**Ejercicio 13: Configuración básica de VLANs**

.

A diagram of a computer network

Description automatically generated

# **Objetivos:**

# Conocer la utilidad de la programación de VLANs.

# Interconectar VLANs distintas.

Un método para proporcionar enrutamiento y conectividad para varias VLAN es mediante el uso de un **enlace troncal 802.1Q** entre uno o más switches y una sola interfaz del router. Este método también se conoce como enrutamiento entre VLANs de **router-on-a-stick**. En este método, la interfaz del ruteador se divide en varias subinterfaces que proporcionan rutas lógicas a todas las VLAN conectadas.

En este ejercicio, configuraremos el enrutamiento entre VLANs basado en troncales y verificaremos la conectividad a los hosts en diferentes VLANs, así como también con un loopback en el router.

Nuestro objetivo es lograr la interconexión de VLANs, en este caso la **VLAN 10** de **Estudiantes** y la **VLAN 20** de la **Facultad**. Estas subredes no pueden comunicarse, solamente si pertenecieran a la misma VLAN. Para poder comunicarse entre VLANs distintas requerimos un router, ya que el router toma decisiones capa 3. De manera nativa los switches no pueden realizar este proceso, ya que los switches no toman decisiones o rutean.

Tenemos en cada VLAN dominios distintos de broadcast o subredes. Utiliza e diseño lógico de la red (segmentación de tráfico) de la siguiente tabla:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Segmento** | **VLAN** | **Puertos asignados** | **Dirección de subred** | **Máscara de subred** |
| **Estudiantes** | 10 | F0/3-10 | 192.168.10.0 | 255.255.255.0 |
| **Facultad** | 20 | F0/11-18 | 192.168.20.0 | 255.255.255.0 |
| **Nativa** | 1 | No aplica | 192.168.1.0 | 255.255.255.0 |

# **Tabla de direccionamiento:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Dispositivo** | **Interface** | **IP Address** | **Máscara de subred** | **Default Gateway** |
| R1 | G0/1.1 | 192.168.1.1 | 255.255.255.0 | N/A |
|  | G0/1.10 | 192.168.10.1 | 255.255.255.0 | N/A |
|  | G0/1.20 | 192.168.20.1 | 255.255.255.0 | N/A |
| S1 | VLAN 1 | 192.168.1.11 | 255.255.255.0 | 192.168.1.1 |
| S2 | VLAN 1 | 192.168.1.12 | 255.255.255.0 | 192.168.1.1 |
| PC0 | NIC | Asignada por DHCP | Asignada por DHCP | Asignada por DHCP |
| PC1 | NIC | Asignada por DHCP | Asignada por DHCP | Asignada por DHCP |
| PC2 | NIC | Asignada por DHCP | Asignada por DHCP | Asignada por DHCP |
| PC3 | NIC | Asignada por DHCP | Asignada por DHCP | Asignada por DHCP |

Para lograr la conectividad entre los equipos de las VLANs, se sugiere proceder con el siguiente orden:

1. Completar la configuración del switch **S1** y **S2**.

* Configurar la **VLAN1** con los datos de la tabla y el **default Gateway**.
* Desactivar administrativamente todos los puertos no utilizados en el switch.

1. Configurar las **VLANs** en los switches **S1** y **S2**:
2. Creación de las VLANs.
3. Definición de los tipos de puertos que se va a utilizar: acceso o troncal.
4. Asignación de puertos a las VLANs y definición de los puertos de acceso.
5. Definición de los puertos troncales.

Verifique en cada switch los nombres y números de VLAN con el comando: **sh vlan brief**.

1. Configurar las **subinterfaces** en el router **R1**:

Configurar **R1** para enrutar a varias VLANs mediante la creación de subinterfaces para cada VLAN. Este método de enrutamiento entre VLANs se denomina **router-on-a-stick**. El enrutamiento entre VLANs **router-on-a-stick** permite rutear por una interfaz múltiples VLANs.

