

**Universidad de San Carlos de Guatemala**  
**Ingeniería en Ciencias y Sistemas**  
**Redes de Computadoras 2**  
**Primer Semestre 2021**  
**Ing. Pedro Pablo Hernandez**  
**Auxiliares: Sergio Silva / Wilson Guerra**

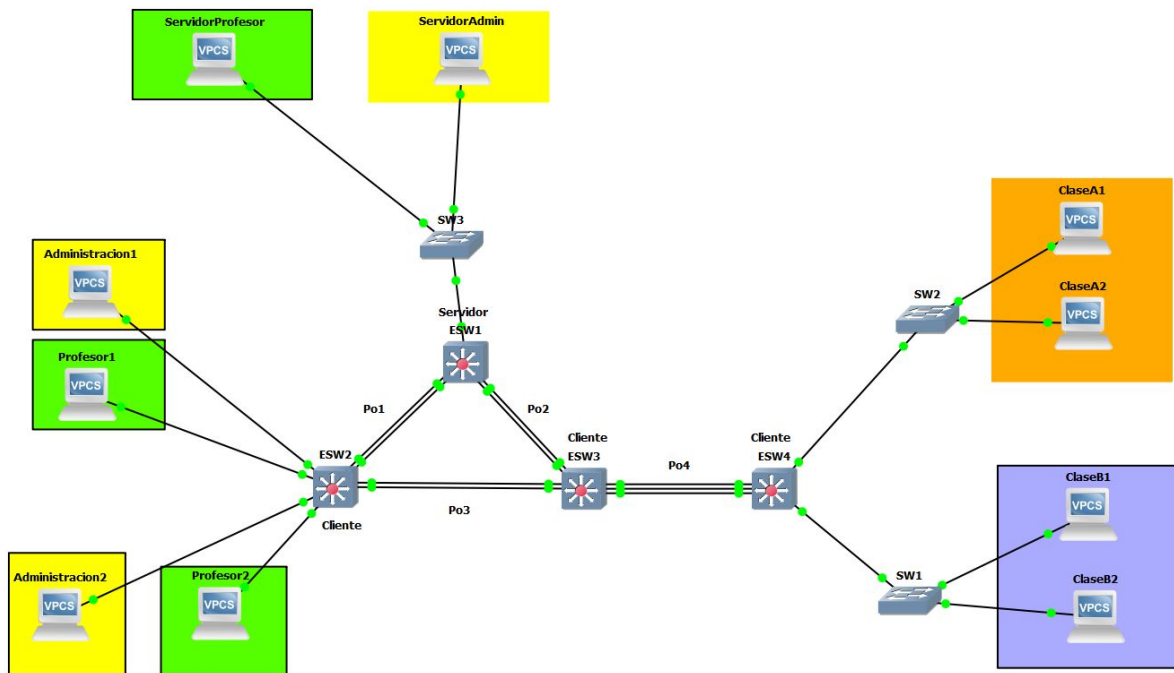


## Practica 2

### Objetivos

- Realizar las configuraciones básicas del switch.
- Configurar las interfaces en los equipos PC host.
- Configurar y conocer el funcionamiento de las VLANs.
- Configurar y conocer los tipos de acceso en los puertos.
- Configurar y conocer VTP en los switches, como sus distintos modos.
- Configurar la comunicación entre distintas VLANs (Inter-Vlan).
- Creación de access-list para filtrado de tráfico.
- Comprender el funcionamiento de STP, sus distintas versiones, y los estados de las interfaces.
- Creación de port-channels, en sus variantes LACP y PAgP.
- Aplicación de medidas de seguridad en los puertos de un switch.

## Topología



## Configuraciones a Realizar

Se debe de configurar la topología anterior de la misma forma en la que se presenta en la imagen.

## VTP

- Los estudiantes deben de realizar el análisis correspondiente para utilizar VTP en donde sea necesario, así como el tipo a utilizar: servidor, cliente o transparente. De igual forma con los puertos que se deben utilizar en la topología.
- El dominio y password a definir será Grupo# (# - será el número de grupo asignado).
- Las vlans a crear son las siguientes:

Administración
Profesores
Clase A
Clase B
Management&Native
BlackHole

- Los números de vlans serán los siguientes:

Administración - 10 + #GrupoAsignado
Profesores - 20 + #GrupoAsignado
Clase A - 30 + #GrupoAsignado
Clase B - 40 + #GrupoAsignado
Management&Native - 99
BlackHole - 999

(Ejemplo si su grupo es el 7, Estudiantes17, Auxiliares27, Profesores37, Administración47. **Si el número de su grupo es de 2 dígitos, tome el segundo dígito.**)

## Direcciones de Red

El estudiante debe seleccionar las direcciones de red que utilizará para cada subred.

