Manual de Proyecto

CONFIGURACIÓN DE VLAN VOZ + DATOS

REQUERIMIENTOS

- Segmentar físicamente la red.
- Segmentar lógicamente (subnetting).
- Vlan de datos.
- Vlan de voz.
- Vlan de administración.
- Port security al menos dos acciones.
- DHCP AGREGAR DNS Y TIEMPO DE CONCESIÓN.

  (Necesitamos un router para DHCP que reparta ips a cada router por vlan, si tenemos un máximo de 4 vlans podemos usar un servidor, en caso de usar por router hay que hacer uso de IPHELPER, investigar su uso.)
- Crear al menos dos servicios en un servidor.

  (Necesitamos un VTP server, cliente y transparente aunque raramente se usa el transparente.)
- Desarrollar modos VTP en su topología.
- Crear dos usuarios para SSH (Admin, usuario restringido).
- Enrutamiento (Estático y/o dinámico).

SEGMENTACIÓN FÍSICA DE LA RED.

La segmentación física en redes implica dividir la infraestructura física de la red en segmentos separados y distintos. Esto se hace mediante la separación física de dispositivos de red, como switches, routers y cables, para crear redes más pequeñas y manejables.

La segmentación física puede incluir la creación de subredes separadas utilizando dispositivos de red dedicados, como switches VLAN-capaces, que permiten aislar tráfico en diferentes puertos o VLANs físicamente separadas. También puede implicar el uso de routers para dividir la red en dominios de broadcast separados o la implementación de firewalls físicos para controlar el flujo de datos entre segmentos.

SEGMENTACIÓN LÓGICA (SUBNETTING).

Implica separar los equipos de forma orientada a un mundo real, a modo de acomodar salones u oficinas.

La segmentación lógica es una técnica utilizada en redes de computadoras para dividir el tráfico de red en segmentos más pequeños, basados en protocolos o servicios específicos. Implica separar el

flujo de datos en capas superiores del modelo OSI, como la capa de aplicación o la capa de transporte.

Esta técnica se usa para mejorar el rendimiento, la seguridad y la gestión de la red. Al dividir la red en segmentos lógicos, se pueden aplicar políticas de seguridad y administración de forma más eficiente, permitiendo un control más preciso sobre cómo fluyen y se manejan los datos.

VLAN DE DATOS, VOZ Y ADMINISTRACIÓN.

- **VLAN de datos:** Está destinada al tráfico de datos generales. Incluye dispositivos como computadoras, servidores y dispositivos de almacenamiento conectados a la red para intercambiar información, correos electrónicos, navegación web, entre otros.
- **VLAN de voz:** Se dedica al tráfico de voz sobre IP (VoIP). Aquí se incluyen dispositivos como teléfonos IP y sistemas de comunicación de voz. Al separar el tráfico de voz, se puede priorizar para garantizar calidad y baja latencia en las llamadas.
- **VLAN de administración:** Esta VLAN es para los dispositivos de administración de red, como switches, routers, puntos de acceso inalámbrico, cámaras de seguridad IP, etc. La segmentación permite un control más seguro y eficiente de estos dispositivos.
-

PORT SECURITY

Cuando se habilita el port security en un switch, se pueden configurar reglas para cada puerto, como la cantidad máxima de direcciones MAC permitidas, las direcciones MAC específicas que pueden acceder al puerto o la acción a tomar si se detectan direcciones MAC no autorizadas (como deshabilitar el puerto o enviar una notificación).

Cuando un dispositivo se conecta a una red que utiliza DHCP, el servidor DHCP puede proporcionar la dirección de uno o más servidores DNS. Estos servidores DNS traducen nombres de dominio a direcciones IP, permitiendo a los dispositivos acceder a recursos en la red utilizando nombres en lugar de direcciones IP.

El tiempo de concesión es el período durante el cual un dispositivo tiene asignada una dirección IP por el servidor DHCP. Este tiempo se especifica en la configuración del servidor DHCP y puede variar desde unos minutos hasta días o más. Al finalizar el tiempo de concesión, el dispositivo debe renovar su asignación de dirección IP o liberarla.

SERVICIOS DE SERVIDOR.

1. **Servidor DHCP:** Puedes configurar un servidor DHCP en un router o switch para asignar direcciones IP automáticamente a dispositivos en la red.
2. **Servidor DNS:** Puedes utilizar un servidor DNS para resolver nombres de dominio en direcciones IP. Puedes configurar esta función en un router o utilizar un servidor dedicado.

3. **Servidor Web:** Puedes simular un servidor web utilizando un PC o un servidor, configurando aplicaciones como HTTP Server o FTP Server en el dispositivo para permitir el acceso a páginas web o transferencias de archivos.
4. **Servidor de Archivos:** Puedes configurar un PC o un servidor para compartir archivos en la red, permitiendo a otros dispositivos acceder y almacenar datos en ese servidor.
5. **Servidor de Correo Electrónico:** Puedes simular un servidor de correo electrónico utilizando un PC o un servidor y configurando aplicaciones de servidor de correo electrónico como SMTP o POP3.

VTP EN SU TOPOLOGÍA.

VTP (Protocolo de Trunking VLAN) es utilizado para propagar automáticamente la información de configuración de VLAN a través de una red. En Packet Tracer, se puede configurar VTP en switches para propagar información sobre VLAN de manera centralizada.

`vtp mode [server/client/transparent]`.

SSH (CREACIÓN DE USUARIOS Y CONFIGURACIÓN DE PERMISOS).