1. Configurar una subinterface para la VLAN 1.
2. Configurar una subinterface para la VLAN 10.
3. Configurar una subinterface para la VLAN 20.
4. Configurar el servicio DHCP para entregar direccionamiento dinámico a las VLANs de **Students** y **Faculty**.
5. Configurar en **R1** una ruta por default hacia el ISP.
6. Configurar en el **ISP** rutas estáticas hacia las subredes de las VLANs 1, 10 y 20.
7. Al terminar la configuración realiza las **pruebas de conectividad** necesarias para comprobar la conexión entre los dispositivos:

Configurar medidas de seguridad básicas en el router

1. Encripte las contraseñas de texto no cifrado.

R1(config)# **service password-encryption**

2. Refuerce las contraseñas.

Un administrador debe garantizar que las contraseñas cumplan con las pautas estándar para contraseñas seguras. Estas pautas podrían incluir combinar letras, números y caracteres especiales en la contraseña y establecer una longitud mínima.

* + 1. Cambie la contraseña cifrada del modo EXEC privilegiado según las pautas.

R1(config)# **enable secret Enablep@55**

* + 1. Exija que se utilice un mínimo de 10 caracteres para todas las contraseñas.

R1(config)# **security passwords min-length 10**

3. Proteja las líneas de consola y VTY.

* + 1. Puede configurar el router para que se cierre la sesión de una conexión que estuvo inactiva durante un período especificado. Si un administrador de red inicia sesión en un dispositivo de red y, de repente, se debe ausentar, este comando cierra automáticamente la sesión del usuario después de un plazo especificado. Los siguientes comandos harán que se cierre la sesión de la línea después de cinco minutos de inactividad.

R1(config)# **line console 0**

R1(config-line)# **exec-timeout 5 0**

R1(config-line)# **line vty 0 4**

R1(config-line)# **exec-timeout 5 0**

R1(config-line)# **exit**

R1(config)#

* + 1. El siguiente comando impide los intentos de inicio de sesión por fuerza bruta. Si alguien falla en dos intentos en un período de **120 segundos**, el router bloquea los intentos de inicio de sesión durante **30 segundos**. Este temporizador está configurado en un valor especialmente bajo para esta actividad de laboratorio.

R1(config)# **login block-for 30 attempts 2 within 120**

4. Verifique que todos los puertos sin usar estén inhabilitados.

Los puertos del router están inhabilitados de manera predeterminada, pero siempre es prudente verificar que todos los puertos sin utilizar tengan un estado inactivo en términos administrativos. Esto se puede verificar rápidamente emitiendo el comando **show ip interface brief**. Todos los puertos sin utilizar que no estén en un estado inactivo en términos administrativos se deben inhabilitar por medio del comando **shutdown** en el modo de configuración de la interfaz.

R1#**sh ip interface brief**

Interface IP-Address OK? Method Status Protocol

GigabitEthernet0/0 unassigned YES unset administratively down down

GigabitEthernet0/1 unassigned YES unset up up

GigabitEthernet0/1.1 192.168.1.1 YES manual up up

GigabitEthernet0/1.10 192.168.10.1 YES manual up up

GigabitEthernet0/1.20 192.168.20.1 YES manual up up

Serial0/0/0 190.40.0.18 YES manual up up

Serial0/0/1 unassigned YES unset administratively down down

Vlan1 unassigned YES unset administratively down down

Emita el comando **show running-config** en la petición del modo EXEC privilegiado para ver la configuración de seguridad que aplicó.

Configurar medidas de seguridad básicas en el switch S1

1. Encripte las contraseñas de texto no cifrado.

S1(config)# **service password-encryption**

2. Refuerce las contraseñas en el switch.

Cambie la contraseña cifrada del modo EXEC privilegiado según las pautas de contraseñas seguras.

S1(config)# **enable secret Enablep@55**

**Nota**: el comando de seguridad **password min-length** no está disponible en el switch 2960.

3. Proteja las líneas de consola y VTY.

* + 1. Configure el switch para que se cierre una línea que haya estado inactiva durante 10 minutos.

S1(config)# **line console 0**

S1(config-line)# **exec-timeout 10 0**

S1(config-line)# **line vty 0 15**

S1(config-line)# **exec-timeout 10 0**

S1(config-line)# **exit**

S1(config)#

4. Verifique que todos los puertos sin usar estén inhabilitados.

Los puertos del switch están habilitados de manera predeterminada. Desactive todos los puertos que no se estén usando en el switch.

