UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

ESCUELA DE CIENCIAS Y SISTEMAS

REDES 2

PRIMER SEMESTRE 2023

Imagen que contiene Logotipo

Descripción generada automáticamenteSECCIÓN

**MANUAL PRACTICA 1**

**NO. GRUPO 8**

|  |  |
| --- | --- |
| Nombre | Carnet |
|  |  |
|  |  |
|  |  |
| **Henrry David Bran Velásquez** | **201314439** |

Guatemala, 16 de febrero del 2023

Manual de configuraciones

Asignación de IP

A cada maquina debemos asignarle una dirección de IP que pertenezca al departamento de su red y en el rango determinado.

A todas las maquinas se les debe asignar una dirección IP estática.

# Departamento de primaria

Red: 192.168.18.0/24   
Host 1:

Graphical user interface, application

Description automatically generated

Host 2:

Graphical user interface, application

Description automatically generated

Host 3:

Graphical user interface, application

Description automatically generated

# Departamento de Básicos

Red: 192.168.28.0/24

Graphical user interface, application

Description automatically generatedHost 1:

Graphical user interface, text, application, email

Description automatically generatedHost 2:

Graphical user interface, text, application, email

Description automatically generatedHost 3:

# Departamento de Diversificado

Red: 192.168.38.0/24

Host 1:

Graphical user interface, text, application

Description automatically generated

Graphical user interface, text, application

Description automatically generatedHost 2:

Graphical user interface, text, application

Description automatically generatedHost 3:

# Colocar nombre a cada switch

Para cambiarle el nombre a un switch desde la terminal, realizamos los siguientes pasos y comandos:

1. Ingresar a la terminal del dispositivo
2. Ingresar comando enable
3. Ingresar comando configure terminal
4. Ingresar comando hostname [Nuevo nombre]

A picture containing text

Description automatically generated

Creación de VLAN y uso de VTP

Para segmentar de forma lógica la comunicación de los departamentos crearemos 3 VLAN distintas

1. VLAN Primaria: Primaria18
2. VLAN Básicos: Básicos28
3. VLAN Diversificado: Diversificado38

Estas tres VLANs hay que crearlas en cada switch, en total existen 5 switch, por lo tanto tendríamos que realizar el proceso 15 veces para que todos los switch tengan conocimiento de las tres VLAN, para evitarnos el proceso de realizarlo repetidamente, podemos utilizan el protocolo VTP (VLAN Trunking Protocol) el cual nos permite configurar las tres Vlan en un solo switch tipo servidor y los otros switch en tipo cliente sincronizan la información del switch maestro. Por ende, los pasos a seguir son los siguientes:

1. Buscar que Switch será el servidor
2. Crear las Vlan correspondientes
3. Colocar en moto Trunk las interfaces entre los Switch

## Buscar el switch servidor

Para que el protocolo VTP funcione debemos seleccionar un switch como servidor. Para encontrar que switch seleccionar tenemos 2 opciones, la primera es verificar físicamente que la conexión entre los switches esté sincronizada o la segunda es usar el comando *sh spanning-tree* en cada switch, hasta encontrar el que diga *this switch is root*.

* Switch client (SW1, SW2, SW3, SW5)

Table

Description automatically generated

* Switch Server (SW4)

Text

Description automatically generated with medium confidence

Una vez tengamos identificado el switch tipo servidor, procederemos a usar el comando VTP para indicar a cada Switch su modo de operación o rol.

## Sincronizar los Switches servidor y cliente por medio de VTP

Existen dos pasos para sincronizar los Switches usando VTP, el paso uno es indicarle a cada Switch su rol y el segundo paso es colocar las conexiones de las interfaces entre switches como truncales.

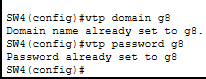
El primer paso es indicarle a cada switch cual va a ser su rol en la red, los únicos roles posibles son: Server, Client y Transparent. En nuestro caso en especifico usaremos los primeros dos.

* VTP mode server

SW4

Text, letter

Description automatically generated



* VTP mode client

SW1

Text

Description automatically generated

Text

Description automatically generated

SW2

Text

Description automatically generated

Text

Description automatically generated

SW3

Text, letter

Description automatically generated

Text

Description automatically generated

SW5

Text, letter

Description automatically generated

Text

Description automatically generated

El segundo paso es colocar las interfaces entre los switches como truncales.

SW1

Text

Description automatically generated



SW2

Text

Description automatically generated

Text

Description automatically generated

SW3

Text

Description automatically generated with medium confidence

Text, letter

Description automatically generated

SW4

Text, letter

Description automatically generated

Text, letter

Description automatically generated

Text

Description automatically generated

SW5

Text, letter

Description automatically generated

Text

Description automatically generated

## Creación de VLAN

Ingresamos al Switch tipo Servidor que en nuestro caso sería el Switch SW4 y creamos las 3 Vlans previamente mencionadas.