En Packet Tracer, la configuración detallada de SSH, la creación de usuarios y la gestión de permisos no es tan completa como en entornos de red reales o en simuladores más avanzados.

En Packet Tracer, la limitación de la configuración de SSH y la gestión de usuarios se debe a que es una herramienta de simulación diseñada para ofrecer un entorno básico y educativo de redes. Por lo tanto, no todas las funcionalidades avanzadas de dispositivos reales están disponibles. Algunas de las limitaciones incluyen:

1. **Complejidad de las características:** Herramientas de simulación como Packet Tracer están diseñadas para proporcionar una representación simplificada de dispositivos de red. Funciones avanzadas como la gestión de usuarios, la autenticación detallada y las configuraciones complejas de seguridad (como autorización granular) pueden no estar completamente implementadas o disponibles.
2. **Dispositivos compatibles:** No todos los dispositivos en Packet Tracer admiten SSH. En versiones anteriores, por ejemplo, se incluían modelos de switches y routers específicos que permitían la configuración de SSH. En versiones más recientes como la 7.9, puede variar, y algunos switches y routers pueden admitir la configuración de SSH, mientras que otros no.
3. **Limitaciones de simulación:** Packet Tracer no proporciona todas las funcionalidades que encontrarías en un entorno de red real. Algunas configuraciones avanzadas, detalles específicos o características de dispositivos pueden no estar disponibles para ser configuradas o probadas.

ENRUTAMIENTO.

El enrutamiento, ya sea estático o dinámico, se refiere a cómo se determina la mejor ruta para enviar datos a través de una red.

Enrutamiento Estático:

- **Configuración manual:** En el enrutamiento estático, los administradores de red configuran manualmente las rutas en los dispositivos de red. Esto significa que cada ruta debe ser introducida y mantenida manualmente en cada dispositivo.
- **Rutas estáticas:** Se especifica la ruta exacta hacia una red específica, indicando el próximo salto (próximo router) que debe utilizarse para alcanzar esa red.
- **Menos adaptable:** No se ajusta automáticamente a cambios en la topología de la red. Si hay cambios en la red, como la caída de un enlace, el administrador debe actualizar manualmente las rutas.

Enrutamiento Dinámico:

- **Automatización:** Utiliza protocolos de enrutamiento para intercambiar información de manera automática entre los dispositivos de red. Los routers intercambian información sobre la red para determinar la mejor ruta.
- **Actualización automática:** Se ajusta a cambios en la red de manera automática. Cuando se produce un cambio en la topología de la red, como la caída de un enlace, los routers intercambian información y recalculan las rutas automáticamente.
- **Más escalable:** Ideal para redes grandes y en constante cambio, ya que reduce la carga administrativa al adaptarse automáticamente a cambios en la red.

Dada la red, su distancia y pequeña complejidad, usaremos el enrutamiento dinámico ya que es más adecuado para redes más grandes y dinámicas, donde la automatización y la adaptabilidad son esenciales.

Se estará trabajando la siguiente dirección de IP:

192.168.20.0/24 para la Data.

10.10.10.0/24 para voz.

192.200.100.0 para IP’s publicas.

PASOS A REALIZAR

1. Diseño de la red
2. Configuraciones básicas para todos los dispositivos aplicando ssh en los routers y los switches.
3. VLANs configurando a todos los equipos y agregando modo trunk en los puertos 12 y 13.
4. Switchport-security.
5. Subnnetting e Ip addressing.
6. OSPF en los routers y switches.
7. IP Statica para el cuarto de servidores.

8. DHCP Sserver configuraciones.
9. Inter-VLAN routing en los switches plus ip dhcp helper addresses.
10. Configuraciones de red inalambrica.
11. Configuración del servicio de telefonía.
12. ACL para SSH.
13. PAT + Access Control List.
14. Site-to-Site IPsec VPN + ACL.

REQUERIMIENTOS

- **Herramienta de trabajo.-** Se usará la herramienta de trabajo Cisco Packet Tracer para diseñar e implementar las soluciones de Red.
- **Diseño Jerarquico.-** Se usará un diseño jerarquico para proveer redundancia en cada nivel.
- **ISPs .-** Se espera que la red este conectada en almenos 2 IPS's para proveer redundancia y permitir la conexión entre cada Router.

  Esta arquitectura ofrece tanto redundancia como capacidad de gestión de tráfico para asegurar la disponibilidad y el rendimiento de la red, lo que es crucial, especialmente en entornos empresariales donde la conectividad ininterrumpida es fundamental.

  - **Agregación o consolidación de tráfico:** Recibe el tráfico de múltiples ubicaciones o proveedores y lo canaliza hacia un servidor o red central para procesamiento adicional.
  - **Mayor capacidad de procesamiento:** Puede manejar grandes volúmenes de tráfico provenientes de diferentes ubicaciones o proveedores antes de enviarlos a su destino final.
  - **Redundancia:** Si uno de los proveedores de internet falla, el otro puede mantener la conexión activa, asegurando que la red no se interrumpa por completo.
  - **Balanceo de carga:** Distribuir el tráfico entre los proveedores para mantener un mejor rendimiento o evitar la congestión en una sola conexión.
- **WIFI.-** Cada departeamento necesita de una red inalambrica para permitir la conexión entre usuarios.
- **VoIP.-** Cada departamente tendra que tener telefonos IP y tendrán que poder comunicarse entre ellos.
- **VLAN.-** Cada departamento tendrá que estar en su respectiva VLAN y diferente sub-red ajena a los demás departamentos.
- **SUBNETTING .-** Asignar el numero correcto de direcciones para cada departamento.
- **CONFIGURACIONES BÁSICAS.-** Configurar cosas básicas como el hostname, contraseñas, mensajes de banner, encriptar contraseñar y deshabilitar IP domain lookup.
- **Inter-VLAN Routing.-** Los dispositivos de cada departamento deben de poder comunicarse unos con otros con el respectivo switch de capa 3 configurado para ese propósito.

