Proyecto Final

El mejor proyecto del mundo

ITESO

Universidad Jesuita
de Guadalajara

Maestro/a: Elsa Julieta Cedillo Elías

Nombre: José Luis Almendarez González

Materia: Interconexión De Redes

Tabla de contenido

Introducción

En este proyecto final vamos a emplear todos los protocolos de las practicas que hemos hecho anteriormente, como podrían ser las rutas dinámicas de vector distancia (RIP) y estado enlace (OSPF), Vlans, NATs de distintos tipos y ejercicios lógicos como la segmentación de redes.

La manera en la que se dividirá este reporte primero con el índice o tabla de contenidos. Después la introducción que como estamos viendo hablara brevemente del contenido del reporte para después continuar con la zona más cargada; el desarrollo.

En el desarrollo lo primero que haremos será explicar los protocolos que utlizamos, su funcionamiento, configuración y detalles.

Una vez explicado definidamente los procedimientos y protocolos empleados mostraremos un diagrama del trabajo final explicado. Explicaremos la segmentación de redes, bajo qué criterios se realizó y se mostrara la tabla de segmentación de redes.

Una vez mostrada la evidencia teórica tendremos que mostrar la evidencia práctica, se verán las configuraciones de cada protocolo para mostrar un ejemplo de configuración en el CLI. Así como se harán ciertas pruebas que comprobarán la funcionalidad individual de cada dispositivo.

Desarrollo

Materiales

- Cisco Packet tracer

Parte 1-. Segmentación de la red

Antes de configurar cualquier protocolo para que esto sea efectivo necesitamos identificar a nuestro dispositivo a través de ips, mascaras subred y una topología física lógica. Tenemos distintas demandas en esta sección pues para cada LAN necesitamos una máscara de red distinta para diferenciar red de otra aparte su respectiva red ip. Después de hacer la segmentación se creó esta tabla:

El mejor proyecto del mundo				
Dispositivo	Interfaz	Direccion Ip	Mascara de red	Gateway
ACL				
Router0	Serial0/1/0	172.16.16.5	255.255.255.252	N/A
	Serial0/1/1	172.16.16.1	255.255.255.252	N/A
Router2	Serial0/1/0	172.16.16.6	255.255.255.252	N/A
	Serial0/1/1	172.16.16.10	255.255.255.252	N/A
Router1	Serial0/1/0	172.16.16.9	255.255.255.252	N/A
	Serial0/1/1	172.16.16.2	255.255.255.252	N/A
Lan 1				
PC0	FastEthernet0	10.10.9.130	255.255.255.192	10.10.9.129
Switch1	FastEthernet0/1	10.10.9.128	255.255.255.192	N/A
	GigabitEthernet0/1	10.10.9.128	255.255.255.192	N/A
Router0	GigabitEthernet0/0/0	10.10.9.129	255.255.255.192	N/A
Lan 2				
PC1	FastEthernet0	10.10.8.2	255.255.255.0	10.10.8.1
Switch2	FastEthernet0/1	10.10.8.0	255.255.255.0	N/A
	GigabitEthernet0/1	10.10.8.0	255.255.255.0	N/A
Router0	GigabitEthernet0/0/1	10.10.8.1	255.255.255.0	N/A
Lan 3				
PC2	FastEthernet0	10.10.9.194	255.255.255.224	10.10.9.193
Switch3	FastEthernet0/1	10.10.9.192	255.255.255.224	N/A
	GigabitEthernet0/1	10.10.9.192	255.255.255.224	N/A
Router 2	GigabitEthernet0/0/0	10.10.9.193	255.255.255.224	N/A
Lan 4				
Server0	FastEthernet0	10.10.9.2	255.255.255.128	10.10.9.1
Switch0	FastEthernet0/1	10.10.9.0	255.255.255.128	N/A
	GigabitEthernet0/1	10.10.9.0	255.255.255.128	N/A
Router1	GigabitEthernet0/0/0	10.10.9.1	255.255.255.128	N/A
Lan 5				
Router 4	GigabitEthernet0/0/1	192.168.0.1	255.255.255.0	N/A
Switch4	FastEthernet0/1	192.168.0.0	255.255.255.192	N/A
	FastEthernet0/2	192.168.0.0	255.255.255.192	N/A
	FastEthernet0/3	192.168.0.64	255.255.255.192	N/A
	FastEthernet0/4	N/A	N/A	N/A
	GigabitEthernet0/1	192.168.0.0	255.255.255.0	N/A
	GigabitEthernet0/2	N/A	N/A	N/A
Switch5	FastEthernet0/1	192.168.0.64	255.255.255.192	N/A
	FastEthernet0/2	192.168.0.128	255.255.255.192	N/A

