurado para rutear el IPv6.

E. Configure las rutas predeterminadas de IPv6 a la nube. Utilice el link Ethernet como la ruta primaria, y el link serial como el respaldo flotante. Utilice una distancia administrativa de **10** para la ruta de reserva. Estas rutas deben especificar la dirección de la interfaz del próximo salto.

F. Configurar una ruta de host IPv6 en Central al Servidor-O1 en la LAN de oficina remota Debe ser una ruta de próximo salto.

Nota: Con el fin de esta evaluación, ingrese por favor las Static rutas del IPv6 en la orden siguiente:

1) Ruta predeterminada de IPv6

2) Ruta predeterminada flotante de IPv6

3) Ruta del host IPv6

Paso 2: Configure las Static rutas en branch-101.

Branch-101 también debe configurarse con rutas estáticas a las otras tres redes de la red Netacad PLC. Requerirá rutas estáticas y predeterminadas flotantes en IPv4 e IPv6 siguiendo las mismas directrices que se usaron para las rutas estáticas centrales.

- o Las rutas IPv6 utilizan argumentos de dirección de próximo salto.
- o Las rutas IPv4 utilizan argumentos de interfaz de salida.
- o Todas las rutas deben preferir los enlaces Ethernet sobre el enlace serie.
- o Las rutas flotantes de reserva utilizan una distancia administrativa de 10.

un. Configure las rutas predeterminadas del IPv4 a la nube usando el link ethernet como el link preferido y el link serial como el respaldo.

Nota: Con el fin de esta evaluación, introduzca por favor las Static rutas del IPv4 en la orden siguiente:

1) Ruta predeterminada de IPv4

2) Ruta predeterminada flotante IPv4

B. Asegúrese de que el dispositivo esté configurado para rutear el IPv6.

c. Configurar las rutas predeterminadas de IPv6 a la nube. Utilice el link Ethernet como la ruta primaria, y el link serial como respaldo. Utilice una distancia administrativa de **10** para la ruta de reserva. Estas rutas deben especificar la dirección de la interfaz del próximo salto.

Nota: Con el fin de esta evaluación, ingrese por favor las Static rutas del IPv6 en la orden siguiente:

1) Ruta predeterminada de IPv6

2) Ruta predeterminada flotante de IPv6

Parte 4: Configurar una LAN inalámbrica mediante un controlador de LAN inalámbrica

En esta parte de la evaluación, configurará el controlador de LAN inalámbrica para proporcionar acceso inalámbrico a la red. El nombre de usuario y la contraseña son el **admin/admin** predeterminado. Conecte con el WLC sobre el HTTPS con la interfaz de administración.

Paso 1: Configure una interfaz VLAN.

un. Cree una nueva interfaz y asígnela el nombre **WLAN 10.** La interfaz debe utilizar el **VLAN10** y el puerto físico **1.**

B. Utilice la información de la tabla de direccionamiento para configurar los valores de direccionamiento de la interfaz. La interfaz utilizará a un pool dhcp que se configure en la subinterfaz que se asigne al VLA N 10 en el router Branch-101.

Paso 2: Configure a un servidor de RADIUS.

un. Configure el WLC con el direccionamiento del IPv4 del servidor de RADIUS.

B. Utilice un secreto compartido de **RADsecret**.

Paso 3: Configurar una LAN inalámbrica.

un. Cree una nueva red inalámbrica (WLAN). Asígnelo **el nombre WLAN 10** y configure el SSID como **SSID-10.**

B. La LAN inalámbrica debe utilizar la interfaz VLAN que se configuró previamente.

c. Configure la red inalámbrica (WLAN) para utilizar la directiva de seguridad WPA2 y la Administración de claves de autenticación dot1x.

d. Configure la red inalámbrica (WLAN) para utilizar al servidor de RADIUS que fue configurado previamente para autenticar a los usuarios de red inalámbrica.

E. Abra la lengueta avanzada y navegue hacia abajo a las secciones de Flexconnect. Active el Switching local de FlexConnect y el Auth local de FlexConnect.

F. Verifique que la red inalámbrica (WLAN) esté configurada y operativa.

Paso 4: Configurar un ámbito DHCP para la red de administración.

Configure un nuevo ámbito DHCP para ser utilizado por los revestimientos y otros dispositivos de administración en la red.

un. Asigne al ámbito DHCP el nombre **Wired_Admin**.

B. Inicie el ámbito en la dirección **192.168.100.240.** Finalice el ámbito en la dirección 192.168.100.249.

c. Otra información que se requiere se puede encontrar en la tabla de direccionamiento.

Paso 5: Configurar un servidor SNMP.

Configure a un servidor SNMP para recibir los desvíos del WLC.

un. Utilice el nombre de comunidad **branch-wireless**.

B. Utilice **172.16.1.100** como la dirección del servidor.

Paso 6: Configurar el host inalámbrico.

Configure la computadora portátil para conectar con la red inalámbrica (WLAN).

un. Cree un nuevo perfil inalámbrico en el host. Utilice el nombre **red de trabajo** para el perfil.

B. Configure el perfil para el SSID de la red inalámbrica (WLAN).

c. Utilice la autenticación de empresa con un nombre de usuario de **user1** y una contraseña de user**1Pass.**

d. Cuando haya terminado, haga clic en **Conectar a la red**. Tomará tiempo para que se establezca la conexión.

Lista de Referencias

Básica

Cisco NetWorking Academy (2021). *Curso CCNA v7*. Switching, Routing, and Wireless Essentials. [Consulta 03 de agosto de 2021]. https://www.netacad.com

Alicia, P. (2020) Cisco CCNA v7 curso práctico. Pearson Education, Inc.

Complementaria

Wendell, O. (2020) CCNA 200-301 Official Cert Guide, Volumen 1 y 2. Publicaciones Altaria, S.L.

Allan, J. (2020) 31 Day Before your CCNA Exam. Cisco System, Inc.