- **Core Switches.-** Los switches de capa 3 se espera que hagan tanto las funcionalidades de routing como switching y se les asignara una dirección IP.
- **DHCP Server.-** Todos los dispositivos en la red (excepto los telefonos) obtendran una IP de forma dinamica del servidor dedicado a DHCP.
- **Cisco Router.-** Exigentemente el router debe soportar el servicio de telefonía.
- **Static Addressing.-** Los dispositivos en el “cuarto” de servidor tendrán direcciones IP estáticas.
- **Servicio de Telefonía.-** Se configurará el VoIP en el gateway router.
- **Routing Protocol.-** Se usará OSPF como protocolo de enrutamiento para anunciar rutas tanto en los routers como en los switches multicapa.
- **Security Port.-** Se buscara que solo un dispositivo este conectado a un puerto de switch, además se usará el método sticky para obtener las direcciones MAC y poder ofrecer un mejor modo de violación en modo de shutdown.
- **SSH.-** Se configurará el SSH en todos los routers y los switches correspondientes para el login.
- **Standart ACL for SSH.-** El uso más común es Por ejemplo, podrías configurar un ACL estándar para SSH en un router o firewall para permitir el tráfico SSH solo desde una dirección IP específica o un rango de direcciones IP autorizadas, limitando así quién puede acceder a los dispositivos de red a través de SSH. Esto ayuda a proteger los dispositivos de posibles intentos de acceso no autorizados o ataques desde direcciones IP no permitidas.
- **NAT + ACL.-** Se configurará el PAT con esa combinación. Esta combinación es útil para administrar el flujo de datos, proteger la red contra posibles amenazas y definir políticas de acceso específicas para diferentes tipos de tráfico, todo ello mientras se mantiene la conectividad eficiente de los dispositivos en la red.
- **IPsec VPN + ACL.-** Se configurará la VPN site-to-site IPsec entre el servidor de sede y el router border. Esta combinación es útil para administrar el flujo de datos, proteger la red contra posibles amenazas y definir políticas de acceso específicas para diferentes tipos de tráfico, todo ello mientras se mantiene la conectividad eficiente de los dispositivos en la red.

  Un ejemplo es; ACLs pueden trabajar en conjunto con NAT para permitir o denegar ciertos tipos de conexiones antes o después del proceso de traducción de direcciones. Por ejemplo, puedes configurar un ACL para permitir el tráfico SSH solo desde ciertas direcciones IP después de que se haya realizado la traducción de direcciones utilizando NAT.

CONFIGURACIÓN BÁSICA

```
#REPETIR EN TODOS LOS SWITCHES RELACIONADOS A LAS AREAS DE TRABAJO
RH-SW(config)#enable password cisco

RH-SW(config)#line console 0
RH-SW(config-line)#password cisco
RH-SW(config-line)#login
RH-SW(config-line)#exit
```

```
RH-SW(config)#banner motd #NO UNAUTHORISED ACCESS#
RH-SW(config)#NO IP domain-lookup
```

Para el ssh es necesario que tanto routers como switches lleven consigo la configuración básica.

```
Switch(config)#ip domain-name cisco.com
Switch(config)#crypto key generate rsa
% Please define a hostname other than Switch.
Switch(config)#hostname HQ-SW1
HQ-SW1(config)#crypto key generate rsa
The name for the keys will be: HQ-SW1.cisco.com
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

HQ-SW1(config)#
*mar. 2 10:36:36.702: %SSH-5-ENABLED: SSH 1.99 has been enabled
HQ-SW1(config)#ip ssh version 2

HQ-SW1(config)#LINE VTY 0 15
HQ-SW1(config-line)#LOGIN LOCAL
HQ-SW1(config-line)#transport input ssh
HQ-SW1(config-line)#exit
HQ-SW1(config)#do wr
```

Este comando accede a la configuración de las líneas de terminal virtual (VTY) que se utilizan para el acceso remoto al dispositivo. El rango de 0 a 15 indica que estás configurando las 16 sesiones VTY disponibles (en la mayoría de los dispositivos Cisco).

Las líneas VTY son las interfaces de red virtuales a través de las cuales puedes iniciar sesión en un dispositivo de red de manera remota.

Este comando configura las líneas VTY para utilizar la base de datos de nombres de usuario y contraseñas locales del dispositivo para la autenticación.

Esto significa que cuando alguien intenta conectarse al dispositivo de forma remota, se le pedirá que proporcione un nombre de usuario y contraseña que estén configurados localmente en el dispositivo.