	FastEthernet0/3	192.168.0.128	255.255.255.192	N/A
	GigabitEthernet0/1	N/A	N/A	N/A
Switch6	FastEthernet0/1	192.168.0.128	255.255.255.192	N/A
	FastEthernet0/2	192.168.0.0	255.255.255.192	N/A
	GigabitEthernet0/1	N/A	N/A	N/A
Vlan10				
PC3	FastEthernet0	192.168.0.2	255.255.255.192	192.168.0.1
PC4	FastEthernet0	192.168.0.3	255.255.255.192	192.168.0.1
Server1	FastEthernet0	192.168.0.4	255.255.255.192	192.168.0.1
Vlan20				
PC5	FastEthernet0	192.168.0.65	255.255.255.192	192.168.0.1
PC6	FastEthernet0	192.168.0.66	255.255.255.192	192.168.0.1
Vlan30				
Laptop0	FastEthernet0	192.168.0.130	255.255.255.192	192.168.0.1
PC7	FastEthernet0	192.168.0.129	255.255.255.192	192.168.0.1
PC8	FastEthernet0	192.168.0.131	255.255.255.192	192.168.0.1
OSPF				
Router2	Serial0/2/0	172.16.16.17	255.255.255.252	N/A
	Serial0/2/1	172.16.16.13	255.255.255.252	N/A
	GigabitEthernet0/0/1	10.10.9.193	255.255.255.224	N/A
Router4	Serial0/1/0	172.16.16.18	255.255.255.252	N/A
	Serial0/1/1	172.16.16.22	255.255.255.252	N/A
Router3	Serial0/1/0	172.16.16.21	255.255.255.252	N/A
	Serial0/1/1	172.16.16.14	255.255.255.252	N/A
Ruteo Estatico				
Router3	GigabitEthernet0/0/0	172.16.16.29	255.255.255.252	N/A
	GigabitEthernet0/0/1	172.16.16.25	255.255.255.252	N/A
Router5	GigabitEthernet0/0/0	172.16.16.26	255.255.255.252	N/A
	GigabitEthernet0/0/1	172.16.0.1	255.255.255.0	N/A
	Serial0/1/0	172.16.16.33	255.255.255.252	N/A
Router6	GigabitEthernet0/0/0	172.16.16.30	255.255.255.252	N/A
	GigabitEthernet0/0/1	200.0.0.1	255.255.255.240	N/A
	Serial0/1/0	172.16.16.34	255.255.255.252	N/A
Otras Lans				
Lan 6				
Switch8	FastEthernet0/1	172.16.0.0	255.255.255.0	N/A
	FastEthernet0/2	172.16.0.0	255.255.255.0	N/A
	FastEthernet0/3	172.16.0.0	255.255.255.0	N/A
	GigabitEthernet0/1	172.16.0.0	255.255.255.0	N/A
PC9	FastEthernet0	172.16.0.10	255.255.255.0	172.16.0.10
PC10	FastEthernet0	172.16.0.20	255.255.255.0	172.16.0.10
PC11	FastEthernet0	172.16.0.30	255.255.255.0	172.16.0.10
Lan 7				
Switch7	FastEthernet0/1	200.0.0.0	255.255.255.240	N/A

	FastEthernet0/2	200.0.0.0	255.255.255.240	N/A
	GigabitEthernet0/1	200.0.0.0	255.255.255.240	N/A
PC12	FastEthernet0	200.0.0.3	255.255.255.240	200.0.0.1
Server2	FastEthernet0	200.0.0.2	255.255.255.240	200.0.0.1

Además, como instrucción de la parte 1 tenemos que implementar la configuración básica en cada router o switch de la red, esto significa que tenemos que establecer una contraseña para la línea de la consola, para el modo administrador, tenemos que encriptar ambas para reforzar la seguridad de los dispositivos y finalmente tenemos que dejar un mensaje de bienvenida en el dispositivo.

Para hacer lo de las contraseñas de la línea de consola primero tenemos que entrar a la interfaz a través del modo administrador en el dispositivo, ahí vamos a aplicar el comando password [Contraseña] y lo vamos a confirmar con el comando login.

Para hacer lo del modo administrador debemos usar el comando enable secret [contraseña] y no habría muchos pasos después de eso.

Para encriptarlo tenemos que usar el comando service password-encryptation y para casi finalizar agregamos el mensaje de bienvenida con el comando banner motd #mensaje#. Finalmente guardamos la configuración con el comando copy running-config startup-config.

Parte 2-. Estático y Dinámico

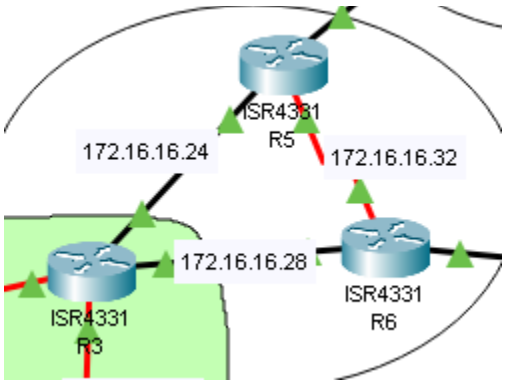
Los primeros protocolos que deberíamos de implementar serían los protocolos el protocolo de ruteo, que consisten en ruteo estático y dinámico(ospf, rip).

El protocolo de ruteo estático es un protocolo que consiste en que tenemos que decirle al router el nombre de la red ip que estamos buscando, su mascara de red para identificarla y a través de que vía vamos a contactar a esta red, en este caso la vía es el puerto del router conectado a través del gigabitEthernet. Configurar este protocolo es sumamente sencillo pues que solo se ocupa un comando, cual es:

ip route [nombre de la red] [mascara de la red] [siguiente salto]

```
R5#show ip route static
     172.16.0.0/16 is variably subnetted, 13 subnets, 3 masks
S       172.16.16.28/30 [1/0] via 172.16.16.25
                        [1/0] via 172.16.16.34
     200.0.0.0/24 is variably subnetted, 2 subnets, 2 masks
S       200.0.0.0/28 [1/0] via 172.16.16.34
```

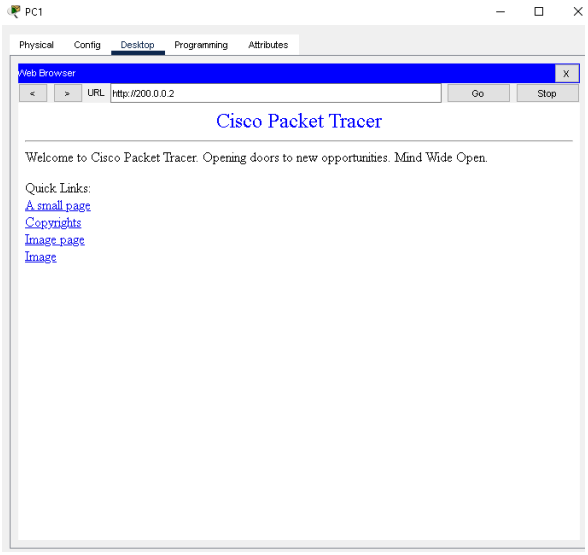
En este caso los que configuramos con la ruta estática son los router 3,5 y 6 como indicamos en la imagen.