1. VLAN Primaria18



1. VLAN Básicos 28



1. VLAN Diversificado 38



Verificamos si las VLAN si han creado correctamente en el Switch.

Table

Description automatically generated

# Colocar las interfaces hacia los dispositivos finales en modo acceso

Las interfaces que conectan hacia los dispositivos finales deben tener el modo acceso y permitir únicamente la vlan que tienen asignada

SW1

Graphical user interface, text

Description automatically generated

SW2

Text

Description automatically generated

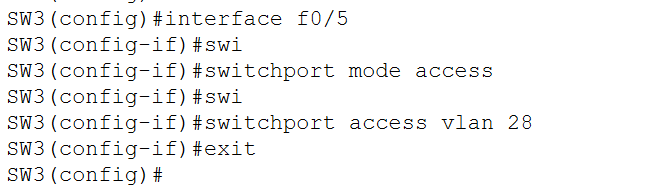
SW3

Text

Description automatically generated

Graphical user interface, text

Description automatically generated



SW4

Graphical user interface

Description automatically generated with medium confidence

A picture containing text

Description automatically generated

SW5

Text

Description automatically generated

## Creación de STP

A lo largo del desarrollo de la practica se realiza la configuración de STP en sus dos versiones PVST y RapidPVST, se realizaran las pruebas para bloquear/desbloquear puertos y medir cuanto tiempo se tarda en conectarse a otro puerto cuando uno se ve afectado.

## Escenario 1 PVST

Se elegirá el escenario 1 para realizar las primeras pruebas con los switches

## Verificación de protocolos PVST

Se verificará que todos los switches estén con el protocolo PVST

SW4 - Server

* Sh vtp st

Texto, Carta

Descripción generada automáticamente

Mostramos las VLAN que tiene y los puertos activos/forwarding

* Sh spanning-tree

Tabla

Descripción generada automáticamente con confianza baja

Texto

Descripción generada automáticamente con confianza baja

Tabla

Descripción generada automáticamente con confianza media

Texto, Carta

Descripción generada automáticamente

SW1 – Client

* Sh vtp st

Texto

Descripción generada automáticamente con confianza media

Mostramos las VLAN que tiene y los puertos activos/forwarding

* Sh spanning-tree

Tabla

Descripción generada automáticamente

Tabla

Descripción generada automáticamente

Tabla

Descripción generada automáticamente

SW2 – Client

* Sh vtp st

Texto

Descripción generada automáticamente con confianza baja

Mostramos las VLAN que tiene y los puertos activos/forwarding

* Sh spanning-tree

Texto

Descripción generada automáticamente con confianza media

Texto

Descripción generada automáticamente

Tabla

Descripción generada automáticamente

SW3 – Client

* Sh vtp st

Imagen que contiene Texto

Descripción generada automáticamente

Mostramos las VLAN que tiene y los puertos activos/forwarding

* Sh spanning-tree

Tabla

Descripción generada automáticamente

Tabla

Descripción generada automáticamente

Tabla

Descripción generada automáticamente

SW5 – Client

* Sh vtp st

Texto

Descripción generada automáticamente

Mostramos las VLAN que tiene y los puertos activos/forwarding

* Sh spanning-tree

Tabla

Descripción generada automáticamente

Tabla

Descripción generada automáticamente

Tabla

Descripción generada automáticamente

## Cambio de puertos o enlaces

Se procederá a crear una tabla de los puertos/enlaces que estén como principal y se bloqueara solo se hará 1 prueba con cada switch con las VLAN que tengan asignadas.

Para todas las pruebas se hará el mismo procedimiento, este es:

Interfaz de usuario gráfica

Descripción generada automáticamenteIngresar al prompt de nuestro pc X.X.X.X en este caso utilice la 192.168.18.1

Ingresamos al switch que queremos bloquear lo mejor es utilizar el que está conectado a nuestro pc que vamos a hacer el ping de salida en nuestro ejemplo SW1 para el ping de salida 192.168.18.1

* Ping -t 192.168.18.3

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Ingresamos a nuestra interfaz que vamos a bloquear esta la sabemos por los pasos anteriores donde se observaba que para la VLAN 18 el puerto Root era Fa0/3, y mediante los comandos

* Ena
* Conf t
* Int Fa0/3
* Shutdown

Apagaremos esa interfaz y ahí es donde mediremos el tiempo que se conecte nuestro ip saliente a la ip entrante mediante el comando ping.