Si queremos que los usuarios accedan con el nivel máximo de privilegio basta con los siguientes comandos.

```
username [username] privilege 15 secret [password]
line vty 0 15
```

```
 login local
 transport input ssh
```

VLANS (DATA Y VOZ)

SE TRABAJARÁ EL MODO TRUNK EN LOS PUERTOS 1 Y 2

YA QUE SE TRABAJARAN MULTIPLES VLANS POR MULTIPLES PERSONAS NECESITAMOS EL MODO TRUNCAL EN LAS MISMAS.

```
RH-SW(config)#vlan 10
RH-SW(config-vlan)#name DATA
RH-SW(config-vlan)#vlan 120
RH-SW(config-vlan)#name VOICE

#MODO TRUNCAL
RH-SW(config)#int range fa0/1-2
RH-SW(config-if-range)#switchport mode trunk

#ACCESS INTERFACES
RH-SW(config)#int range fa0/3-24
RH-SW(config-if-range)#switchport mode access

#CONFIGURACIÓN DE "DATA" PARA QUE LA INFORMACIÓN VIAJE
RH-SW(config-if-range)#switchport access vlan 10

#LO MISMO PARA LA VLAN DE VOZ
RH-SW(config-if-range)#switchport voice vlan 120


RH-SW(config)#do sh start
```

AHORA DEPENDE DE NOSOTROS CONFIGURAR LOS PUERTOS DE LOS SWITCHES DE CAPA 3.

Necesitamos y queremos que la vlan de voz pase al router sede que tenemos arriba dedicado exclusivamente a la voz, entonces en cada uno de los switches necesitamos identificar qué puertos seran acces y qué puertos serán truncal para una comunicación constante con las areas de trabajo y una comunicación estable con los routers dedicados a la redundancia y comunicación con la administración.

Ya que el router sede dedicado a voz actuara como gateway para TODOS los telefonos se considera que unicamente los puertos hacía los routers de arriba no sean trunk.

```
#MISMA CONFIGURACIÓN EN AMBOS SWITCHES
Switch(config)#int range gig1/0/2-7
Switch(config-if-range)#switchport mode trunk

#AHORA HAY QUE CREAR TODAS LAS VLANS EN ESTOS SWITCH TAMBIEN
Switch(config)#vlan 10
Switch(config-vlan)#name RH
Switch(config-vlan)#vlan 20
Switch(config-vlan)#name TI
Switch(config-vlan)#vlan 30
Switch(config-vlan)#name LEGAL
Switch(config-vlan)#vlan 40
Switch(config-vlan)#name FINANZAS
Switch(config-vlan)#vlan 50
Switch(config-vlan)#name OPERACIONES
Switch(config-vlan)#vlan 120
Switch(config-vlan)#name VOICE
Switch(config-vlan)#exit
```

PORT SECURITY

En el “cuarto” de servidores necesitamos que todos los puertos esten cubiertos y que nadie sea capaz de conectarse, en caso del mismo hemos de apagar todos los puertos según el servidor atacado o en su caso, de todos los servidores.

Se considera que el apagar puertos es el método más efectivo contra un ataque.

```
Switch(config)#int range fa0/2-6
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#
Switch(config-if-range)#switchport port-security maximum 1
Switch(config-if-range)#switchport port-security mac-address sticky
Switch(config-if-range)#
Switch(config-if-range)#switchport port-security violation shutdown
Switch(config-if-range)#exit

SERVER-SITE(config)#vlan 90
SERVER-SITE(config-vlan)#name ADMINISTRADOR
SERVER-SITE(config-vlan)#exit
SERVER-SITE(config)#int fa0/7
SERVER-SITE(config-if)#switchport access vlan 90
SERVER-SITE(config-if)#exit
SERVER-SITE(config)#do wr
```

```
SERVER-SITE(config)# int range fa0/7-24
SERVER-SITE(config-if-range)#switchport mode access
SERVER-SITE(config-if-range)#switchport access vlan 99
% Access VLAN does not exist. Creating vlan 99
SERVER-SITE(config-if-range)#shutdown

SERVER-SITE(config)#enable password admin
SERVER-SITE(config)#line console 0
SERVER-SITE(config-line)#password admin
SERVER-SITE(config-line)#login
SERVER-SITE(config-line)#exit
SERVER-SITE(config)#exit

SERVER-SITE(config)#NO IP domain-lookup
SERVER-SITE(config)#service password-encryption
SERVER-SITE(config)#exit

SERVER-SITE(config)#do wr
```

SUBNETTING

RECORDANDO QUE:

192.168.20.0/24 para DATA

10.10.10.0/24 para VOICE

192.200.100.0 para REDES PUBLICAS

192.168.20.0

HQ NETWORK (RED SEDE)

DEPARTAMENTO	RED Y MASCARA DE RED	H VALIDOS	GATEWAY	BROADCAST
RH	192.168.20.0/26	192.168.20.1 a 192.168.20.62	192.168.20.1	192.168.20.63
TI	192.168.20.64/26	192.168.20.65 a 192.168.20.126	192.168.20.65	192.168.20.127
LEGAL	192.168.20.128/26	192.168.20.129 a 192.168.20.190	192.168.20.129	192.168.20.191
FINANZAS	192.168.20.192/27	192.168.20.193 a 192.168.20.222	192.168.20.193	192.168.20.223
OPERACIONES	192.168.20.224/27	192.168.20.225 a 192.168.20.254	192.168.20.225	192.168.20.255

SERVER SITE

NO.	NOMBRE	DIRECCIÓN IP	HOST VALIDOS	GATEWAY	BROADCAST
1	SERVER-SITE	192.168.21.0/28	192.168.21.1 a 192.168.21.254	192.168.21.1	192.168.21.15

