Manual de configuraciones

Asignacion 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

Host 1:

Graphical user interface, application

Description automatically generated

Host 2:

Graphical user interface, text, application, email

Description automatically generated

Host 3:

Graphical user interface, text, application, email

Description automatically generated

# Departamento de Diversificado

Red: 192.168.38.0/24

Host 1:

Graphical user interface, text, application

Description automatically generated

Host 2:

Graphical user interface, text, application

Description automatically generated

Host 3:

Graphical user interface, text, application

Description automatically generated

# 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.

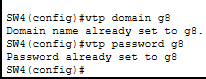
El primer paso es indicarle a cada switch cual va a ser su rol en la red, los únicos roles posibles son: Server, Client y Transparent. En nuestro caso en especifico usaremos los primeros dos.

* 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

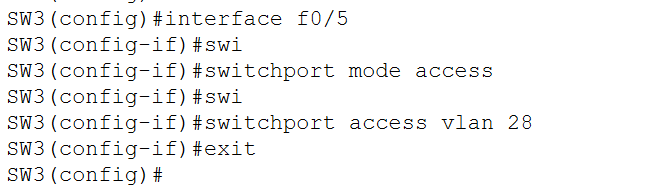
SW3

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

Texto, Carta

Descripción generada automáticamente

Mostramos las VLAN que tiene y los puertos activos/forwarding

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

Texto

Descripción generada automáticamente con confianza media

Mostramos las VLAN que tiene y los puertos activos/forwarding

Tabla

Descripción generada automáticamente

Tabla

Descripción generada automáticamente

Tabla

Descripción generada automáticamente

SW2 – Client

Texto

Descripción generada automáticamente con confianza baja

Mostramos las VLAN que tiene y los puertos activos/forwarding

Texto

Descripción generada automáticamente con confianza media

Texto

Descripción generada automáticamente

Tabla

Descripción generada automáticamente

SW3 – Client

Imagen que contiene Texto

Descripción generada automáticamente

Mostramos las VLAN que tiene y los puertos activos/forwarding

Tabla

Descripción generada automáticamente

Tabla

Descripción generada automáticamente

Tabla

Descripción generada automáticamente

SW5 – Client

Texto

Descripción generada automáticamente

Mostramos las VLAN que tiene y los puertos activos/forwarding

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:

Ingresar al prompt de nuestra pc X.X.X.X en este caso utilice la 192.168.18.1

Interfaz de usuario gráfica

Descripción generada automáticamente

Ingresamos al switch que queremos bloquear lo mejor es utilizar el que esta conectado a nuestra 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 entrente mediante el comando ping.

Por utlimo tendiramos algo así:

En nuestra 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

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 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 |