TALLER VLAN

TELEMATICA I S7B

ANDERSON RENE GOMEZ AZA

14/09/2023

ESCUELA TECNOLOGICA INSTITUTO TECNICO CENTRAL

1. ¿Qué es una VLAN?
    a. Una VLAN (Virtual Local Area Network) es una técnica de segmentación de redes que permite dividir una red física en múltiples redes virtuales. Aunque todos los dispositivos comparten la misma infraestructura física, como switches y cables, las VLANs les dan la apariencia y el funcionamiento de redes separadas. Esto facilita la organización de dispositivos en grupos lógicos, como departamentos o equipos, mejorando la seguridad y la eficiencia de la red. Las VLANs también permiten un mejor control del tráfico de datos y la optimización de recursos al aislar y priorizar ciertos flujos de información. En resumen, las VLANs son una herramienta fundamental en la administración de redes para crear redes virtuales dentro de una red física.
2. Características de una VLAN.
    a. Las VLAN (Virtual Local Area Networks) tienen varias características clave que las hacen útiles y versátiles en la administración de redes:
    b. Segmentación Lógica: Una de las características más importantes de una VLAN es su capacidad para segmentar una red física en redes lógicas separadas. Esto significa que grupos de dispositivos pueden estar en la misma VLAN, independientemente de su ubicación física en la red.
    c. Aislamiento de Tráfico: Las VLANs proporcionan un alto grado de aislamiento de tráfico. Los dispositivos en una VLAN pueden comunicarse entre sí como si estuvieran en la misma red, pero el tráfico entre VLANs generalmente requiere un enrutamiento, lo que mejora la seguridad y la privacidad.
    d. Mayor Seguridad: Al aislar el tráfico entre grupos de dispositivos, las VLANs mejoran la seguridad de la red. Los dispositivos en una VLAN no pueden comunicarse directamente con dispositivos en otra VLAN sin pasar por un router o un dispositivo de capa 3, lo que permite implementar políticas de seguridad más efectivas.
    e. Flexibilidad: Las VLANs son flexibles y se pueden reconfigurar fácilmente según las necesidades cambiantes de la organización. Puedes agregar, eliminar o modificar VLANs sin cambiar la infraestructura física de la red.
    f. Mejora del Rendimiento: La segmentación de la red en VLANs puede mejorar el rendimiento al reducir la congestión y optimizar el tráfico. Esto es especialmente útil en redes empresariales donde se maneja una gran cantidad de datos.

g. Gestión Eficiente: Las VLANs facilitan la gestión de la red al agrupar dispositivos lógicamente. Esto simplifica las tareas administrativas, como la asignación de recursos y la configuración de políticas de seguridad.
h. Etiquetado de Tráfico: Las VLANs pueden etiquetar el tráfico de red con identificadores numéricos (VLAN IDs), lo que permite a los dispositivos y switches identificar a qué VLAN pertenece cada trama de datos.

En conjunto, estas características hacen que las VLANs sean una herramienta esencial para optimizar y asegurar las redes empresariales y mejorar su gestión.

3. CLASIFICACION DE LAS VLAN.
    a. VLAN Basadas en Puerto (Port-Based VLAN): En este tipo de VLAN, los dispositivos se asignan a una VLAN según el puerto físico del switch al que están conectados. Todos los dispositivos en un puerto específico pertenecen a la misma VLAN.
    b. VLAN Basadas en Protocolo (Protocol-Based VLAN): Estas VLAN se crean en función del protocolo utilizado. Los dispositivos que utilizan un protocolo específico se agrupan en una VLAN correspondiente. Por ejemplo, todos los dispositivos que ejecutan el protocolo IPX/SPX podrían estar en una VLAN separada de los que usan TCP/IP.
    c. VLAN Basadas en Subred (Subnet-Based VLAN): En esta configuración, los dispositivos se asignan a VLAN en función de su dirección IP o subred. Los dispositivos que pertenecen a una misma subred se agrupan en una VLAN.
    d. VLAN Basadas en Etiquetas (Tagged VLAN): En esta configuración, se utilizan etiquetas o tags en los paquetes de datos para identificar a qué VLAN pertenecen. Esto es común en entornos que utilizan el estándar 802.1Q, como VLANs en redes troncales.
    e. VLAN de Gestión (Management VLAN): Se crea una VLAN especial para gestionar dispositivos de red, como switches y routers. Esta VLAN permite un acceso seguro a la administración de los dispositivos de red y ayuda a aislarla de las VLAN de datos regulares.
    f. VLAN de Voz (Voice VLAN): Se utiliza para separar el tráfico de voz sobre IP (VoIP) de otros tipos de tráfico de datos. Esto asegura una calidad de servicio adecuada para las llamadas telefónicas en redes VoIP.
    g. VLAN Nativas (Native VLAN): Es una VLAN que se utiliza en las conexiones troncales para el tráfico no etiquetado. En una conexión troncal, los paquetes de datos no etiquetados se asignan automáticamente a la VLAN nativa.
    h. VLAN Compartidas (Shared VLAN): En este caso, múltiples VLAN comparten una misma infraestructura física sin que puedan comunicarse directamente entre ellas. Se utilizan en entornos donde se necesita una separación física, pero no una separación lógica completa.

4. Usos de la VLAN en las redes.
   Las VLAN (Virtual Local Area Networks) tienen una amplia gama de usos en redes para mejorar la seguridad, el rendimiento y la gestión. Algunos de los usos más comunes de las VLAN en las redes incluyen:
   a. Segmentación de Departamentos o Grupos
   b. Aislamiento de Tráfico
   c. Optimización del Rendimiento
   d. Redes de Voz sobre IP (VoIP)
   e. Aislamiento de Dominios de Difusión
   f. Redes Inalámbricas (Wi-Fi)
   g. Gestión de Invitados
   h. VLAN de Administración
   i. Implementación de Políticas de Seguridad

   En resumen, las VLAN son una herramienta fundamental en la administración de redes que brinda flexibilidad, seguridad y rendimiento mejorado al permitir la creación de redes lógicas dentro de una infraestructura física compartida. Sus usos varían según las necesidades específicas de la organización y la red.

