Práctica 8 Redes de Computadores: VLANs Redes LAN Virtuales

Kevin Mateo Alvarado Suarez (kevin.alvarado@ucuenca.edu.ec),
Santiago Ariel Armijos Goercke (santiago.armijos@ucuenca.edu.ec)
Universidad de Cuenca
Redes de Computadores

Resumen

En este informe se exponen los fundamentos conceptuales esenciales para comprender el proceso de creación de Redes de Área Local Virtuales (VLAN). Además, se analizan las diversas ventajas y desventajas de este procedimiento, que consiste básicamente en establecer redes lógicas independientes dentro de una infraestructura física compartida. Estas redes lógicas independientes se configuran como segmentos más pequeños dentro de una red física cableada más extensa, y pueden emplearse con diversos propósitos. Las estaciones de trabajo se agrupan en soluciones de red independientes de su ubicación física, siempre y cuando estén conectadas en la misma LAN. Esto se logra mediante la implementación de VLANs, tomando en consideración los aspectos detallados en este documento.

I. Introducción

En determinadas circunstancias, la utilización de una única red LAN en un área geográfica limitada puede ocasionar problemas administrativos en la red. Esto es especialmente evidente al intentar gestionar el acceso a recursos por parte de grupos específicos de dispositivos, ya que implica aplicar configuraciones de acceso a cada equipo de la red. También surge complicación al necesitar administrar el tráfico de entrada y salida para cada uno de estos grupos particulares de dispositivos. Por esta razón, en tales situaciones resulta viable la implementación de VLANs, las cuales son un método que posibilita la creación de redes independientes dentro de una misma infraestructura física. Un usuario puede configurar múltiples redes VLANs en un solo router, donde cada una de estas redes agrupa los equipos de un segmento de red específico. Además, se obtiene la ventaja de gestionar el tráfico permitido y bloqueado para cada VLAN. Este informe aborda el proceso de creación de VLANs, junto con sus beneficios y desventajas, y proporciona un ejemplo práctico mediante el uso del software Cisco Packet Tracer.

II. Objetivos

1. Conocer qué son y para qué sirven las VLANs.
2. Conocer los tipos de VLANs que existen.
3. Conocer las ventajas y desventajas de las VLANs.
4. Simular el uso de VLANs.

III. Marco Teórico

III.1. ¿Qué son las VLANs?

Las redes de Área Local Virtuales (LAN virtuales), también conocidas como VLANs, representan una tecnología de redes que posibilita la creación de redes lógicas autónomas dentro de una infraestructura física común. Estas VLANs se emplean tanto en entornos domésticos como profesionales con el propósito de segmentar la red de manera efectiva y utilizar cada segmento de forma diferenciada. Al establecer estos segmentos, se brinda la capacidad de permitir o bloquear el tráfico entre las distintas VLAN mediante dispositivos como routers o switches. Para implementar estas redes lógicamente independientes en la misma infraestructura física, es esencial utilizar switches gestionables que admitan VLANs y faciliten la segmentación adecuada de la red. Asimismo, resulta fundamental contar con routers compatibles con VLAN, ya que, de lo contrario, no se podrían gestionar ni controlar las comunicaciones entre ellas. [1]

III.2. ¿Qué tipos de VLANs existen?

En la actualidad, disponemos de diversos tipos de VLANs que podemos emplear en distintos dispositivos, específicamente en switches y puntos de acceso WiFi. Entre las variedades de VLANs, se encuentran aquellas basadas en el estándar 802.1Q VLAN Tagging, las VLAN basadas en puerto, las VLAN basadas en direcciones MAC y las VLAN basadas en aplicaciones, siendo esta última poco utilizada en la práctica. [1]