ENTRE ROUTERS Y SWITCHES SEDE

NO.	DIRECCION IP
HQ-SW1	192.168.21.16/30
HQ-SW2	192.168.21.20/30

ENTRE ROUTERS E ISP'S

192.200.100.0

NO.	DIRECCION IP
HQ-ISP1	190.200.100.0/30
HQ-ISP2	190.200.100.4/30
SRV-ISP1	190.200.100.8/30
SRV-ISP2	190.200.100.12/30

CADA IP SE COLOCO EN SU RESPECTIVA LINEA DENTRO DEL DIAGRAMA

ROUTER VOICE

```
YA QUE EL TRAFICO DE VOZ VIAJA A TRAVES DE UNA VLAN NECESITAMOS HACER QUE
ROUTER INTERVENGA
Router(config-if)#int fa0/0.120
Router(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/0.120, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.120, chang

Router(config-subif)#encapsulation dot1Q 120
Router(config-subif)#ip add 10.10.10.1 255.255.255.0
Router(config-subif)#exit
Router(config)#do wr
```

HQ-SW1

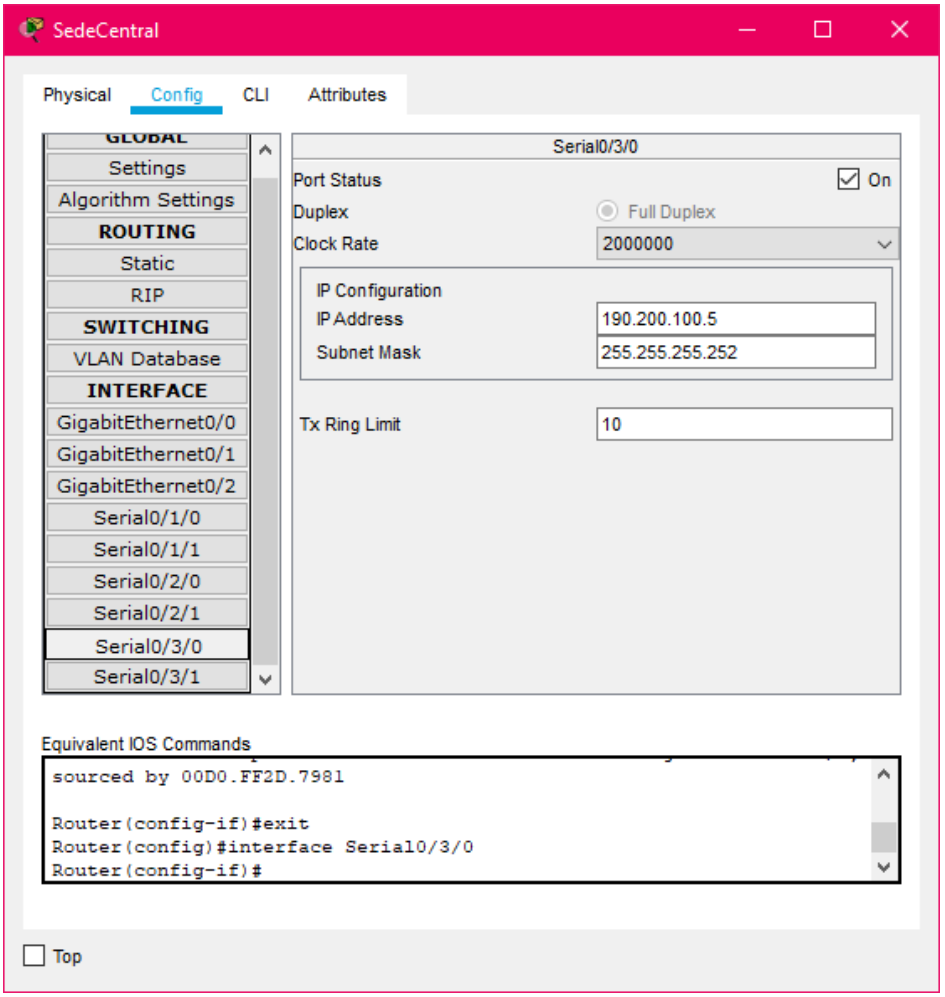
```
Switch(config)#int giga1/0/1
Switch(config-if)#no switchport
Switch(config-if)#ip add 192.168.21.17 255.255.255.252
Switch(config-if)#no sh
```

```
Switch(config-if)#
Switch(config-if)#do wr
```

HQ-SW2

```
Switch(config)#int giga1/0/1
Switch(config-if)#no switchport
Switch(config-if)#ip add 192.168.21.21 255.255.255.252
Switch(config-if)#n sh
Switch(config-if)#do wr
```

PARA FACILITAR EL PROCESO EN LOS DEMAS ROUTERS ENTRAMOS Y CONFIGURAMOS POR LA INTERFAZ.



OSPF (ROUTERS Y SWITCHES)

Se selecciono el OSPF como método de enrutamiento dinámico por varias razones.

Es altamente escalable, lo que significa que puede adaptarse a redes grandes y complejas. Además, es eficiente en la convergencia de la red, lo que miniza el tiempo necesario para

reconfigurar rutas en caso de cambios. También ofrece mayor flexibilidad al permitir la definición de áreas en la red para una administración más fácil y un mejor control del tráfico. Además, su capacidad de calcular rutas basadas en múltiples criterios, como ancho de banda o costo, **lo hace una elección robusta para redes que quieren optimización y control de tráfico.**

Como se menciono anteriormente, buscamos implementar la **redundancia**.