5. Capa del modelo OSI donde se utiliza las VLAN.
   Las VLAN (Virtual Local Area Networks) operan principalmente en la capa 2 (capa de enlace de datos) y, en algunos casos, en la capa 3 (capa de red) del modelo OSI (Open Systems Interconnection).
   a. En la capa 2, las VLAN se basan en la etiquetación de tráfico Ethernet, específicamente utilizando el estándar 802.1Q. Este estándar permite que los paquetes Ethernet se etiqueten con una identificación numérica llamada VLAN ID, que indica a qué VLAN pertenece ese paquete. Los switches utilizan esta información para separar y dirigir el tráfico de acuerdo con las VLAN configuradas. Esto se conoce como VLAN basada en puertos o VLAN basada en etiquetas (tagged VLANs).
   b. En la capa 3, las VLAN se pueden utilizar para segmentar el tráfico de red en función de direcciones IP o subredes. Esto se hace mediante enrutadores o dispositivos de capa 3 que pueden encaminar el tráfico entre VLANs basándose en la dirección IP de destino. Esta segmentación basada en la capa 3 se utiliza en redes más grandes o cuando se requiere un mayor nivel de aislamiento y control de tráfico.
6. Dispositivos que intervienen en las VLAN.
   a. Switches: Los switches son dispositivos esenciales para la implementación de VLAN. Los switches de capa 2 y capa 3 se utilizan para crear, asignar y gestionar VLAN. Los switches de capa 2 admiten VLAN basadas en puertos y etiquetas, mientras que los switches de capa 3 permiten el enrutamiento entre VLANs.
   b. Router: Los routers pueden ser utilizados para el enrutamiento entre VLANs en caso de VLANs de capa 3. Los routers también pueden proporcionar conectividad entre VLANs y subredes diferentes.

c. Dispositivos Terminales: Estos son los dispositivos finales, como computadoras, servidores, impresoras, teléfonos IP y cualquier otro dispositivo conectado a la red. Se asignan a VLANs según su función o ubicación.
d. Puntos de Acceso Inalámbrico (AP): En redes inalámbricas, los AP pueden admitir múltiples VLAN para separar el tráfico de diferentes grupos de usuarios o dispositivos inalámbricos.
e. Controladores de Dominio: En entornos de red más grandes, los controladores de dominio pueden utilizarse para gestionar la autenticación y la asignación de VLAN a dispositivos en función de políticas de seguridad y políticas de acceso.
f. Servidores de Aplicaciones: Los servidores que proporcionan servicios específicos, como aplicaciones empresariales o servicios de voz sobre IP (VoIP), pueden asignarse a VLAN específicas para administrar y optimizar el tráfico relacionado con esas aplicaciones.
g. Firewalls y Dispositivos de Seguridad: Los dispositivos de seguridad, como firewalls y sistemas de detección y prevención de intrusiones (IDS/IPS), pueden implementarse entre VLANs para controlar y asegurar el tráfico entre ellas.
h. Dispositivos de Monitoreo: En algunas configuraciones, se pueden utilizar dispositivos de monitoreo, como sondas de tráfico o analizadores de paquetes, para supervisar y analizar el tráfico dentro de las VLAN y garantizar un rendimiento óptimo y seguridad.
i. Switches de Nivel de Acceso (Access Switches): En una topología de red escalable, se pueden utilizar switches de nivel de acceso para conectar dispositivos terminales a la red

7. Comandos utilizados más comunes en la configuración de una VLAN.
   La configuración de VLAN en dispositivos de red como switches generalmente implica el uso de comandos a través de la línea de comandos o interfaces de administración web. Aquí tienes algunos de los comandos más comunes utilizados en la configuración de VLAN en switches Cisco (IOS) como ejemplo:
   a. Ingreso al modo de configuración global:
      i. enable
      ii. configure terminal
   b. Creación de una VLAN:
      i. vlan <número>
      ii. Por ejemplo, para crear una VLAN con el número 10:
         1. vlan 10
   c. Asignación de un nombre a una VLAN:
      i. name <nombre_de_la_vlan>
      ii. Por ejemplo:
         1. name VLAN-VENTAS
   d. Asignación de un puerto a una VLAN:
      i. interface <tipo> <número>
      ii. switchport mode access
      iii. switchport access vlan <número_de_la_vlan>
      iv. Por ejemplo, para asignar el puerto Ethernet 0/1 a la VLAN 10:

1. interface Ethernet0/1
2. switchport mode access
3. switchport access vlan 10

e. Configuración de un puerto como troncal (para conectar switches):
   i. interface <tipo> <número>
   ii. switchport mode trunk
   iii. switchport trunk allowed vlan <lista_de_vlans>
   iv. Por ejemplo, para configurar un puerto Ethernet como troncal y permitir el tráfico de varias VLANs:
      1. interface Ethernet0/1
      2. switchport mode trunk
      3. switchport trunk allowed vlan 10,20,30
f. Mostrar información de VLAN:
   i. show vlan
   ii. Este comando muestra una lista de todas las VLAN configuradas en el switch, junto con detalles como los puertos asociados.
g. Eliminar una VLAN:
   i. no vlan <número>
   ii. Por ejemplo, para eliminar la VLAN 10:
      1. no vlan 10