En el router 5 aquí podemos ver las rutas conectadas directamente de manera estática. Al ser un router conectado a 2 distintos router podemos ver como incluso hay 2 vías distintas para alcanzar a la red.

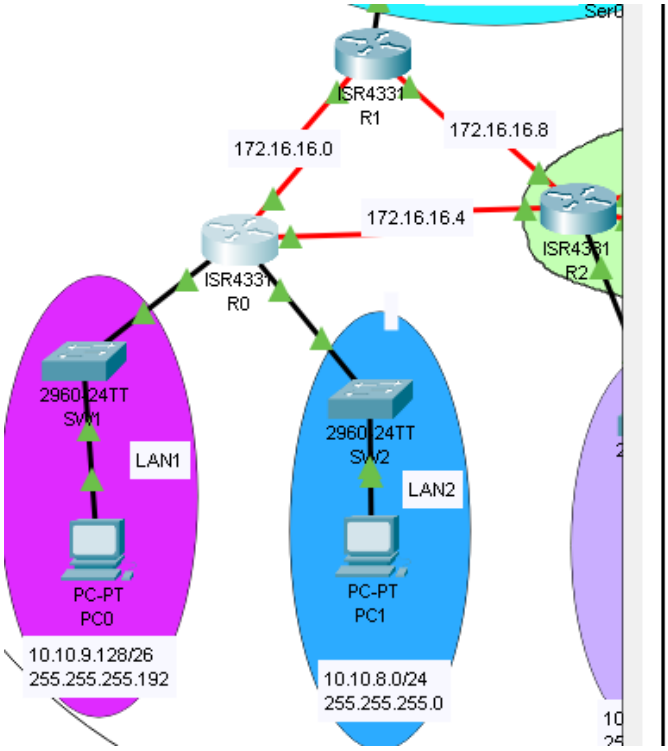
Mas adelante el router 3 compartiría protocolo de enrutamiento con ospf pero eso lo exploraremos más adelante en el reporte.

Otra cosa que se nos pidió aparte de la redundancia implícita y la segmentación que también da comportamientos específicos fue que la LAN 7 tenga un servidor que todos los computadores puedan acceder desde cualquier lado de la red, como podemos ver en esta imagen.



La siguiente configuración con la que tenemos que estar enfocados en la red son las conexiones dinámicas cuyas vamos a dividir en ospf y en rip.

Las rip las vamos a configurar en los routers 0, 1 y 2. cómo podemos ver en la imagen. Para poder configurar es bastante sencillo, puesto que es un protocolo de vector-distancia y como sabemos únicamente tenemos que poner las redes a las que el router es adyacente




```
!
interface Vlan1
 no ip address
 shutdown
!
router rip
 version 2
 network 10.0.0.0
 network 172.16.0.0
 no auto-summary
!
ip classless
!
ip flow-export version 9
!
!
!
banner motd ^CJose Almen
!
!
!
!
!
line con 0
 password 7 0822455D0A16
 login
!
line aux 0
!
line vty 0 4
 login
```

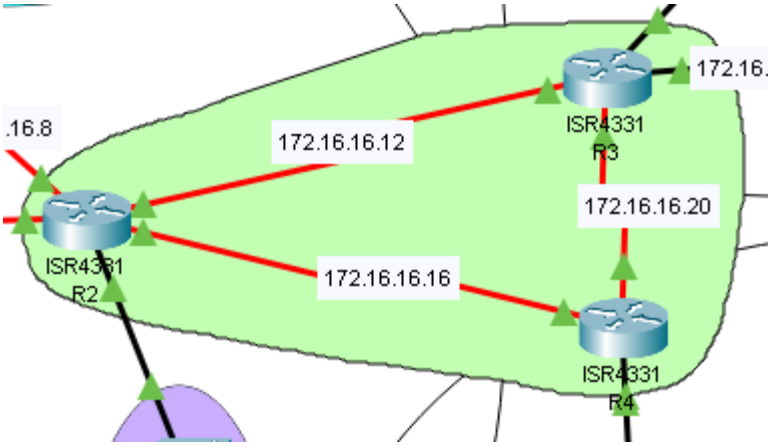
Como podemos ver en la imagen el router 0 está configurado con rip y tenemos vinculadas las dos redes esenciales para poder conectar tanto las lans como las conexiones con los routers.

Para poder configurar el protocolo rip lo que tenemos que hacer es entrar al modo administrador y entrar a la interfaz del protocolo con el comando router rip, después seleccionamos la version 2 con su comando homónimo, para evitar confusiones con el enrutamiento tenemos que poner el comando no auto-summary. Después ya podemos establecer nuestras conexiones, con el comando network [red adyacente]. Esto lo repetimos en todos los routers hasta que justamente la redundancia haga que todos estén comunicados.