* + 1. Puede verificar el estado de los puertos del switch emitiendo el comando **show ip interface brief**.

S1#

S1#**sh ip interface brief**

Interface IP-Address OK? Method Status Protocol

FastEthernet0/1 unassigned YES manual up up

FastEthernet0/2 unassigned YES manual up up

FastEthernet0/3 unassigned YES manual down down

FastEthernet0/4 unassigned YES manual up up

FastEthernet0/5 unassigned YES manual down down

FastEthernet0/6 unassigned YES manual down down

FastEthernet0/7 unassigned YES manual down down

FastEthernet0/8 unassigned YES manual down down

FastEthernet0/9 unassigned YES manual down down

FastEthernet0/10 unassigned YES manual down down

FastEthernet0/11 unassigned YES manual down down

FastEthernet0/12 unassigned YES manual down down

FastEthernet0/13 unassigned YES manual down down

FastEthernet0/14 unassigned YES manual down down

FastEthernet0/15 unassigned YES manual down down

FastEthernet0/16 unassigned YES manual up up

FastEthernet0/17 unassigned YES manual down down

FastEthernet0/18 unassigned YES manual down down

FastEthernet0/19 unassigned YES manual down down

FastEthernet0/20 unassigned YES manual down down

FastEthernet0/21 unassigned YES manual down down

FastEthernet0/22 unassigned YES manual down down

FastEthernet0/23 unassigned YES manual down down

FastEthernet0/24 unassigned YES manual down down

GigabitEthernet0/1 unassigned YES manual down down

GigabitEthernet0/2 unassigned YES manual down down

Vlan1 192.168.1.11 YES manual up up

S1#

* + 1. Use el comando **interface range** para desactivar varias interfaces a la vez.

S1(config)# interface f0/3

S1(config-if-range)# shutdown

S1(config-if-range)# exit

S1(config)# **interface range f0/5-15, f0/17-24, g0/1-2**

S1(config-if-range)# **shutdown**

S1(config-if-range)# **end**

S1#

* + 1. Verifique que todas las interfaces inactivas tengan un estado inactivo en términos administrativos.

S1#**sh ip interface brief**

Interface IP-Address OK? Method Status Protocol

FastEthernet0/1 unassigned YES manual up up

FastEthernet0/2 unassigned YES manual up up

FastEthernet0/3 unassigned YES manual administratively down down

FastEthernet0/4 unassigned YES manual up up

FastEthernet0/5 unassigned YES manual administratively down down

FastEthernet0/6 unassigned YES manual administratively down down

FastEthernet0/7 unassigned YES manual administratively down down

FastEthernet0/8 unassigned YES manual administratively down down

FastEthernet0/9 unassigned YES manual administratively down down

FastEthernet0/10 unassigned YES manual administratively down down

FastEthernet0/11 unassigned YES manual administratively down down

FastEthernet0/12 unassigned YES manual administratively down down

FastEthernet0/13 unassigned YES manual administratively down down

FastEthernet0/14 unassigned YES manual administratively down down

FastEthernet0/15 unassigned YES manual administratively down down

FastEthernet0/16 unassigned YES manual up up

FastEthernet0/17 unassigned YES manual administratively down down

FastEthernet0/18 unassigned YES manual administratively down down

FastEthernet0/19 unassigned YES manual administratively down down

FastEthernet0/20 unassigned YES manual administratively down down

FastEthernet0/21 unassigned YES manual administratively down down

FastEthernet0/22 unassigned YES manual administratively down down

FastEthernet0/23 unassigned YES manual administratively down down

FastEthernet0/24 unassigned YES manual administratively down down

GigabitEthernet0/1 unassigned YES manual administratively down down

GigabitEthernet0/2 unassigned YES manual administratively down down

Vlan1 192.168.1.11 YES manual up up

S1#

* + 1. Emita el comando **show running-config** en la petición del modo EXEC privilegiado para ver la configuración de seguridad que aplicó.