El OSPF es ideal para redes que buscan redundancia debido a su capacidad de soportar múltiples rutas hacia un mismo destino. el OSPF asegura que, en caso de que un enlace falle, la red **pueda automáticamente redigir el tráfico por otras rutas disponibles sin interrupciones significativas.**

```
Switch(config)#ip routing
```

El comando `ip routing` en un switch de capa 3 (multicapa) habilita la funcionalidad de enrutamiento en el dispositivo. Esto permite que el switch realice enrutamiento entre diferentes VLANs y redes, actuando más como un router que como un switch de capa 2 tradicional. **El switch podrá entonces tomar decisiones de enrutamiento y reenviar tráfico entre diferentes subredes basándose en la tabla de enrutamiento que construye a través de protocolos de enrutamiento estáticos o dinámicos como OSPF o EIGRP.**

```
Switch(config)#router ospf 10
Switch(config-router)#router-id 1.1.1.1
Switch(config-router)#network 10.10.10.0 0.0.0.3 area 0
Switch(config-router)#
Switch(config-router)#network 192.168.21.16 0.0.0.3 area 0
Switch(config-router)#no network 10.10.10.0 0.0.0.3 area 0
Switch(config-router)#network 10.10.10.0 0.0.0.255 area 0
Switch(config-router)#
Switch(config-router)#network 192.168.20.0 0.0.0.255 area 0
Switch(config-router)#exit
```

Segundo switch de Capa 3

```
HQ-SW2(config)#ip routing
HQ-SW2(config)#
HQ-SW2(config)#router ospf 10
HQ-SW2(config-router)#router-id 2.2.2.2
HQ-SW2(config-router)#network 10.10.10.0 0.0.0.255 area 0
HQ-SW2(config-router)#network 192.168.21.20 0.0.0.3 area 0
HQ-SW2(config-router)#network 192.168.20.0 0.0.0.255 area 0
```

```
HQ-SW2(config-router)#exit
HQ-SW2(config)#do wr
```

Router de Voz

```
VOIP-R(config)#router ospf 10
VOIP-R(config-router)#router-id 3.3.3.3
VOIP-R(config-router)#nework 10.10.10.0 0.0.0.255 area 0
                          ^
% Invalid input detected at '^' marker.

VOIP-R(config-router)#network 10.10.10.0 0.0.0.255 area 0
VOIP-R(config-router)#exit
VOIP-R(config)#do wr
```

Router Sede

```
Router(config)#router ospf 10
Router(config-router)#router-id 4.4.4.4
Router(config-router)#
Router(config-router)#network 192.168.21.16 0.0.0.3 area 0
Router(config-router)#network 192.168.21.16 0.0.0.3 area 0
02:38:38: %OSPF-5-ADJCHG: Process 10, Nbr 1.1.1.1 on GigabitEthernet0/0
Router(config-router)#network 192.168.21.20 0.0.0.3 area 0
Router(config-router)#
02:39:13: %OSPF-5-ADJCHG: Process 10, Nbr 2.2.2.2 on GigabitEthernet0/1 fr

Router(config-router)#network 190.200.100.0 0.0.0.3 area 0
Router(config-router)#network 190.200.100.4 0.0.0.3 area 0
Router(config-router)#exit
Router(config)#do wr
```

Router ISP1

```
Router(config)#router ospf 10
Router(config-router)#router-id 5.5.5.5
Router(config-router)#
Router(config-router)#network 190.200.100.0 0.0.0.3 area 0
Router(config-router)#network 190.200.100.8 0.0.0.3 area 0
02:41:06: %OSPF-5-ADJCHG: Process 10, Nbr 4.4.4.4 on Serial0/2/0 from LOAD

Router(config-router)#network 190.200.100.8 0.0.0.3 area 0
```

```
Router(config-router)#exit
Router(config)#do wr
```

Router ISP2

```
Router(config)#router ospf 10
Router(config-router)#router-id 6.6.6.6
Router(config-router)#network 190.200.100.4 0.0.0.3 area 0
Router(config-router)#
02:42:28: %OSPF-5-ADJCHG: Process 10, Nbr 4.4.4.4 on Serial0/2/0 from LOAD

Router(config-router)#network 190.200.100.12 0.0.0.3 area 0
Router(config-router)#exit
Router(config)#do wr
```

Router SIDE-To-SIDE

```
Router(config)#router ospf
% Incomplete command.
Router(config)#router ospf 10
Router(config-router)#router-id 7.7.7.7
Router(config-router)#network 192.168.21.0 0.0.0.15 area 0
Router(config-router)#network 190.200.100.8 0.0.0.3 area 0
Router(config-router)#
02:44:48: %OSPF-5-ADJCHG: Process 10, Nbr 5.5.5.5 on Serial0/2/1 from LOAD

Router(config-router)#network 190.200.100.12 0.0.0.3 area 0
Router(config-router)#exit
Router(config)#
```