- Para llevar a cabo esto, se le otorga una única red 192.168.5X.0/24 la cual deberá de administrar en subredes para los departamentos que se solicitan, donde la X corresponde al número de grupo asignado. (Ejemplo: Para el grupo 7, serían la red 192.168.57.0/24- **Si el número de su grupo es de 2 dígitos, tome el segundo dígito.**). El tamaño de las subredes queda a discreción de los estudiantes.
- Las direcciones deben ser mostradas de manera explícita en la topología, de lo contrario, no se calificará.
- Se debe agregar al manual de configuración, una tabla donde se especifique la información de las subredes resultantes. Se adjunta un ejemplo llamado "Tabla Subredes" en la parte de anexos.
- Deben realizar un manual de configuración con todos los detalles técnicos de la topología, configuración por cada dispositivo, IPs asignada, vlans, puertos, etc.

## Configuración de STP

A lo largo del desarrollo de la práctica se debe realizar la configuración de las siguientes versiones:

- STP
- RSTP
- PVSTP

Una de estas tres versiones será configurada en conjunto con una de las versiones de port-channels existentes, por lo que deberán de realizar pruebas y elegir la combinación que tenga la mejor convergencia.

## Port-channels

Se requiere que exista un ancho de banda considerable para poder intercambiar grandes cantidades de información entre los pcs de los profesores y los alumnos, por lo que se solicita la creación de port-channels.

- Se solicita la configuración de Etherchannel, creando los siguientes port-channel:
  - Po1: Entre el ESW1 y el ESW2 (2 enlaces).
  - Po2: ESW1 y el ESW3 (2 enlaces).
  - Po3: Entre el ESW2 y el ESW3 (2 enlaces).
  - Po4: Entre el ESW3 y el ESW4 (3 enlaces).

Se deberá implementar los tipos de port-channel:

- LACP
- PAgP

Uno de estos dos tipos en combinación con uno de los protocolos de spanning-tree anteriores deberá ser implementado en la solución final. Esto se explicará más a detalle en la sección **“Elección de Escenario con Mejor Convergencia”**.

## Seguridad de interfaces de red

Es de gran importancia aplicar políticas de seguridad sobre las interfaces de los equipos de capa 2, por lo que se le solicita lo siguiente:

### Políticas de puerto compartidas

- Todas las interfaces que no sean utilizadas, deben ser asignadas a la vlan 999 (Blackhole).
- Cambiar la vlan nativa de las interfaces trunk a la vlan 99(Management&Native).
- Desactivar el protocolo DTP de los puertos troncales, si este se encuentra presente en los dispositivos.
- Se debe activar el port-security de los puertos.

### Seguridad para interfaces asignadas a la vlan de alumnos

- Configurar las interfaces de conexión entre los host de alumnos( Clase A y B) y el switch con el modo de port-security mac-address dynamic.
- Configurar que solo se permite el acceso como máximo de 5 direcciones MAC.

### Seguridad para interfaces asignadas a la vlan de profesores

- Configurar las interfaces de conexión entre los host de profesores y el switch con el modo de port-security mac-address sticky.
- Configurar que solo se permita el acceso de una única MAC.
- En caso de detectar una violación de seguridad, el puerto se debe apagar.

### Seguridad para interfaces asignadas a la vlan de administración

- Configurar las interfaces de conexión entre los host de administración y el switch con el modo de port-security mac-address sticky.
- Configurar que solo se permita el acceso de una única MAC.
- En caso de detectar una violación de seguridad, el puerto se debe apagar.

## InterVLAN

Se debe implementar la comunicación entre VLANs, queda a discreción de los estudiantes la manera y el lugar donde realizará dicha configuración. Se debe garantizar la comunicación entre distintas vlans, asegurando que exista comunicación entre los siguientes dispositivos:

- Profesores y Alumnos (Clase A y Clase B).
- Administración y ServidorAdmin, ServidorProfesor.
- Profesores y ServidorProfesor
- Administración y Profesores.
- Alumnos y Alumnos (Clase A con Clase B).

**\*Importante: Cualquier otra combinación no listada, no debe ser permitida.**

**\*\*Importante: Se debe hacer uso de access-list para realizar dicha configuración.**

## Filtrado de vlans en enlaces troncales

Debe analizar la topología, y basado en el flujo de la comunicación entre vlans, aplicar reglas de filtrado de vlan en los enlaces troncales, para reducir el tráfico innecesario.

**\*\*Importante: al aplicar filtrado, se debe mantener el paso para paquetes de las vlans por defecto(1, 1002-1005) y vlans nativas.**

## Access-List

Se deben crear ACL que filtren el tráfico entre distintas VLANs, para de esta manera cumplir con las restricciones de tráfico entre vlans definidas en el apartado de InterVLAN.

Los nombres a utilizar para las ACL deben ser representativos.