Finalmente, lo único que nos quedaría configurar para la parte 2 sería la parte del enrutamiento dinámico por medio de ospf. Cual es un protocolo de estado enlace, lo que significa que usa el algoritmo de Dijkstra

Lo que hace este algoritmo es que dentro de una misma zona comunica todos los routers y se conecta con otros routers a través de routers adyacentes llamados abr nos sirve como entrada y salida de información, lo que nos permite segmentar un poco más este enrutamiento. Lo que siempre es bueno para el control de nuestra red.

Como podemos ver en el esquema los routers que usaremos para configurar esto serán el router 2, 3 y 4. Como podemos observar tanto como el router 2 como el 3 repiten algoritmo. Solo es una anotación para decir que no hay problema de comunicación. Al contrario, lo que esto permite es que todos los routers se puedan conectar entre sí.

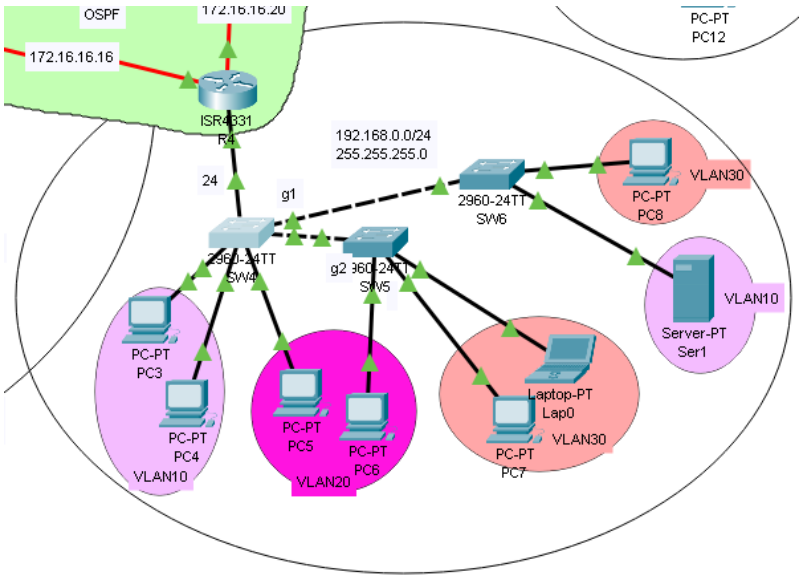


Para configurar ospf lo que tenemos que hacer es entrar al modo configuración y después de hacer eso usamos el comando router ospf 1 y ya podemos declarar rutas, tanto como el rip lo que tenemos que declarar son las ips adyacentes. Es importante que para que se comuniquen correctamente al menos en esta situación todas tienen que estar en la misma área, hecho eso incluso desde un router podemos ver todas las conexiones del área en la tabla de enrutamiento como podemos ver en el ejemplo. Para todo esto usamos el comando network [ip adyacente][wildcard][area].

```
R3#show ip route ospf
     10.0.0.0/8 is variably subnetted, 5 subnets, 5 masks
O       10.10.9.192 [110/65] via 172.16.16.13, 01:39:38, Serial0/1/1
     172.16.0.0/16 is variably subnetted, 14 subnets, 3 masks
O       172.16.16.16 [110/128] via 172.16.16.22, 01:39:38, Serial0/1/0
                     [110/128] via 172.16.16.13, 01:39:38, Serial0/1/1
O    192.168.1.0 [110/65] via 172.16.16.22, 02:16:44, Serial0/1/0
O    192.168.2.0 [110/65] via 172.16.16.22, 02:16:44, Serial0/1/0
O    192.168.3.0 [110/65] via 172.16.16.22, 02:16:44, Serial0/1/0
```

Parte 3-. Vlans

Lo siguiente que tenemos que hacer para que todas las configuraciones queden establecidas en nuestros dispositivos es establecer las vlan como se indica en el siguiente diagrama:



Como podemos ver esta configuración vlan consta de 3 vlans conectadas a través de distintos switches. Que están conectados a un router por el cual la configuración es efectiva. Esto es una pequeña descripción de los 3 pasos que tenemos que hacer, que son:

- Establecer las vlans y su conexión con el switch
- Establecer en los switches el modo trunk de configuración
- Hacer que haya una conexión entre vlans a través del puerto.

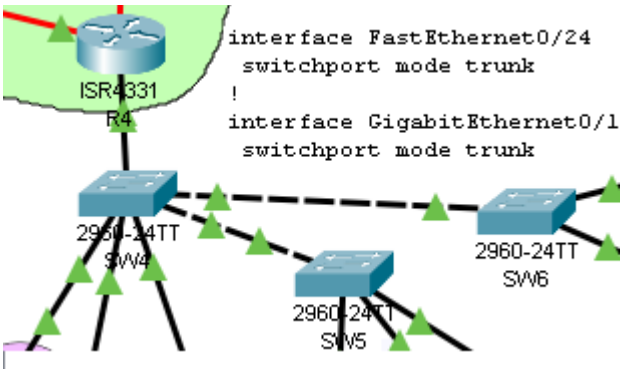
Para lo primero establecemos nuestras ip en su respectiva topología lógica. Donde la vlan10 va a pertenecer a 192.168.1.0; la vlan20 pertenecerá a la 192.168.2.0 y la vlan 30 a la 192.168.3.0.

Una vez en nuestro switch tenemos que crear las vlan, esto lo hacemos entrando al modo administrador, después el de configuración y escribimos el comando vlan [id] para entrar a la interfaz, dentro de esa interfaz asignamos un identificador en código ASCII, es decir le ponemos un nombre a la vlan. Esto lo hacemos con el comando name [nombre]. Así creamos la vlan. Después lo que haremos es asignar la vlan al respectivo puerto.