Comandos para mostrar

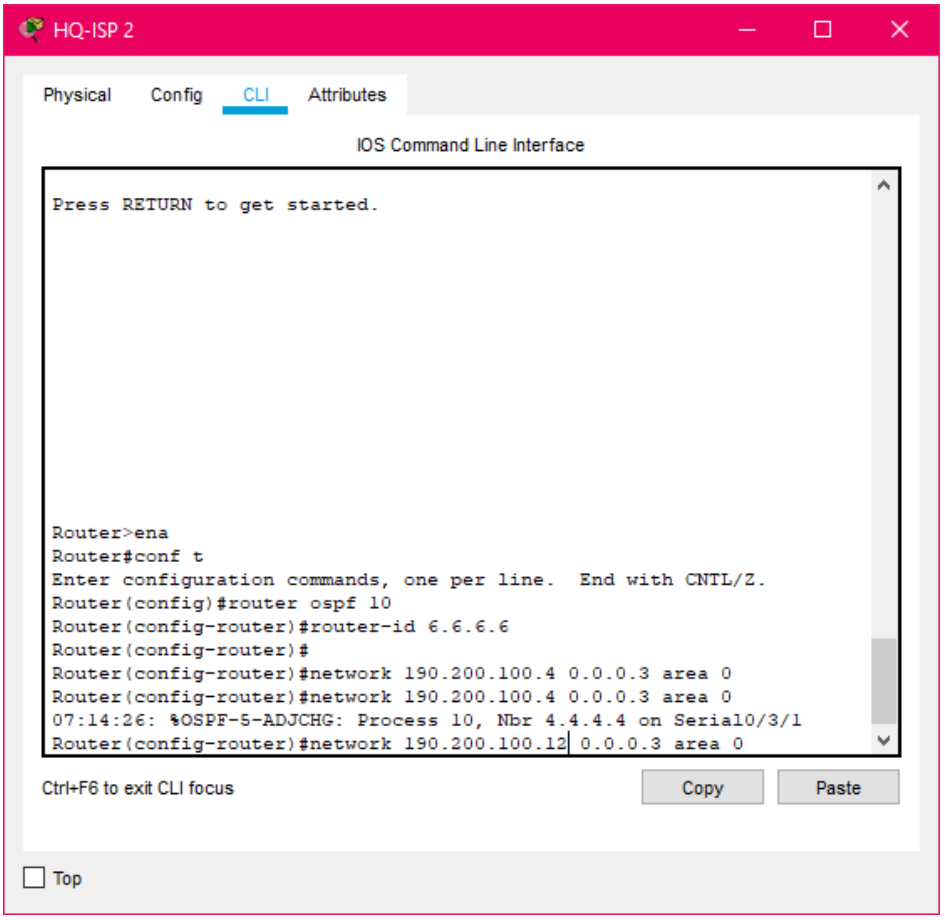
```
do sh running-config
do sh ip route ospf
do sh ip ospf neigh
do sh ip ospf interface
```

En esta sección de comandos iniciamos la configuración del OSPF y establecemos el ID del proceso en 10.

Después asigmanos el ID del OSPF a 1.1.1.1, ID que debe ser único en el área OSPF para así agregar las redes que incluira dicho proceso y determinando a qué área OSPF pertenecen.

Se hace el mismo proceso en el segundo switch “caja” con cambios mínimos.

```
Switch(config)#router ospf 10
Switch(config-router)#router-id 2.2.2.2
Switch(config-router)#network 10.10.10.0 0.0.0.255 area 0
Switch(config-router)#
Switch(config-router)#network 192.168.21.20 0.0.0.3 area 0
Switch(config-router)#
Switch(config-router)#network 192.168.20.0 0.0.0.255 area 0
Switch(config-router)#
Switch(config-router)#exit
Switch(config)#
Switch(config)#do wr
Building configuration...
Compressed configuration from 7383 bytes to 3601 bytes[OK]
[OK]
```



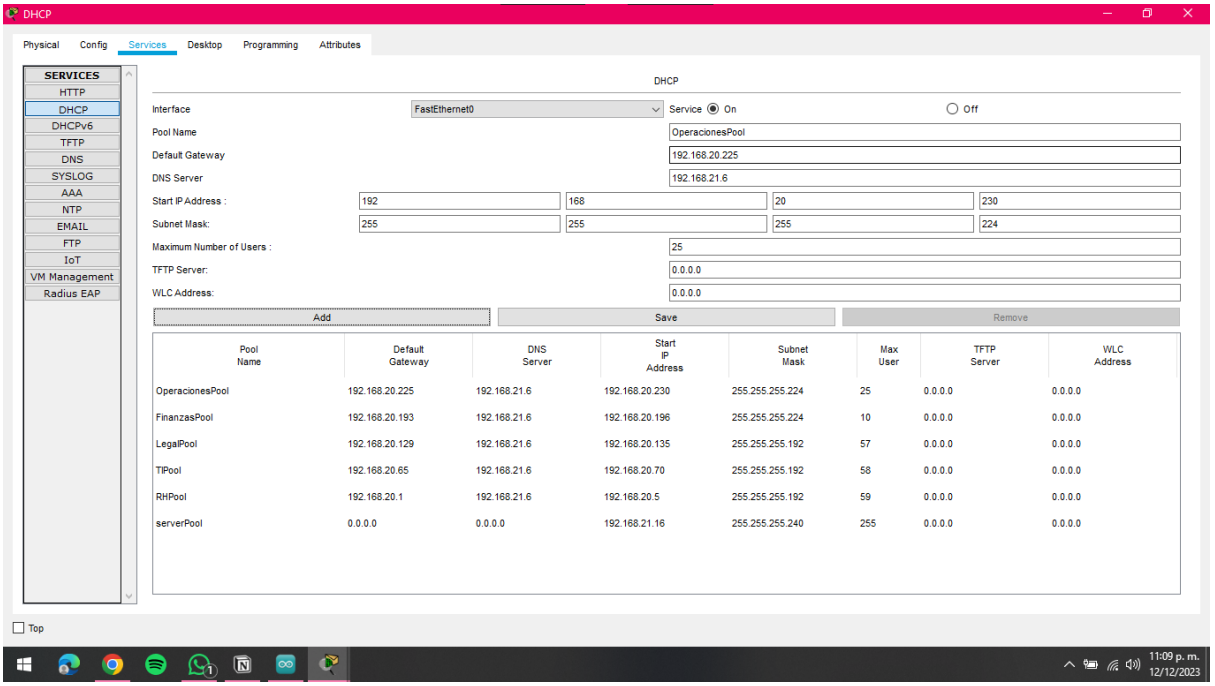
IP ESTATICA PARA EL CUARTO DE SERVIDORES

