Laboratorio Evaluación: VLANs, VTP, Router-on-a-Stick y Seguridad de Puertos

Contexto:  
Eres el administrador de red del Departamento de Informática de una universidad. La red está segmentada por VLANs: Administración académica (VLAN 10), Tesorería (VLAN 20) y Soporte técnico (VLAN 30). Cada PC tiene asignado un puerto específico del switch y la seguridad exige que ningún otro dispositivo pueda conectarse por error o intento de intrusión.

# Objetivos

- Implementar VLANs y propagar configuración usando VTP.  
- Configurar enlaces troncales entre switches.  
- Habilitar Router-on-a-Stick para comunicación entre VLANs.  
- Aplicar seguridad de puertos con port-security.  
- Diagnosticar eventos de seguridad usando comandos de verificación.

# Instrucciones Generales:

* Utiliza el **modo CLI** para toda la configuración.
* Guarda frecuentemente con el comando write memory o copy running-config startup-config.
* Al terminar, realiza las pruebas de conectividad y toma capturas según se indica.
* Guarda tu archivo Packet Tracert con tu nombre, apellido, carrera, sección **(ej:JuanitoPérezIECIS1)**, utiliza el mismo nombre para guardar el archivo con tus respuestas (Word o PDF) y sube ambos a la plataforma.
* Esta guía esta formulada para desarrollarse en el laboratorio y entregada al final de la clase.

# Instrucciones:

1. Cambie los nombres de los dispositivos de red (switches y router) en el intérprete de comando ocupando el comando **hostname**, recuerde grabar sus configuraciones (en SW y Router) con el comando **WR**.
2. Utilice los **siguientes bloques ip** para asignarles dirección a los dispositivos de acuerdo a la VLAN a la que pertenecen, cuidando de dejar la **primera ip utilizable como gateway**.

|  |  |  |
| --- | --- | --- |
| **VLAN** | **Identificador de Red** | **Máscara** |
| ADMINISTRACION (VLAN 10) | 192.168.10.0 | 255.255.255.0 |
| TESORERIA (VLAN 20) | 192.168.20.0 | 255.255.255.0 |
| TECNICO (VLAN 30) | 192.168.30.0 | 255.255.255.0 |

1. Configura **los enlaces troncales** entre switches y hacia el router.
2. Configura VTP en el switch **SWPISO1** (modo VTP Server).
3. Dominio: redes
4. Contraseña: CDR123 (VTP Password)
5. Crea las VLANs en **SWPISO1** utilizando los nombre y números de las tablas.
6. Configura **SWPISO2** y **SWPISO3** como VTP Clients y verifica propagación de VLANs.
   1. **show vtp status**
   2. **show vlan brief**
7. Configura las Interfaces de los switches para los siguientes rangos

|  |  |
| --- | --- |
| **Vlan** | **Interface** |
| ADMINISTRACION (VLAN 10) | Fa0/1- Fa0/10 |
| TESORERIA (VLAN 20) | Fa0/11- Fa0/20 |
| TECNICO (VLAN 30) | Fa0/21- Fa0/22 |

* 1. Deja una captura de tus resultados al aplicar **show vlan brief** en los switches configurados.

1. Configure Router-on-a-Stick en **RCENTRAL**, creando subinterfaces para cada VLAN
2. Verifique **conectividad** entre todas las PCs, utilizando **“Add Simple PDU”** (la cartita) en modo tiempo real.

|  |  |  |
| --- | --- | --- |
| **Source** | **Destination** | **Type** |
| Administracíon1 | Técnico3 | ICMP |
| Administracíon1 | Tesorería3 | ICMP |
| Administracíon1 | Administracíon3 | ICMP |
| Tesorería1 | Administracíon2 | ICMP |
| Tesorería1 | Tesorería2 | ICMP |
| Tesorería1 | Técnico2 | ICMP |
| Técnico1 | Tesorería3 | ICMP |
| Técnico1 | Administracíon2 | ICMP |