En este caso lo que tenemos que hacer es en el modo de configuración entrar a la interfaz del puerto que queremos configurar como podría ser interface fastEthernet 0/24. Después activamos el acceso del puerto con el comando switchport mode Access y establecemos la vlan que queremos asignar a ese puerto con el comando switchport Access vlan [id]. Una vez hecho eso ya vamos a poder conectar los dispositivos de la vlan a su respectivo puerto. Aquí un ejemplo de cómo se debería ver.

```
.
interface FastEthernet0/1
 switchport access vlan 10
!
interface FastEthernet0/2
 switchport access vlan 10
!
interface FastEthernet0/3
 switchport access vlan 20
```

El siguiente paso de la configuración es que debemos establecer el modo trunk en los switches ya que varios switches tienen más de una vlan conectada. Realmente es muy sencillo, solo le tenemos que indicar al switch porque puerto estará recibiendo la información de distintas vlan para que pueda hacer la gestión. Esto lo hacemos entrando al modo configuración, entrando la interfaz del puerto que queremos configurar y usamos el comando switchport mode trunk. Aquí tenemos que pensar es en que puerto configurar eso. Pondré como ejemplo a mi configuración del switch 4.



Aquí lo propio es configurarlo en el gigabitEthernet y en los fastEthernet conectados a los dispositivos, como podría ser el fastEthernet 0/24 y el gigabitEthernet 0/1. De igual manera ahí podemos ver dos configuraciones cuando está conectado a 3 dispositivos importantes, esto es porque en el gigabitEthernet 0/2 del switch 5 esto ya está configurado y solo necesitamos la configuración de manera unidireccional.

Finalmente, como cereza del pastel solo nos falta que todas las vlans se puedan comunicar entre sí y por supuesto que esta información pueda salir del router. En pocas palabras vamos a hacer que el

router 4 tenga 3 distintas ips asignadas. Como había comentado cada vlan tiene su propia ip y para que esto funcione correctamente también debe tener su default Gateway único en la red. Para esto seleccionamos el puerto de la interfaz a la que está conectada el switch, pero ponemos un ".[id]" al final como podemos ver en la imagen. Esto nos va a llevar a una subinterfaz de la red que con el comando encapsulation dot1Q [vlan id] vamos a poder asignar una ip única. Esto lo repetimos la misma cantidad de veces de vlans que tenemos y finalmente para que la información salga de aquí, configuramos nuestro protocolo dinámico con las ips que ya definimos anteriormente. Como había dicho en un principio al configuramos 3 ips dentro del mismo puerto del router.

```
interface GigabitEthernet0/0/0
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0/0/0.10
 encapsulation dot1Q 10
 ip address 192.168.1.1 255.255.255.0
!
interface GigabitEthernet0/0/0.20
 encapsulation dot1Q 20
 ip address 192.168.2.1 255.255.255.0
!
interface GigabitEthernet0/0/0.30
 encapsulation dot1Q 30
 ip address 192.168.3.1 255.255.255.0
!
.
router ospf 4
 log-adjacency-changes
 network 172.16.16.16 0.0.0.3 area 1
 network 172.16.16.20 0.0.0.3 area 1
 network 192.168.0.0 0.0.0.255 area 1
 network 192.168.2.0 0.0.0.255 area 1
 network 192.168.3.0 0.0.0.255 area 1
 network 192.168.1.0 0.0.0.255 area 1
'
```

Parte 4-. NATs

Para el tema de las nat tenemos que hacer 2 configuraciones distintas, una nat estática para la LAN 6 y una nat dinámica para la LAN 7.

Para la nat estática es muy sencillo todo lo que queremos hacer es traducir las ips que tenemos en las lans a una ip publica entonces en el router que es nuestro default Gateway vamos al modo de configuración y usamos el comando ip nat inside source static [ip] [mascara de red], dejando en claro a que ip queremos hacer la traducción. Después de eso nos dirigimos a las interfaces conectadas para declarar las instrucciones de entrada y de salida. En el caso del router6 que sería el que configuraríamos para esto tenemos que seleccionar las interfaces y usar el comando ip nat [inside/outside] para declarar de qué lado van a llegar las ips que tenemos que traducir y por donde las va a traducir y mandar. Y debería quedar como en la siguiente imagen.

```
interface GigabitEthernet0/0/0
 ip address 200.0.0.1 255.255.255.240
 ip nat inside
 duplex auto
 speed auto
interface Serial0/1/0
 ip address 172.16.16.34 255.255.255.252
 ip nat outside
 clock rate 2000000
 speed auto
```

Lo siguiente que seguiría seria configurar la nat en el router 5 ya que es el correspondido para la LAN 7.

Para configurar la nat dinámica primero tenemos que asignar el inside y el outside la traducción como lo hicimos anteriormente, después vamos a hacer una access-list que tenga una lista de las direcciones fuente internas que se traducirán. Con el comando access-list 1 permit [ip][mascara de red]. Después implementaremos la nat dinámica con el comando ip nat pool [nombre] [1era ip] [ultima ip] netmask [mascara de red]. Esto lo que es como su nombre lo indica es un pool de donde la nat dinámica puede escoger para traducir. Para finalizar, usamos el comando ip nat inside source list 1 pool [nombre] para declarar quien vamos a usar ese pool para traducir y que el protocolo inicie. Y algo así debería quedar.

```
ip nat pool POOL1 172.16.0.1 172.16.0.254 netmask 255.255.255.0
ip nat inside source list 1 pool POOL1
```

Parte 5-. ACLs

Finalmente tenemos que configurar las listas de control de acceso, como nosotros ya sabemos estas listas sirven para brindar una mejorar seguridad y también un mejor control de flujo de datos. Realmente para esto es muy sencillo pues lo único que ocupamos hacer es restringir el acceso al servidor de la LAN 4. entonces eso significa que ocupamos una acl extendida.