- **802.1Q VLAN Tagging**: Este tipo de VLAN es el más común y hace uso del estándar 802.1Q para etiquetar o desetiquetar VLANs. El estándar implica la introducción de una cabecera 802.1Q en la trama Ethernet convencional, con el propósito de diferenciar las diversas VLANs configuradas. Cabe destacar que este estándar no encapsula la trama original de Ethernet, sino que añade 4 bytes al encabezado Ethernet existente, y modifica el campo .EtherType.al valor 0x8100 para indicar que el formato de la trama ha sido alterado. Cuando implementamos el estándar 802.1Q y creamos VLANs en un switch, tenemos la opción de configurar los puertos de manera ”tagged”(con etiqueta) o üntagged”(sin etiqueta).
- **VLAN tagged:** En las tramas Ethernet se incorpora la .etiqueta”del ID de la VLAN configurada. Estas VLANs son reconocidas por todos los switches, puntos de acceso WiFi profesionales y routers. En un puerto determinado, se pueden configurar una o más VLANs en modo ”tagged”. En los enlaces troncales (entre un router y un switch, entre switches y entre switch y punto de acceso), se configuran generalmente como ”tagged”para transmitir todas las VLANs.
- **VLAN untagged:** En las tramas Ethernet se elimina la etiqueta configurada. Estas VLANs son comprendidas por todos los dispositivos, pero se utilizan principalmente para equipos finales como ordenadores, portátiles, impresoras, cámaras IP y otros dispositivos similares. En un puerto específico, solo se puede configurar una VLAN como üntagged”, ya que no se podría interpretar adecuadamente por el equipo final la presencia de dos VLANs como üntagged”.

Cuando empleamos este estándar, los switches ofrecen la posibilidad de configurar los puertos físicos de diversas maneras: [1]

- **Acceso:** Estos son los puertos destinados a la conexión de PC, impresoras, smartphones y otros dispositivos finales. En este tipo de puerto de acceso, se configura una VLAN como üntagged”.
- **Troncal o trunk:** Estos puertos transportan una o varias VLANs de un dispositivo a otro. Por ejemplo, si deseamos enlazar un switch con otro y transmitir todas o algunas de las VLANs, es necesario configurar el puerto en modo troncal o trunk, seleccionando las VLANs que se desean transmitir como ”tagged”.
- **Dynamic:** La configuración de estos puertos varía según el tipo de paquete que recibe el switch, pudiendo establecerse como acceso o trunk. No se recomienda configurar los puertos de un switch en modo dinámico por motivos de seguridad, con el objetivo de prevenir posibles ataques.

III.2.1. ***VLAN basadas en puerto****:* Denominada también como conmutación por puerto en los menús de configuración de routers y switches, esta modalidad es la más difundida y empleada en switches de gama baja. En este enfoque, cada puerto se asigna a una VLAN específica, y los usuarios conectados a ese puerto automáticamente forman parte de la VLAN asignada. Los usuarios pertenecientes a una misma VLAN tienen visibilidad entre sí, aunque no la tienen hacia las redes locales virtuales contiguas.

La limitación principal de esta modalidad radica en su falta de flexibilidad al momento de reubicar usuarios. En caso de que un usuario cambie su ubicación física, sería necesario reconfigurar la VLAN correspondiente. En las VLAN basadas en puerto, las decisiones y el reenvío se basan en la dirección MAC de destino y el puerto asociado, convirtiéndola en la forma más sencilla y común de VLAN. Es por esta razón que los switches de gama baja suelen integrar la VLAN basada en puerto en lugar de la basada en el estándar 802.1Q. [1]

III.2.2. ***VLAN basadas en MAC****:* El razonamiento sigue una lógica similar al caso anterior, aunque en lugar de asignarse a nivel de puerto, se realiza a nivel de la dirección MAC del dispositivo. La ventaja de este enfoque radica en que permite la movilidad sin necesidad de realizar cambios en la configuración del switch o del router. No obstante, surge un problema evidente: la inclusión de todos los usuarios puede volverse laboriosa. Únicamente los switches de alta gama admiten la VLAN basada en MAC. Cuando el switch detecta la conexión de una dirección MAC específica, la asigna automáticamente a una VLAN determinada, ofreciendo así una solución útil en situaciones que requieren movilidad.

Consideremos el escenario en el que nos conectamos con nuestro portátil en varios puertos Ethernet en la oficina y deseamos que siempre se nos asigne la misma VLAN. En este caso, la implementación de VLANs basadas en MAC permite lograrlo sin necesidad de reconfigurar el switch. Esta funcionalidad es común en entornos empresariales extensos, donde se requiere una segmentación efectiva de los equipos. [1]

III.2.3. ***VLAN etiquetadas****:* Exploraremos el etiquetado 802.1q, conforme a la definición del estándar IEEE 802.1q. Este mecanismo permite que un dispositivo de red agregue información a una trama en la capa 2, posibilitando la identificación de la pertenencia a una VLAN específica. Dicho etiquetado

posibilita la existencia de VLANs que engloban varios dispositivos en un entorno de red. Cuando un dispositivo recibe un paquete, interpreta la etiqueta y determina la VLAN a la que pertenece la trama. Es relevante destacar que algunos dispositivos no admiten la recepción simultánea de paquetes etiquetados y no etiquetados en una misma interfaz de red. Si se presenta esta situación, se recomienda contactar a los administradores para resolver el problema.