int vlan 10

ROUTING INTER-VLAN (AÑADIENDO IP DHCP HELPER)

```
HQ-SW1>ena
Password:
HQ-SW1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
HQ-SW1(config)#int vlan 10
HQ-SW1(config-if)#
%LINK-5-CHANGED: Interface Vlan10, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed state to u

HQ-SW1(config-if)#ip add 192.168.20.1 255.255.255.192
```

```
HQ-SW1(config-if)#ip helper-address 192.168.21.5
HQ-SW1(config-if)#exit
HQ-SW1(config)#int vlan 20
HQ-SW1(config-if)#
%LINK-5-CHANGED: Interface Vlan20, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan20, changed state to u

HQ-SW1(config-if)#ip add 192.168.20.65 255.255.255.192
HQ-SW1(config-if)#ip helper-address 192.168.21.5
HQ-SW1(config-if)#ex
HQ-SW1(config)#int vlan 30
HQ-SW1(config-if)#
%LINK-5-CHANGED: Interface Vlan30, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan30, changed state to u

HQ-SW1(config-if)#ip add 192.168.20.129 255.255.255.192
HQ-SW1(config-if)#ip helper-address 192.168.21.5
HQ-SW1(config-if)#ex
HQ-SW1(config)#int vlan 40
HQ-SW1(config-if)#
%LINK-5-CHANGED: Interface Vlan40, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan40, changed state to u

HQ-SW1(config-if)#ip add 192.168.20.193 255.255.255.224
HQ-SW1(config-if)#ip helper-address 192.168.21.5
HQ-SW1(config-if)#ex
HQ-SW1(config)#int vlan 50
HQ-SW1(config-if)#
%LINK-5-CHANGED: Interface Vlan50, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan50, changed state to u

HQ-SW1(config-if)#ip add 192.168.20.225 255.255.255.224
HQ-SW1(config-if)#ip helper-address 192.168.21.5
HQ-SW1(config-if)#ex
HQ-SW1(config)#do wr
```



SERVICIO DE TELEFONÍA

```
VOIP-R(config)#service dhcp
VOIP-R(config)#ip dhcp pool VOICE
VOIP-R(dhcp-config)#network 10.10.10.0 255.255.255.0
VOIP-R(dhcp-config)#default-router 10.10.10.1%DHCPD-4-PING_CONFLICT: DHCP

VOIP-R(dhcp-config)#default-router 10.10.10.1
VOIP-R(dhcp-config)#option 150 ip 10.10.10.1
VOIP-R(dhcp-config)#
VOIP-R(dhcp-config)#dns-server 10.10.10.1
VOIP-R(dhcp-config)#exit

VOIP-R(config)#ip dhcp excluded-address 10.10.10.1

VOIP-R(config)#telephony-service
VOIP-R(config-telephony)#max-ephones 20
VOIP-R(config-telephony)#max-dn 20
VOIP-R(config-telephony)#
VOIP-R(config-telephony)#ip source-address 10.10.10.1 port 2000
VOIP-R(config-telephony)#auto assign 1 to 20

VOIP-R(config-ephone-dn)#number 408
VOIP-R(config-ephone-dn)#ex
VOIP-R(config)#
VOIP-R(config)#ephone-dn 9
VOIP-R(config-ephone-dn)#%LINK-3-UPDOWN: Interface ephone_dsp DN 9.1, char
```

```
VOIP-R(config-ephone-dn)#number 409
VOIP-R(config-ephone-dn)#ex
VOIP-R(config)#ephone-dn 10
VOIP-R(config-ephone-dn)#%LINK-3-UPDOWN: Interface ephone_dsp DN 10.1, cha

VOIP-R(config-ephone-dn)#number 410
VOIP-R(config-ephone-dn)#ex
VOIP-R(config)#
VOIP-R(config)#do wr
Building configuration...
```

ACL PARA SSH

```
access-list 10 permit 192.168.20.224 0.0.0.3
access- list 10 deny any

line vty 0 15
access class 10 in
exit

do wr
```

VTP

```
HR-SW(config)#vtp mode transparent
Setting device to VTP TRANSPARENT mode.

HR-SW(config)#vtp domain ciscovtp
Changing VTP domain name from NULL to ciscovtp
HR-SW(config)#vtp password cisco
Setting device VLAN database password to cisco
HR-SW(config)#do sh vtp status
VTP Version capable             : 1 to 2
VTP version running             : 1
VTP Domain Name                 : ciscovtp
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : 00E0.F9CE.A800
Configuration last modified by 0.0.0.0 at 3-1-93 00:24:30
```

```
Feature VLAN :
--------------
VTP Operating Mode                : Transparent
Maximum VLANs supported locally   : 255
Number of existing VLANs          : 7
Configuration Revision            : 0
MD5 digest                        : 0xD2 0xA2 0xEE 0xB0 0x24 0x2D 0x08 0xA
                                    0xCC 0xAB 0x50 0x86 0x81 0x6D 0xE8 0x2
HR-SW(config)#
```

```
#USER SIN PRIVILEGIOS EN SSH
HQ-SW1(config)# username user privilege 1 password cisco
HQ-SW1(config)#ip domain-name cisco.com

HQ-SW1(config)#line vty 0 15
HQ-SW1(config-line)#transport input ssh
HQ-SW1(config-line)#privilege level 1
HQ-SW1(config-line)#login local
HQ-SW1(config-line)#exit
HQ-SW1(config)#line vty 0 15
HQ-SW1(config-line)#exec-timeout 0 30
HQ-SW1(config-line)#exit
```

MANUAL DE PROYECTO 2