UNIVERSIDAD DE LAS FUERZAS ARMADAS "ESPE"
DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN
REDES DE COMUNICACIÓN

Integrantes: Mathius Moyano, Vinicio Guaman, Anthonny Chavez, Michelle Perugachi.
NRC: 9910
Fecha: 07/06/20223
Tema: VLANS

VLANs

Las VLAN (Virtual Local Area Networks) es un grupo de puertos que permite a los dispositivos comunicarse entre sí a través de la capa Ethernet MAC, independientemente de la red de área local (LAN) física. Un puerto es miembro de una VLAN si puede enviar y recibir datos de la VLAN. Un puerto es un miembro sin etiqueta de una VLAN si todos los paquetes destinados a ese puerto en la VLAN no tienen etiqueta VLAN. Un puerto es un miembro etiquetado de una VLAN si todos los paquetes destinados a ese puerto en la VLAN tienen una etiqueta VLAN. Las VLAN se suelen utilizar para aislar los terminales como grupo de trabajo.

Cada VLAN actúa como una red lógica independiente, con sus propias políticas de seguridad y configuraciones de red. Los dispositivos dentro de una VLAN pueden comunicarse entre sí de manera transparente, como si estuvieran conectados a la misma red física, aunque puedan estar en diferentes ubicaciones físicas.

- **Diferencia entre LAN y VLAN**

  - **Alcance:** Una LAN tradicional es una red física que conecta dispositivos en una ubicación geográfica limitada, mientras que una VLAN es una red lógica que puede agrupar dispositivos de diferentes ubicaciones físicas en una misma red virtual.
  - **Segmentación:** En una LAN tradicional, todos los dispositivos están en el mismo segmento de red y pertenecen a la misma red broadcast. En una VLAN, los dispositivos se agrupan lógicamente en diferentes redes virtuales y pueden estar aislados del tráfico de otras VLAN.
  - **Configuración:** Para establecer una LAN, se requiere la configuración física de los dispositivos de red, como switches y cables, para conectarlos en una topología de red específica. En cambio, una VLAN se configura mediante la configuración de switches de red para etiquetar los paquetes y asignarlos a las VLAN correspondientes.
  - **Flexibilidad y administración:** Una VLAN ofrece una mayor flexibilidad y facilidad de administración, ya que permite la creación de múltiples redes lógicas sobre una infraestructura física común. Esto facilita la administración, la seguridad y el control de tráfico dentro de la red.

Configuracion basica(crea y se asignan puertos)

Creación VLAN

```
Switch>enable
```

Para configurar VLANs debemos pasar del modo usuario al modo privilegiado con el comando ***enable***.

```
Switch#config t
```

Luego vamos a configuración global con el comando ***config t***

```
Switch(config)#hostname CONF-BASICVLANS
```

Luego le damos un nombre al Switch con el comando ***hostname NAME***.

```
CONF-BASICVLANS(config)#vlan 10
```

Para crear VLANs le damos un número a la VLAN en este caso será el número 10, lo hacemos mediante el comando ***vlan numberVLAN***.

```
CONF-BASICVLANS(config-vlan)#name REDES9910
```

Luego le damos un nombre a la VLAN en este caso REDES9910, mediante el comando ***name NOMBREVLAN***.

Asignación de puertos

```
CONF-BASICVLANS(config)#int range fa0/10-14
```

Para asignar puertos en este ejemplo, lo hacemos desde el modo de configuración de interfaz con el comando ***int range INTERFACE_A_USAR***, para nuestro ejemplo int range fa0/10-14.

```
CONF-BASICVLANS(config-if-range)#switchport mode access
```

Luego configuramos la interfaz en el modo “access”, mediante el comando ***switchport mode access***.

```
CONF-BASICVLANS(config-if-range)#switchport access vlan 10
```

Finalmente para asignar la interfaz a la VLAN 10, lo hacemos mediante el comando ***switchport access vlan NUMBER***.

Puertos de Acceso, Puerto troncal, IEEE 802.1Q (trama)

Puertos de Acceso:

Un puerto de acceso en redes se refiere a un punto de conexión físico o lógico en un dispositivo de red, como un switch, un router o un punto de acceso inalámbrico, que se utiliza para conectar otros dispositivos de red.