En relación con la interfaz, esta puede ser miembro de una VLAN etiquetada o no etiquetada. Cada interfaz de red es exclusivamente un miembro sin etiquetar de una VLAN. En este contexto, la interfaz de red se encarga de transmitir las tramas de la VLAN nativa como tramas sin etiquetar. Es posible que una interfaz de red forme parte de diversas VLANs, sin que las demás estén etiquetadas.

Al configurar el etiquetado, es crucial garantizar su consistencia con la configuración asignada a la VLAN en todos los puntos. Además, el puerto al que nos conectamos debe estar en la misma VLAN que la interfaz. Asimismo, es importante tener en cuenta que, si la configuración de la VLAN no está sincronizada y propagada, la configuración debe realizarse de forma independiente en todas las unidades. [1]

III.2.4. ***VXLAN****:* Se trata de una red de área local virtual extensible conocida como VXLAN. Esta tecnología sobrepone redes de capa 2 sobre una infraestructura de capa 3 mediante la encapsulación de tramas de capa 2 en paquetes UDP.

Cada una de las redes superpuestas recibe el nombre de segmento VXLAN y se identifica mediante un identificador único de 24 bits llamado VXLAN Network Identifier (VNI). La comunicación entre dispositivos solo es posible si pertenecen a la misma VXLAN.

Las ventajas que proporciona esta tecnología incluyen:

- Mayor escalabilidad en entornos de nube virtualizada: El ID de VXLAN es de 24 bits, permitiendo la creación de hasta 16 millones de redes aisladas. Esto supera la capacidad de las VLAN, que tienen IDs de 12 bits y permiten 4094 redes también aisladas.
- Mayor flexibilidad en la gestión de la conectividad.
- Facilita la implementación de funciones de capa 3 en las redes subyacentes.

La red virtual en la capa 2 se abstracta de la red física subyacente, lo que implica que la red virtual no es visible para la red física. Esto conlleva beneficios como la eliminación de la necesidad de una infraestructura física adicional y la reducción de la duplicación de direcciones MC en las máquinas virtuales que comparten el mismo segmento de VXLAN. [1]

III.2.5. ***VLAN Híbrida****:* Existen VLANs que se basan en puertos y otras que se etiquetan. Sin embargo, hay una alternativa adicional a estas tecnologías: las VLAN Híbridas. Estas se fundamentan en la distribución de paquetes de datos según las etiquetas asignadas, y además, la estructura de la red se define mediante una conexión deliberada de los puertos.

Todos los tipos de conexiones VLAN son válidos, pero la elección entre ellos depende de las conexiones deseadas en la red o del nivel de seguridad que se pretende establecer. Las VLAN Híbridas facilitan la interconexión de equipos de trabajo sin importar su ubicación física y, lo que es aún más crucial, sin afectar negativamente la seguridad de la red ni la segmentación interna a la que está sujeta. [1]

III.3. Ventajas de utilizar VLANs

A continuación, se enumeran los beneficios de la utilización de VLANs: [2]

1. Seguridad: Las VLANs permiten la creación de redes lógicamente independientes, brindando la capacidad de aislarlas para que solo tengan conexión a Internet y negar el tráfico entre distintas VLANs.
2. Segmentación: Las VLANs posibilitan la segmentación de todos los dispositivos en diversas redes, asignando a cada una de ellas una VLAN diferente. Por ejemplo, es viable establecer una red interna de gestión para routers, switches y puntos de acceso, una red principal para administradores, otra para dispositivos IoT y una adicional para invitados.
3. Flexibilidad: Gracias a las VLANs, es sencillo y rápido colocar dispositivos en diferentes redes, permitiendo establecer políticas de comunicación donde se regule el tráfico hacia otras VLANs o hacia Internet.
4. Optimización de la red: Al tener redes más pequeñas, especialmente en entornos con miles de dispositivos conectados, se limita la difusión de broadcast en dominios más reducidos, lo que optimiza el rendimiento de la red al evitar la transmisión de mensajes de broadcast a todos los dispositivos conectados. Además, el uso de VLANs disminuye la necesidad de routers, ya que estas crean dominios de transmisión utilizando switches en su lugar.