Para configurar esto nos vamos al modo de configuración dentro del router que queremos modificar. En mi caso el router 1 y dentro de config t usamos el comando access-list 100, de 100 a 199 las acl son extendidas. Para configurar una acl extendida el formato es:

Access-list 100 [permit/deny] [protocolop] [ip seleccionada][wild-card][match][ip objetivo] [puerto][protocolo].

Esto puede variar dependiendo de lo que estemos buscando, de igual manera es la naturaleza de la acl pues al final de cuenta no son más que un montón de instrucciones.

Para esta instrucción en específico el resultado sería:

```
R1#show access-lists
Extended IP access list 100
    10 permit tcp 10.10.9.128 0.0.0.63 host 10.10.9.2 eq www (6 match(es))
    20 permit tcp 200.0.0.0 0.0.0.15 host 10.10.9.2 eq www (5 match(es))
    30 permit tcp 172.16.0.0 0.0.0.255 host 10.10.9.2 eq www (5 match(es))
```

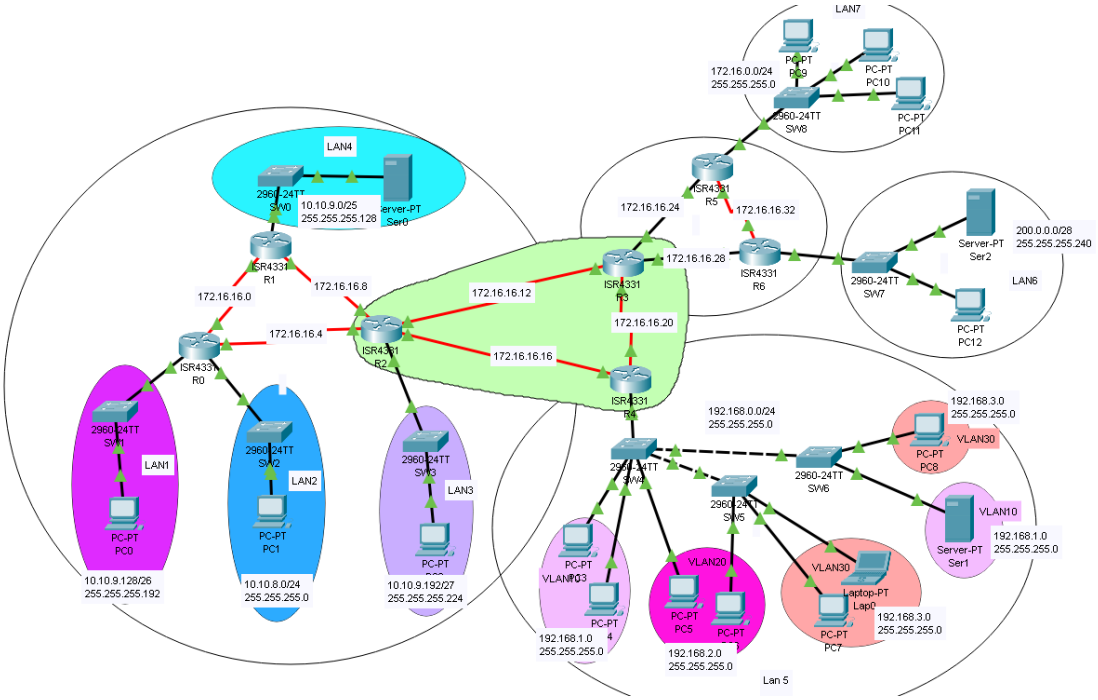
Como podemos ver en ip seleccionada ponemos el nombre entero de la red, esto porque la LAN entera va a tener autorización sobre la instrucción.

Para finalizar solo tenemos que asignar esto a un puerto de entrada o salida como si fuera el portero de un antro.

En este caso lo vamos a configurar por conveniencia más que nada todo en el router 1, donde en el puerto que está conectado al switch lo vamos a seleccionar y vamos a usar el comando access-group 100 out, asignado estas instrucciones a este puerto en específico.

Extra

Antes de continuar con las pruebas de que todo funcione correctamente primero quería mostrar el diagrama completo.



Pruebas

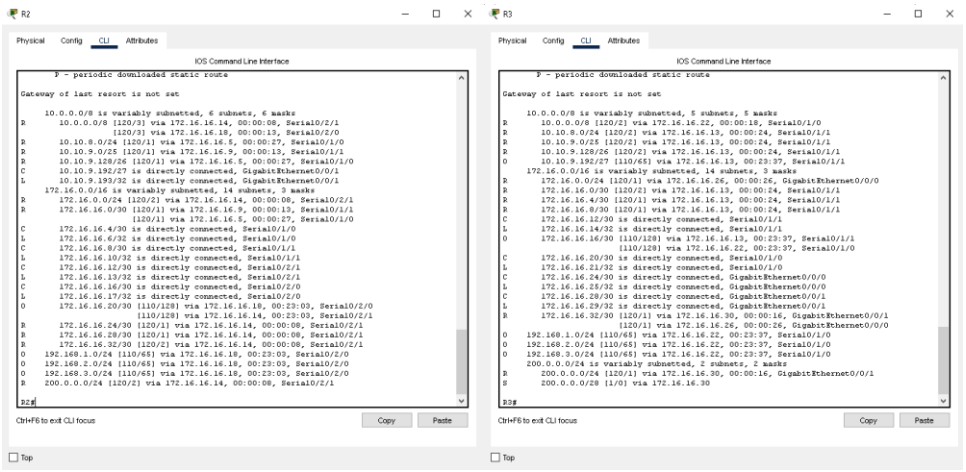
Segmentación de la red

Acerca de esta parte no sé qué más agregar la manera de verificar y hacer pruebas es revisando la tabla de segmentación, así como el diagrama de segmentación anexado anteriormente en el documento.