En redes de área local (LAN) y las redes de área amplia (WAN), un puerto de acceso se refiere a un puerto físico en un dispositivo de red que proporciona conectividad a otros dispositivos de red, como computadoras, impresoras, servidores, etc. Estos puertos suelen estar etiquetados con números o nombres para identificarlos, como "Ethernet 1/1", "GigabitEthernet 0/1", "LAN 2", etc.

Cada puerto de acceso está asociado con una interfaz de red específica en el dispositivo y suele utilizarse para conectar un cable de red, como un cable Ethernet, a otro dispositivo o a una toma de red en una pared. Esto permite la transmisión de datos entre los dispositivos conectados a través del puerto de acceso, también existen los puertos de acceso lógicos, que son interfaces virtuales configuradas en un dispositivo de red para segmentar el tráfico de red en diferentes redes virtuales (VLANs) o para proporcionar servicios específicos, como puertos de administración remota.

Puerto troncal:

Un puerto troncal, "trunk port", es un tipo de puerto utilizado en redes de conmutación (switching) para transportar datos entre diferentes dispositivos de red, como switches o routers.

Un puerto troncal se utiliza principalmente para la configuración de enlaces entre switches o para conectar un switch a un router o a otro dispositivo de red. Su función principal es permitir la transmisión de múltiples VLANs (Virtual Local Area Networks) a través de un solo cable, lo que facilita la segmentación del tráfico y la optimización del rendimiento de la red.

Cuando se configura un puerto como troncal, se utiliza un protocolo de etiquetado de VLAN, como IEEE 802.1Q, para marcar los paquetes de datos con información de VLAN. Esto permite que los paquetes sean transmitidos correctamente entre los diferentes dispositivos de red conectados a través del puerto troncal, manteniendo la separación y la identificación de las VLANs.

IEEE 802.1Q(trama)

Es una modificación al estándar de Ethernet. El protocolo IEEE 802.1Q fue un proyecto del grupo de trabajo 802 de IEEE para desarrollar un mecanismo que permita a múltiples redes interconectadas con puentes o switches compartir transparentemente el mismo medio físico sin problemas de interferencia entre las redes que comparten el medio. Se usa para definir el protocolo de encapsulamiento usado para implementar este mecanismo en redes Ethernet. Permite identificar a una trama como proveniente de un equipo conectado a una red

determinada. Una trama perteneciente a una VLAN sólo se va a distribuir a los equipos que pertenezcan a su misma VLAN, de forma que se separan dominios de broadcast.

Trama

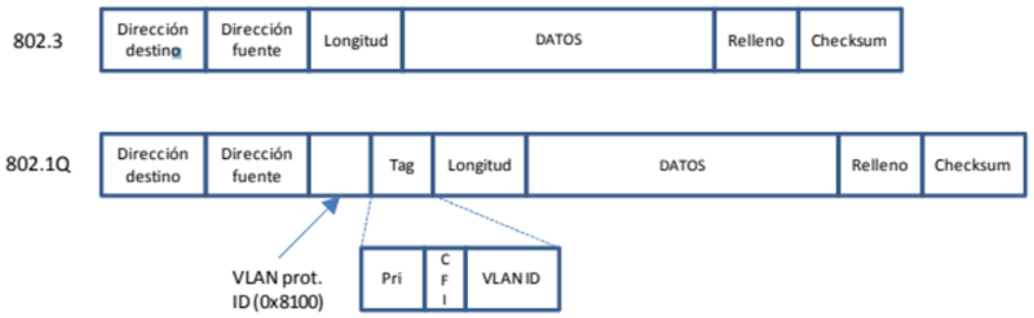
El protocolo 802.1Q propone añadir 4 bytes al encabezado Ethernet original en lugar de encapsular la trama original. El valor del campo EtherType se cambia a 0x8100 para señalar el cambio en el formato de la trama.

La VLAN tag se inserta en la trama Ethernet entre el campo “Dirección fuente” y “Longitud. Los primeros 2 bytes del VLAN tag consisten en el “Tag Type" (tipo de tag) de 802.1Q y siempre está puesto a 0x8100. Los últimos 2 bytes contienen la siguiente información:

· Los primeros 3 bits son el campo User Priority Field que pueden ser usados para asignar un nivel de prioridad.

