**Ejercicio 18: Extiende el tamaño de tus VLANs**

.

**Topología:**

A diagram of a network

Description automatically generated

1. Identifica el direccionamiento que se requiere para configurar las IPs de todos los **switches** y su **default gateway** en la **VLAN nativa**.

Recuerda que tenemos en cada VLAN dominios distintos de broadcast o subredes. Utiliza el diseño lógico de la red (segmentación de tráfico) de la siguiente tabla:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Segmento** | **VLAN** | **IPs** | **Puertos asignados** | **Orden** | **Dirección de subred** | **Máscara de subred** | **Prefijo de red** |
| **Management** | **10** | **10** | F0/1-6 | **2** | **192.168.1.128** | **255.255.255.240** | **28** |
| **Users** | **20** | **120** | F0/7-19 | **1** | **192.168.1.0** | **255.255.255.128** | **25** |
| **Services** | **30** | **5** | F0/20-24 | **3** | **192.168.1.144** | **255.255.255.248** | **29** |
| **Native** | **1** | **5** | No aplica | **4** | **192.168.1.152** | **255.255.255.248** | **29** |

1. Asigna direcciones IP válidas a las **VLANs 1** de los switches y a la subinterface **g0/0.1** del ruteador. Por

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Dispositivo** | **Interface** | **Dirección IP** | **Máscara de subred** | **Default Gateway** |
| RFrontera | G0/0.1 | **192.168.1.158** | **255.255.255.248** | N/A |
| SCompany | VLAN 1 | **192.168.1.153** | **255.255.255.248** | **192.168.1.158** |
| SUsers | VLAN 1 | **192.168.1.154** | **255.255.255.248** | **192.168.1.158** |
| SManagers | VLAN 1 | **192.168.1.155** | **255.255.255.248** | **192.168.1.158** |
| SServices | VLAN 1 | **192.168.1.156** | **255.255.255.248** | **192.168.1.158** |

1. Completa la configuración del **RFrontera**.
2. Realiza la configuración básica en los switches **SManagers** y **SServices**.
3. Crea la **base de datos de las VLANs** en todos los switches.
4. Configura los **puertos de acceso** a las VLANs correspondientes en los switches **SManagers**, **SUsers** y **SServices**.
5. Configura los **puertos troncales** en todos los switches.
6. Configura la dirección IP de la **VLAN 1** en todos los switches y su default gateway.
7. Al terminar la configuración realiza las **pruebas de conectividad** necesarias para comprobar la conexión entre los dispositivos.

* Conexión entre dispositivos que pertenecen a la misma VLAN.
* Conexión entre dispositivos que pertenecen a VLANs distintas.
* Conexión de mis dispositivos hacia el servidor externo CNN.
* Conexión por telnet del servidor **CNN** hacia todas las IPs de los switches.

**Introducción:**

**La vlan nativa** se usa para el tráfico de vlan sin etiquetar. La vlan nativa es utiliza para que todos aquellos frames (datagramas) que no incluyen una etiqueta (tag), osea untagged, sean enviados a la vlan nativa y asi se descartan. Si lo quieres ver desde un punto de vista de seguridad, la vlan nativa ayuda a evitar algún tipo de amenaza, donde se descartan aquellos datagramas que no cuentan con una etiqueta que indique a que vlan corresponden.

La **vlan de administración** se usa para la configuración de los switches.

Aunque la vlan nativa y la vlan de administracion pueden ser la misma, por buena práctica se recomienda que sean totalmente distintas.

 La vlan de administracion se recomienda que se aplique a todos los switches (igual la vlan nativa), esta vlan de administracion sera unicamente una, donde se asociara al default gateway, y deben estar en el mismo segmento de red, tanto el SVI, como el default gateway, ejemplo:

vlan 100

name VLAN-ADMINISTRATIVA

interface vlan 100

description VLAN-ADMINISTRATIVA

ip address **172.16.100**.10 255.255.255.0

no shut

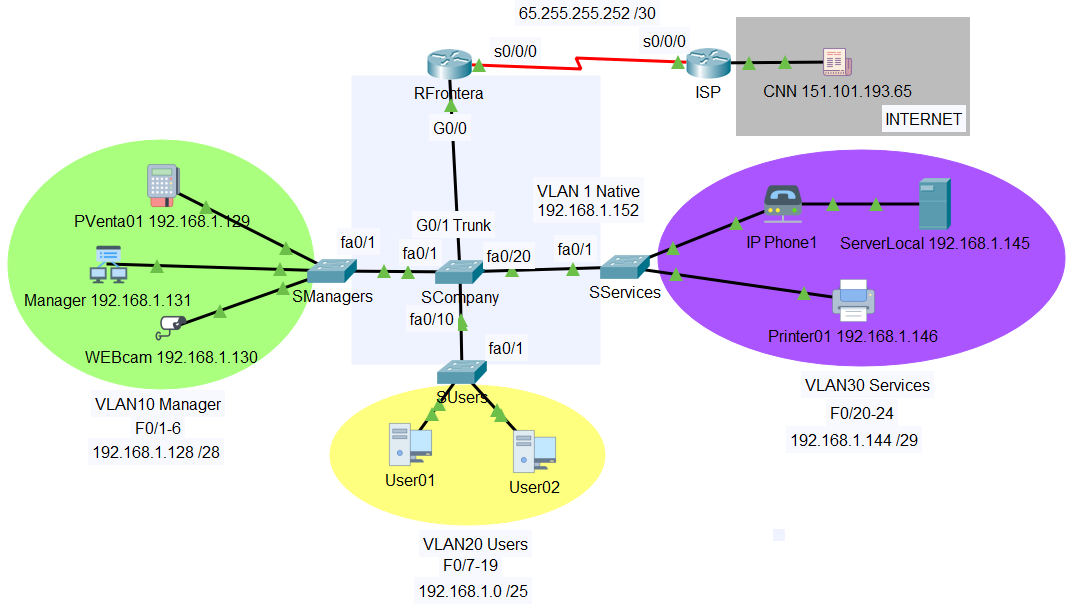
ip default-gateway **172.16.100**.1

Cuando te dice que la vlan de administración estara activa unicamente cuando esta conectando a otro switches es que por ejemplo la vlan esta fluyendo a traves de un enlace trunk entre 2 switches, de lo contrario si ejecutas un **show ip interface brief**, veras que el estado es UP - DOWN.

OJO, por buena practica se recomienda que la vlan de administracion sea unicamente para ese rol, igual que la vlan nativa, no debe ser asignado a ningun departamento a ningun usuario. Recuerda que si tienes multiples vlans, necesitas un equipo capa 3 (como un router, firewall o switch multicapa) para habilitar la comunicacion entre todas las vlans, de esta manera desde tu red de IT podras tener comunicacion con la vlan de administracion, osea, gracias al inter vlan routing.

El enlace troncal

1. vlan de administracion: estas la que se va a usar para la configuracion del switch
2. enlace troncal: son los que transportan el trafico de las vlan a otros dispositivos de red
4. los enlaces troncales se configuran en la vlan nativa para que el trafico sin etiquetar se mande por o ahi o se configuran a parte
6. y otra cosa que no me queda clara es que en la vlan de administracion para que la interfaz SVi este activa tiene que haber un dispositivo conectada a la misma. osea que por ejemplo para el depto de infraestructura yo le tendria que asiga la vlan de administración?
7. Extiende el tamaño de las VLANs agregando los switches **SManagers** y **SServices**.
8. Conecta el puerto fa0/1 del switch **SManagers** al puerto fa0/1 (F0/1-6) del Switch **SCompany**.
9. Conecta el puerto fa0/1 del switch **SUsers** al puerto fa0/10 (F0/7-19) del Switch **SCompany**.
10. Conecta el puerto fa0/1 del switch **SServices** al puerto fa0/20 (F0/20-24)del Switch **SCompany**.



1. Identifica la **máscara de subred** que se requiere para configurar las IPs de todos los **switches** y su **default gateway** en la **VLAN nativa**.

Recuerda que 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** |
| **Management** | 10 | F0/1-6 | 192.168.1.128 | 255.255.255.240 |
| **Users** | 20 | F0/7-19 | 192.168.1.0 | 255.255.255.128 |
| **Services** | 30 | F0/20-24 | 192.168.1.144 | 255.255.255.248 |
| **Native** | 1 | No aplica | 192.168.1.152 | **255.255.255.248** |

# Asigna direcciones IP válidas a las **VLANs 1** de los switches y a la subinterface **g0/0.1** del ruteador.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Dispositivo** | **Interface** | **IP Address** | **Máscara de subred** | **Default Gateway** |
| RFrontera | G0/0.1 | **192.168.1.158** | **255.255.255.248** | N/A |
| SCompany | VLAN 1 | 192.168.1.153 | **255.255.255.248** | **192.168.1.158** |
| SUsers | VLAN 1 | **192.168.1.154** | **255.255.255.248** | **192.168.1.158** |
| SManagers | VLAN 1 | **192.168.1.155** | **255.255.255.248** | **192.168.1.158** |
| SServices | VLAN 1 | **192.168.1.156** | **255.255.255.248** | **192.168.1.158** |

1. Realiza la configuración básica en los switches **SManagers** y **SServices**.
2. Crea la **base de datos de las VLANs** en todos los switches.
3. Define los puertos del **f0/2-24** del switch **SManagers** como puertos de acceso a la **VLAN 10**.
4. Define los puertos del **f0/2-24** del switch **SServices** como puertos de acceso a la **VLAN 30**.
5. Configura los **puertos troncales** en todos los switches.
6. Al terminar la configuración realiza las **pruebas de conectividad** necesarias para comprobar la conexión entre los dispositivos.

* Conexión entre dispositivos que pertenecen a la misma VLAN.
* Conexión entre dispositivos que pertenecen a VLANs distintas.
* Conexión de mis dispositivos hacia el servidor externo CNN.
* Conexión por telnet del servidor CNN hacia todas las IPs de los switches.