Estático y Dinámico

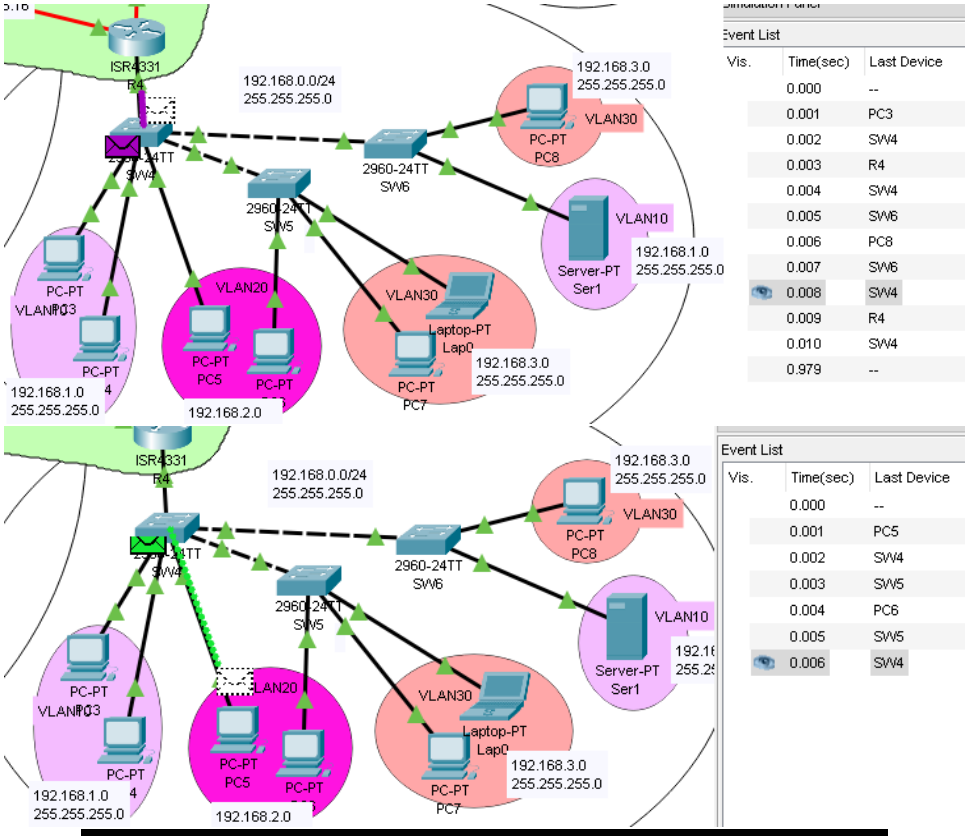
La mejor manera de comprobar que si funciona las rutas es haciendo un ping entre distintos dispositivos de la red y mostrando la ip route de los routers, en este caso estamos mostrando la tabla de ruteo del router 2 y 3. Ya que esos son los que comparten protocolo.

Successful	PC0	PC8	ICMP		0.000	N	0	(edit)	(delete)
Successful	PC1	R5	ICMP		0.000	N	1	(edit)	(delete)
Successful	R5	PC4	ICMP		0.000	N	2	(edit)	(delete)
Successful	Ser1	R1	ICMP		0.000	N	3	(edit)	(delete)



Vlans

Gracias a las siguientes imágenes podemos observar la comunicación entre mismas y distintas vlans, además de comprobar gracias al tracert de una computadora de la LAN 1 que demuestra que toda la información puede entrar y salir del enredado sistema de las vlan. También podemos observar que para distintas vlans se comunican a través de las subinterfaces de los routers mientras que para la misma solo se pasan la información a través de los switches.




```
Tracing route to 192.168.1.2 over a maximum of 30 hops:

  1    0 ms      0 ms      0 ms      10.10.9.129
  2    0 ms      0 ms      1 ms      172.16.16.6
  3    1 ms      1 ms      1 ms      172.16.16.18
  4    7 ms      0 ms      6 ms      192.168.1.2

Trace complete.

Tracing route to 192.168.2.4 over a maximum of 30 hops:

  1    0 ms      0 ms      0 ms      10.10.9.129
  2    5 ms      0 ms      1 ms      172.16.16.6
  3    22 ms     1 ms      5 ms      172.16.16.18
  4    0 ms      1 ms      1 ms      192.168.2.4

Trace complete.
```