Por último, tendríamos algo así:

En nuestro pc

Interfaz de usuario gráfica, Texto

Descripción generada automáticamente

El swtich

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Tabla

Descripción generada automáticamente con confianza media

Procedemos a llenar la tabla PVST

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| PING SALIENTE | PING ENTRANTE | VLAN | PUERTO ROOT A BLOQUEAR/APAGAR | TIEMPO | SWITCH |
| 192.168.18.1 | 192.168.18.3 | 18 | Fa0/3 | 32.5 Segundos | SW1 |
| 192.168.28.1 | 192.168.28.2 | 28 | Fa0/1 | 57.37 segundos | SW3 |
| 192.168.38.1 | 192.168.38.3 | 38 | Fa0/2 | 56.84 segundos | SW2 |

## Escenario 2 RAPID-PVST

Se elegirá el escenario 2 para realizar las primeras pruebas con los switches

## Verificación de protocolos Actuales

Se verificará que todos los switches estén con el protocolo PVST

SW4 - Server

* Sh spanning-tree

Texto

Descripción generada automáticamente

Texto

Descripción generada automáticamente



Entonces si verificamos nos damos cuenta que todos los switches están en modo PVST y hay que cambiarlos todos a modo Rapid-PVST

* Ena
* Conf t
* Spanning-tree mode rapid-pvst
* Exit
* Sh run

Texto, Carta

Descripción generada automáticamente

Texto

Descripción generada automáticamente

Entonces ya tendremos el switch de modo rapid-pvst, por último miramos sus puertos root-FWD o designados

* Sh spanning-tree

Texto

Descripción generada automáticamente

Tabla

Descripción generada automáticamente con confianza media

Tabla

Descripción generada automáticamente con confianza baja

Tabla

Descripción generada automáticamente con confianza media

Como suponemos todos los switch están en PVST entonces hay que cambiarlos todos a Rapid-PVST

SW 1

Texto, Carta

Descripción generada automáticamente

SW2

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

SW3

Texto, Correo electrónico

Descripción generada automáticamente

SW 5

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Ya cambia la configuración de todos los switches se procederá a hacer un ping como con el pvst y ver cuales son sus enlaces root y bloquearlos/apagarlos

Procedemos a llenar la tabla RAPID-PVST

PING 1

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

PING 2

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

PING 3

Una captura de pantalla de una computadora

Descripción generada automáticamente

Tabla de pruebas con el escenario 2 Rapid-PVST

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| PING | PING SALIENTE | PING ENTRANTE | VLAN | PUERTO ROOT A BLOQUEAR/APAGAR | TIEMPO | SWITCH |
| 1 | 192.168.18.1 | 192.168.18.3 | 18 | Fa0/3 | Ni un segundo cuando tome el tiempo ni se notó el cambio | SW1 |
| 2 | 192.168.28.1 | 192.168.28.2 | 28 | Fa0/1 | Ni se notó el cambio | SW3 |
| 3 | 192.168.38.1 | 192.168.38.3 | 38 | Fa0/2 | Igual que los anteriores ni se notó el cambio | SW2 |

## Conclusión PVST Y RAPID-PVST

La mejor opción sería el rapid-pvst como se pude observar en las tablas se hicieron las mismas pruebas en los mismos switches y el mismo ping a las VPC y gano con gran diferencia el Rapid-PVST, tarde más tiempo en darle pausar el botón del cronometro que esa conexión se efectuará ni siquiera tuvo líneas de perdida, en conclusión, el mejor escenario sería el 2 que tuvo un menor tiempo de convergencia.

# Seguridad para las interfaces asignadas a la VLAN

Se configuraron los puertos en modo acceso de los switches con port-security en modo MAC address, asignándoles así la MAC del dispositivo al que se encuentran conectados de manera que en caso de que se conecta algún dispositivo diferente el puerto se apagará.

## MAC Address de los dispositivos

|  |  |
| --- | --- |
| **IP** | **MAC** |
| 192.168.18.1 | 0060.5C02.1C9D |
| 192.168.18.2 | 0009.7CBD.4C80 |
| 192.168.18.3 | 000A.4102.53EA |
| 192.168.28.1 | 0003.E4DC.A8A0 |
| 192.168.38.3 | 0060.47E3.3659 |
| 192.168.28.2 | 0040.0B97.34E5 |
| 192.168.28.3 | 00D0.FF05.5619 |
| 192.168.38.1 | 0010.115E.71EC |
| 192.168.38.2 | 000C.8534.5838 |

## Comando Utilizados para configurar el Port Security

Para configurar el port security necesitamos la MAC address del dispositivo para obtenerla entramos al command prompt de la PC y ejecutamos el siguiente comando:

Text

Description automatically generated

Luego copiamos la MAC e ingresamos a la interfaz del switch que se encuentra conectada al dispositivo y ejecutamos el siguiente comando:

Text, letter

Description automatically generated

Para poder ver la configuración del port security en las interfaces corremos el siguiente comando:

Graphical user interface, text

Description automatically generated

De esta manera ya queda configurada el port security de la interfaz del puerto