

Estudiante: Nathaly Ma deline  
Flores Quispe

## TAREA #2 SWITCHES ETHERNET

Un switch ethernet es un dispositivo de red que conecta múltiples dispositivos dentro de una red local (LAN), permitiendo que se comuniquen entre sí. Funciona en la capa de enlace de datos del modelo OSI.

Funciones principales:

- **Commutación:** distribuye datos entre los dispositivos según la dirección MAC, asegurando que los datos lleguen solo a su destino.
- **Segmentación de red:** mejora el rendimiento al reducir colisiones al segmentar redes en subredes menores.

### 1. Protocolo 802.1Q

El protocolo es un estándar de red para la creación de VLANs (Redes de Área Local Virtuales) en redes Ethernet.

Fundamentación:

- **Etiquetas VLAN:** agrega una etiqueta al marco (frame) de Ethernet, lo que permite identificar la VLAN a la que pertenece el tráfico. Esta etiqueta incluye un identificador de VLAN (VLAN ID) de 12 bits, permitiendo hasta 4096 VLANs diferentes.

- **Tráfico:** cuando un switch recibe un marco con un tag de VLAN puede procesar y dirigir el tráfico apropiadamente a los puertos de la VLAN correspondiente.

• **Sencillez y eficiencia:**

- Reduce la congestión de la red al segmentar el tráfico.
- Mejora la seguridad ya que se puede limitar el acceso a los recursos de la red.

• **Implementación:**

- Los dispositivos de red (switches) deben ser compatibles con el protocolo para gestionar correctamente el tráfico etiquetado.

• **Ventajas:**

- Gestión centralizada.
- Mayor flexibilidad en la administración de la red.
- Reducción de la complejidad de seguridad.

## 2- VLAN (Redes de Área Local Virtual)

Las VLAN son redes lógicas que permiten segmentar una red física en varias redes independientes, mejorando el rendimiento y la seguridad.

### Características de las VLAN

■ Por defecto = la VLAN por defecto en un switch es generalmente la VLAN 1. Cuando se conecta un dispositivo a un puerto de un switch sin una VLAN específica configurada, este dispositivo se le asigna automáticamente a la VLAN por defecto.

Implicaciones = los dispositivos en esta VLAN pueden comunicarse entre sí, pero no pueden comunicarse directamente con dispositivos en otras VLAN a menos que hayan un router o un switch de capa 3 que realice el enrutamiento.

■ Nativa = la VLAN nativa es aquella que se configura en el puerto de un switch que realiza el tagging de frames 802.1Q. Esta VLAN es transparente para el tráfico sin etiquetas.

Funcionalidad = cualquier frame que no esté etiquetado es tratado como perteneciente a la VLAN nativa. Esto es especialmente relevante en configuraciones trunk (trunking) donde múltiples VLAN son transportadas a través de un solo enlace.

Seguridad = es importante configurar adecuadamente la VLAN nativa para evitar ataques, como el VLAN hopping, donde un atacante podría hacer que su tráfico sea interpretado como proveniente de la VLAN nativa.

■ Administración = las VLAN permiten una mejor administración de la red, facilitando la gestión del tráfico y la implementación de políticas de seguridad.

Implementación = los administradores pueden crear, modificar y eliminar VLANs según

necesidades. Esto incluye asignar archivos de configuración específicos a puertos, definir la cantidad de VLANs requeridas y asegurar que el tráfico entre VLANs esté controlado mediante ACLs (Listas de Control de Acceso).

Ventajas:

- Mejora la eficiencia del tráfico de red al reducir el dominio de difusión.
- Fomenta la segregación de grupos de trabajo y departamentos, permitiendo que la comunicación interna se mantenga privada y segura dentro de cada VLAN.

### 3. Relación a una VLAN

Está determinada por la configuración del puerto en el switch.

Asignación de Puertos: cada puerto puede ser asignado a una VLAN específica. Los dispositivos conectados a ese puerto podrán comunicarse solo con otros dispositivos dentro de la misma VLAN, a menos que haya un enrutador o un switch de capa 3 para interconectar VLANs.

Ventajas:

- Segmentación de Red, permite dividir una red física en varias redes lógicas.
- Mejora del rendimiento, reduce la cantidad del tráfico en la red, ya que los broadcast se limitan a la VLAN correspondiente.
- Facilidad de gestión, permite mover, agregar o cambiar dispositivos con facilidad sin modificar la infraestructura física.
- Reducción de costos, minimiza la necesidad de hardware adicional al optimizar la infraestructura de red existente.

4º Puede un elemento de red (ejemplo un servidor) pertenecer a 2 o más VLANs?

Dar ejemplo si es posible

Sí, un elemento de red, como un servidor, puede pertenecer a múltiples VLANs utilizando un enfoque conocido como "VLANs Trunking".

Ejemplo:

- Configuración de Trunking: si un servidor tiene múltiples interfaces de red, cada una configurada en diferentes VLANs, puede recibir tráfico de varias VLANs. Por ejemplo, un servidor puede tener una interfaz en la VLAN 10 y otra en la VLAN 20, permitiendo la comunicación simultánea con diferentes segmentos de la red.
- Configuración del Switching: la configuración de los switches debe permitir el trunking para que el tráfico de diferentes VLANs fluya a través del mismo enlace físico.