NATs

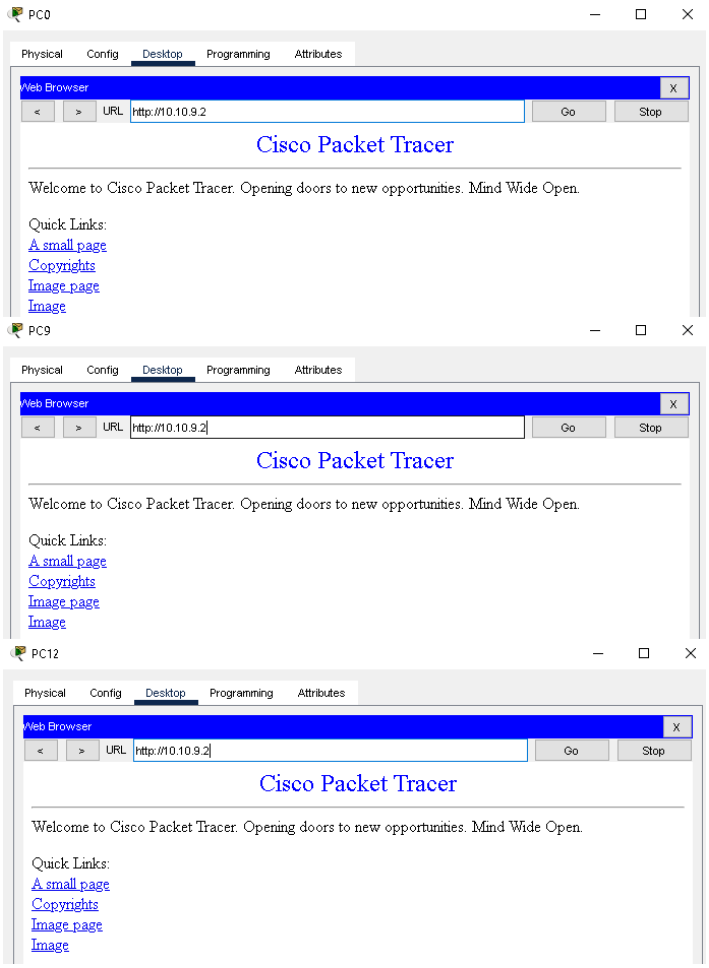
En estos screenshot que tome podemos observar cómo tanto la nat dinámica y la nat estática ya están integrada en sus respectivos routers.

```
-- Inside Source
access-list 1 pool POOL1 refCount 0
 pool POOL1: netmask 255.255.255.0
       start 172.16.0.1 end 172.16.0.254
       type generic, total addresses 254 , allocated 0 (0%), misses 0
```

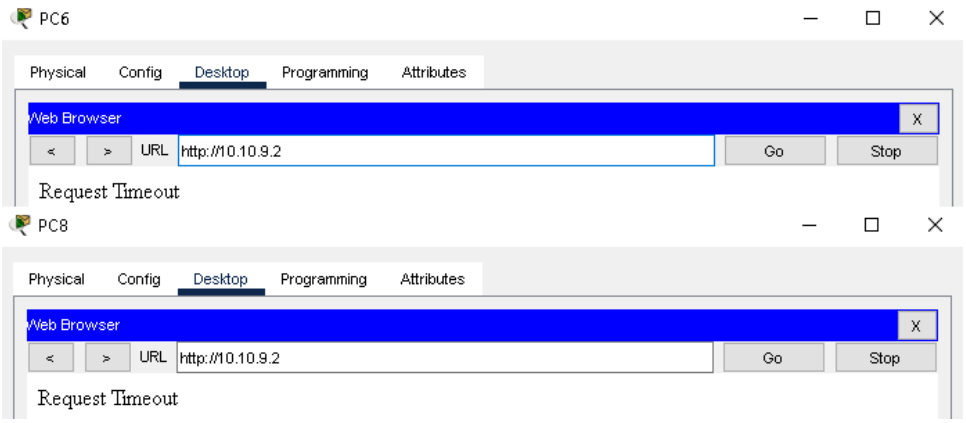
```
Total translations: 0 (0 static, 0 dynamic, 0 extended)
Outside Interfaces: Serial0/1/0
Inside Interfaces: GigabitEthernet0/0/0
Hits: 0  Misses: 191
Expired translations: 0
Dynamic mappings:
```

ACLs

La parte de ACL nos pide que tan solo las LAN 1,6 7 y aquí están los Screenshots de que pueden llegar al servidor.



Mientras otros pc que no pertenecen a estas lans no pueden llegar a él.



Conclusión

Un proyecto largo sin duda alguna, en el momento que escribo esto aún tengo que corregir la redacción de ciertas partes para hacerlo más claro. Sin embargo, me alegra poder terminarlo. Sin duda todos los protocolos que vimos me los imagino usándolos en nuestra vida diaria cuando diseñamos o trabajemos con una red. Entonces es muy importante que nos encontramos cómodos trabajando con estos protocolos y métodos de configuración.

La verdad es que aún me quede con unas dudas acerca de la NAT pero después de la presentación espero poder preguntárselas. Todo lo demás acerca de la segmentación, la ACL, el ruteo o las VLAN me quedo totalmente claro. Ese sería mi proyecto maestra espero tenga todo lo requerido y fue un gusto poder haber tomado el curso con usted, si nos encontramos en una materia de redes en el futuro estaré gustoso de ser su estudiante.

Referencias

- *Configurar NAT estatico en dispositivos Cisco | Pasos para configurar NAT Cisco - ManageEngine Network Configuration Manager*. (s. f.). Manage Engine. Recuperado 7 de mayo de 2022, de https://www.manageengine.com/latam/network-configuration-manager/configuracion-de-nat-estatico-dispositivos-cisco.html
- Fernández, R. P. (2021, 30 marzo). *Configuración de VLANs en Packet Tracer*. Ingeniero Técnico Industrial Mecánico & Administrador de Sistemas. Recuperado 5 de mayo de 2022, de https://www.raulprietofernandez.net/blog/packet-tracer/configuracion-de-vlans-en-packet-tracer