· El próximo bit es el campo Canonical Format Indicator (CFI) usado para indicar la presencia de un campo Routing Information Field (RIF).

· Los restantes 12 bits son el VLAN Identifier (VID) que identifica de forma única a la VLAN a la cual pertenece la trama Ethernet.



- **Tipos de VLANs y ventajas de tener VLANs**

  Existen varios tipos de VLAN, cada uno con su propia finalidad. Los tipos más comunes de VLANs son:

  - **VLANs basadas en puertos:** Estas VLANs se crean asignando un puerto específico de un switch a una VLAN. Todos los dispositivos conectados a ese puerto formarán parte de la VLAN.
  - **VLANs basadas en protocolos:** Estas VLANs se crean asignando un protocolo específico a una VLAN. Todo el tráfico de ese protocolo quedará confinado a la VLAN. Por ejemplo, se puede crear una VLAN para todo el tráfico VoIP.
  - **VLANs basadas en MAC:** Estas VLANs se crean asignando una dirección MAC específica a una VLAN. Todo el tráfico de esa dirección MAC quedará

confinado en la VLAN. Esto puede ser útil para aislar dispositivos que generan mucho tráfico de difusión.

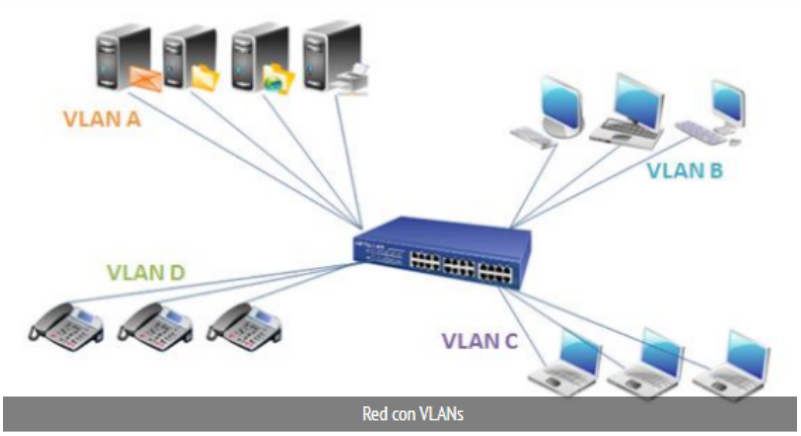
Además de estos tipos comunes de VLANs, también hay una serie de VLANs especializadas, tales como:

- **VLANs de invitados:** Estas VLANs se crean para los invitados que se conectan a su red. Pueden utilizarse para aislar el tráfico de invitados del tráfico corporativo.
- **VLANs de gestión:** Estas VLANs se crean para dispositivos de gestión de red, como switches y routers. Pueden utilizarse para aislar el tráfico de gestión del tráfico corporativo.
- **VLAN de voz:** Estas VLAN se crean para el tráfico de VoIP. Pueden utilizarse para priorizar el tráfico VoIP sobre otros tipos de tráfico.

Detalles adicionales sobre cada uno de los tipos de VLAN

VLANs basadas en puertos: Las VLANs basadas en puertos son el tipo más común de VLAN. Son fáciles de configurar y se pueden utilizar para segmentar la red en función de la ubicación física. Por ejemplo, puede crear una VLAN para cada planta de su edificio de oficinas.
VLANs basadas en protocolos: Las VLANs basadas en protocolos son menos comunes que las VLANs basadas en puertos, pero pueden ser útiles para aislar tipos específicos de tráfico. Por ejemplo, se puede crear una VLAN para todo el tráfico VoIP. Esto ayudaría a mejorar el rendimiento de sus aplicaciones VoIP aislándolas de otros tipos de tráfico.
VLANs basadas en MAC: Las VLANs basadas en MAC son el tipo menos común de VLAN. Son útiles para aislar dispositivos que generan mucho tráfico de difusión. Por ejemplo, se puede crear una VLAN para una impresora que genere mucho tráfico de difusión. Esto ayudaría a mejorar el rendimiento de la red al aislar el tráfico de difusión del resto de la red.

Las VLAN, o redes de área local virtual, son una forma de dividir una red en redes lógicas más pequeñas. Esto se puede hacer por una variedad de razones, como la seguridad, el rendimiento y la administración.