## Elección de escenario con mejor resultado de convergencia

La topología final debe ser aquella con la mejor convergencia, es decir, cual es el mejor escenario/combinación de protocolo de spanning-tree y tipo de port-channel, por lo que se debe realizar un estudio de todos los posibles escenarios:

Escenario	Tipo Port-channel	Protocolo spanning-tree
1	Port Channel LACP	STP
2	Port Channel LACP	RSTP
3	Port Channel LACP	PVSTP
4	Port Channel PAgP	STP
5	Port Channel PAgP	RSTP
6	Port Channel PAgP	PVSTP

La manera de realizar la prueba es la siguiente:

- Se elige una combinación de protocolo de spanning-tree y un tipo de port-channel.
- Se configura la topología con dichos protocolos.
- Se identifica cual es el enlace activo/forwarding y cual se encuentra bloqueado/blocked.
- Se procede a eliminar el enlace activo/forwarding, y se mide la convergencia.
- Se documenta dicho tiempo de ser posible.

Finalmente se elige como propuesta final aquel escenario que presente el menor tiempo de convergencia.

**Nota: Se debe adjuntar al manual técnico, screenshots de las configuraciones de cada switch, donde se pueda observar el tipo de stp y port-channel implementados, esto por cada escenario.**

## Restricciones

- La práctica se realizará en grupos de máximo 3 integrantes.
- Todos los integrantes del grupo deben de tener conocimiento del desarrollo de la red.
- Para la calificación se debe de presentar la práctica en una computadora de los integrantes del grupo.
- **Las configuraciones deben de realizarse desde consola, no en la interfaz gráfica, si se configuran desde la interfaz tendrá nota de 0.**
- Se debe de crear un repositorio de GitHub donde se irá actualizando el desarrollo de la práctica, el cual debe de contener como mínimo 2 commits por semana por parte de cada uno de los integrantes del grupo.
- Durante la calificación se preguntará información relevante de la práctica para comprobar la autoría del mismo.

- El manual técnico debe ser un pdf con el nombre **Practica2\_Manual\_#grupo.pdf**
- La implementación de la red debe realizarse en EVE-NG y el nombre del archivo debe de ser **Practica2\_Implementacion\_#grupo**.

## Penalizaciones

- Falta de seguimiento de desarrollo continuo por medio de Github tendrá una penalización del 10%.
- Falta de seguimiento de instrucciones conforme al método de entrega (nombre del repositorio) tendrá una penalización del 5%.
- Falta de puntualidad conforme a la entrega tendrá una penalización de la siguiente manera:
  - a. 1-10 minutos – 10%.
  - b. 11-59 minutos – 30%.
  - c. Pasados 60 minutos tendrá una nota de 0 y no se calificará.

## Observaciones

- Programa a utilizar: **Eve-NG**
- Durante la calificación se solicitará a los estudiantes, agregar host nuevos a una red/vlan, y se solicitará que realicen las configuraciones necesarias en los equipos para su correcto funcionamiento.
- La entrega se realizará por medio de **Github**, cada grupo deberá crear un repositorio con el nombre: **REDES2\_1S2021\_P2\_GRUPO#**, ejemplo: **REDES2\_1S2021\_P2\_GRUPO3**, y agregar a su auxiliar correspondiente como colaborador del mismo, para poder analizar su progreso y finalmente a partir del mismo repositorio realizar la calificación correspondiente.
- Además de tener a su auxiliar como colaborador del repositorio para tener un control y orden de las personas que entreguen deberán de colocar el Link de su repositorio en la Tarea que cada auxiliar asignará en su plataforma correspondiente.
- Fecha y hora de entrega: **Miércoles 24 de Febrero, antes de las 23:59 horas.**
- **Las copias serán penalizadas con una nota de 0 y castigadas según lo indique el reglamento.**

## Anexos

**Tabla Subredes**

Vlan	Dirección de Red	Primera dirección asignable	Última dirección asignable	Dirección de broadcast	Máscara de subred
1	192.168.4.32/27	192.168.4.33	192.168.4.62	192.168.4.63	
20	192.168.4.64/27	192.168.4.65	192.168.4.94	192.168.4.95	
....	.....	.....	.....	.....	

### Vlan BlackHole

Este VLAN es utilizado para asignar a todos los dispositivos que no están en uso.

### Access-List

Una lista de control de acceso o ACL (del inglés, access control list) es un concepto de seguridad informática usado para fomentar la separación de privilegios. Es una forma de determinar los permisos de acceso apropiados a un determinado objeto, dependiendo de ciertos aspectos del proceso que hace el pedido.<sup>1</sup>

Las ACL permiten controlar el flujo del tráfico en equipos de redes, tales como enrutadores y conmutadores. Su principal objetivo es filtrar tráfico, permitiendo o denegando el tráfico de red de acuerdo a alguna condición.

### Convergencia

[STP y Convergencia](#)