1. Use la herramienta de simulación con el filtro activado para **ICMP** y capture una trama en algún switch y responda:
2. Deje una captura de pantalla de la trama utilizada
3. ¿Qué VLAN ID aparece en la trama capturada?
4. ¿Qué dirección MAC de origen y destino se observa?
5. ¿Qué sucede si el puerto troncal no se configura correctamente?
6. Si un switch recibe por un troncal una trama etiquetada con una VLAN que **no tiene en su base de datos**, ¿qué hará con esa trama?
7. Configura **seguridad de puertos** en los puertos de acceso donde se conectan los PCs:
8. Solo una MAC permitida (máximo 1).
9. Habilita sticky MAC.
10. Configura acción de violación: shutdown.
11. Simula un cambio de dispositivo (cambia un PC por el PC INTRUSO) y verifica si el puerto es desactivado.
12. Toma una captura de pantalla al ejecutar el comando **show port-security** en los switches en los que hayas configurado seguridad de puerto
13. Toma una captura de pantalla de la información de seguridad del puerto donde simulaste el cambio de dispositivo (**show port-security interface f 0/x**)
14. ¿Por qué es necesario configurar port-security si ya tenemos segmentación por VLAN?
15. ¿Qué ventajas tiene usar sticky MAC frente a direcciones estáticas?

# Rúbrica de Evaluación:

|  |  |  |
| --- | --- | --- |
| **Criterio** | **Descripción** | **Puntaje Máximo** |
| **USER Profile** | Nombre y correo configurado en USER profile del archivo .pkt | 2 |
| **Direccionamiento** | Asignación correcta de IP, máscara y gateway en PCs y subinterfaces del router | 6 |
| **Hostname** | Cambio de nombre en switches y router según lo indicado en la guía | 3 |
| **Guardar configuración** | Uso del comando 'wr' para guardar la configuración en todos los dispositivos | 2 |
| **Interfaces troncales** | Configuración de interfaces troncales | 5 |
| **Creación de VLANs** | VLANs creadas en SWPISO1 con nombre e ID según guía | 5 |
| **Asignación de puertos** | Puertos asignados a VLANs y configurados como 'access' en los 3 switches | 6 |
| **VTP servidor** | Configuración de VTP en SWPISO1 como servidor con dominio 'redes' y clave 'CDR123' | 5 |
| **VTP clientes** | Configuración de VTP en SWPISO2 y SWPISO3 como clientes | 5 |
| **Propagación de VLANs** | Verificación de traspaso correcto de VLANs desde el servidor | 4 |
| **Capturas VLAN/VTP** | Capturas de 'show vlan brief' en los 3 switches | 3 |
| **Router-on-a-Stick** | Configuración completa de subinterfaces en RCENTRAL con IP y encapsulación | 6 |
| **Pruebas de conectividad** | Verificación de ping exitoso entre PCs de distintas VLANs | 4 |
| **Port-security** | Configuración de seguridad en puertos de acceso: 1 MAC, sticky y violation shutdown | 6 |
| **Simulación de intrusión** | Cambio de equipo en un puerto seguro para generar violación de seguridad | 4 |
| **Captura de show port-security interface** | Captura del estado tras la violación en la interfaz testeada | 2 |
| **Captura de show port-security** | Captura general en todos los switches con seguridad activa | 2 |
| **Captura de trama** | Captura en Simulación Mode de una trama con etiqueta VLAN | 3 |
| **Pregunta: VLAN ID** | Respuesta escrita del VLAN ID de la trama | 2 |
| **Pregunta: MAC origen y destino** | Respuesta de ambas direcciones MAC observadas | 2 |
| **Pregunta: Campo 802.1Q** | Explicación del campo y diferencia con trama sin VLAN | 4 |
| **Pregunta: puerto troncal mal configurado** | Efecto de no configurar correctamente el trunk | 3 |
| **Pregunta: VLAN no existente** | Qué sucede si una VLAN no está en el switch receptor | 3 |
| **Pregunta: ¿por qué port-security si hay VLAN?** | Fundamentación del uso de seguridad adicional | 3 |
| **Pregunta: ventajas de sticky MAC** | Comparación entre sticky y MAC estática | 3 |
|  | **Total** | **93** |