Estas son algunas de las ventajas de tener VLAN:

Seguridad: las VLAN se pueden usar para aislar dispositivos entre sí asignando cada dispositivo a una VLAN diferente. Esto significa que los dispositivos de una VLAN no pueden comunicarse con los dispositivos de otra VLAN a menos que se les permita específicamente hacerlo. Esto puede ayudar a prevenir el acceso no autorizado a datos y recursos.
Rendimiento: las VLAN pueden ayudar a mejorar el rendimiento de la red al reducir la cantidad de tráfico de transmisión. El tráfico de difusión se envía a todos los dispositivos de una red, por lo que sí tiene una gran cantidad de dispositivos, el tráfico de difusión puede ralentizar la red. Al crear VLAN, se puede reducir la cantidad de tráfico de transmisión en la red.
Administración: las VLAN pueden facilitar la administración de una red al agrupar dispositivos según su función o ubicación. Esto facilita la configuración y solución de problemas de red.
Escalabilidad: las VLAN pueden ayudar a que una red sea más escalable al permitirle agregar nuevos dispositivos sin tener que cambiar el diseño físico de su red.
Flexibilidad: las VLAN pueden ayudar a que una red sea más flexible al permitirle crear diferentes redes lógicas para diferentes propósitos. Por ejemplo, podría crear una VLAN para su tráfico de voz y una VLAN separada para su tráfico de datos. Esto le permitiría priorizar el tráfico de voz sobre el tráfico de datos, lo que podría mejorar el rendimiento de sus aplicaciones de voz.
Confiabilidad: las VLAN pueden ayudar a que una red sea más confiable al aislar los dispositivos entre sí. Esto significa que si falla un dispositivo en una VLAN, no afectará a los otros dispositivos en la VLAN.

Además de estas ventajas, las VLAN también se pueden usar para mejorar la escalabilidad, la flexibilidad y la confiabilidad.

Si se está considerando usar VLAN, hay algunas cosas que debe tener en cuenta. Primero, debe asegurarse de que sus conmutadores de red admite VLAN. En segundo lugar, debe decidir cómo desea segmentar su red. Finalmente, debe configurar sus conmutadores y dispositivos para usar VLAN.

- **Conclusiones**
  - Las VLAN (redes de área local virtual) son una herramienta poderosa que se puede utilizar para mejorar la seguridad, el rendimiento y la flexibilidad de una red. Al dividir una red física en varias redes lógicas, las VLAN pueden ayudar a aislar el tráfico, mejorar el rendimiento y aumentar la seguridad.

  - Es una herramienta que permite segmentar una red física en múltiples redes lógicas.

- **Referencias**

CISCO. (2020, July 20). *Asignación de una VLAN de Interfaz como Puerto de Acceso o Tronco en un Cisco Business Switch*. Cisco. Retrieved June 7, 2023, from https://www.cisco.com/c/es_mx/support/docs/smb/switches/Cisco-Business-Switching/kmgmt-2253-assign-an-interface-vlan-as-an-access-or-trunk-port-on-a-swi.pdf

Hernández, C., & Vicente, J. (n.d.). *Características y configuración básica de VLANs*. https://riunet.upv.es/bitstream/handle/10251/16310/Art%C3%ADculo%20docente%20configuraci%C3%B3n%20b%C3%A1sica%20VLANs.pdf

García Pacheco, S., & Güette Montalvo, O. (2008). *Mejorando la seguridad de las redes a partir de la implementación de VLANS*. Universidad Tecnológica de Bolívar.

Olivar, J. (2018). Beneficios de implementar Redes Locales Virtuales (VLAN) mediante los estándares 802.1w, 802.1Q, EtherChannel y GLBP. *Revista Electrónica para la Divulgación de Innovaciones y Tecnología Educativa*, *1*(2), 59–75. http://redited.org/index.php/1/article/view/14

Onofa, E., & Andrés, J. (2022). *Diseño de red para empresas aplicando QoS para el tráfico de red y VLANs*. PUCE - Quito.

Porturas, C., & Noé, A. (2019). *Implementación de redes virtuales utilizando Vlan para reducir el tamaño del dominio de difusión de la red en el Inabib*. Universidad de Ciencias y Humanidades.