5. Reducción de costos: La necesidad de actualizaciones de red se reduce, y las VLANs pueden crear dominios de transmisión que eliminan la necesidad de costosos routers, lo que conlleva a una disminución de costos.

III.4. Desventajas de utilizar VLANs

A continuación, se detallan las limitaciones asociadas al uso de VLANs: [2]

1. Administración compleja: La gestión puede volverse complicada cuando se tienen múltiples VLANs, llegando a requerir un esfuerzo y costo similares o incluso superiores al manejo de redes LAN convencionales.
2. Aislamiento: En redes de gran escala, puede ser necesario utilizar varios routers para lograr una comunicación fluida, lo que incrementa los costos de implementación.
3. Seguridad: La presencia de múltiples VLANs puede facilitar la propagación de un virus a través de toda la red de manera rápida y sencilla.
4. Latencia: Aunque las redes VLAN son más eficientes que las WAN, no alcanzan la misma eficacia que una LAN, lo que implica ciertos niveles de latencia.

IV. Desarrollo

IV.1. Explicación

Se hará una red con 3 VLANs internas conectadas en un mismo Switch, para cada red se usara una IP de tipo C (192.168.0.0 - 192.168.1.0 - 192.168.2.0).

IV.2. Disposición de los dispositivos

Para esta practica usaremos los siguientes dispositivos: 2 laptops (para usar la consola para programar los routers), 1 router, 1 switch y 6 computadores de escritorio.

En el caso de la laptop el router y el switch usaremos cable consola para conectarlos y usaremos cable directo para conectar entre dispositivos de diferentes tipos.

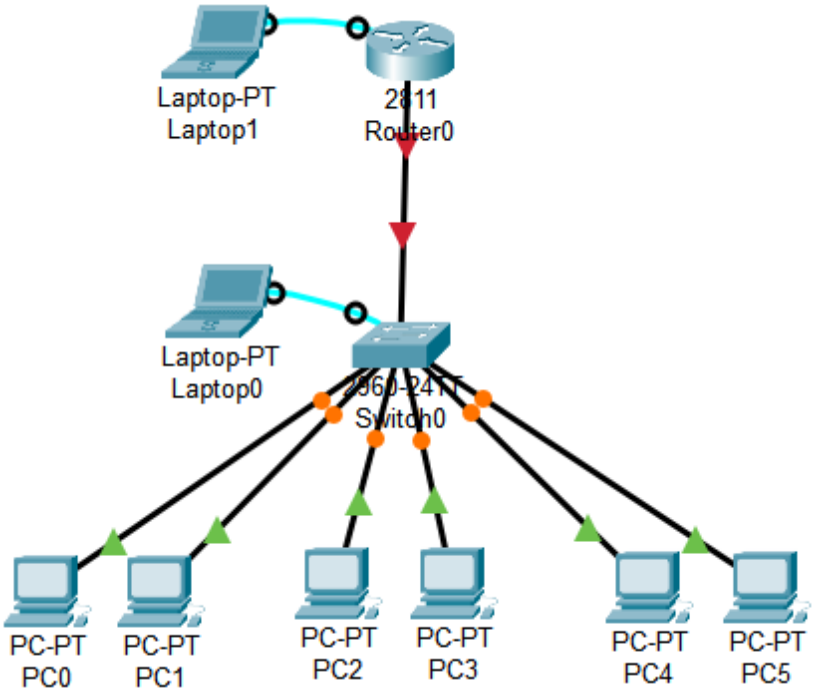

Figura 1: Conexión Dispositivos.

IV.3. Programación Switch

A continuación se muestras los comandos usados en esta sección:

IV.3.1. Creación VLANs:

```
Switch(config)#vlan 10
Switch(config-vlan)#name admin
Switch(config-vlan)#exit
Switch(config)#vlan 20
Switch(config-vlan)#name disenio
Switch(config-vlan)#exit
Switch(config)#vlan 30
Switch(config-vlan)#name student
Switch(config-vlan)#exit

Switch(config)#interface range fa 0/2-3
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 10
Switch(config-if-range)#exit
Switch(config)#interface range fa 0/4-5
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 20
Switch(config-if-range)#exit
Switch(config)#interface range fa 0/6-7
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 30
Switch(config-if-range)#exit
```

IV.3.2. Creación de la troncal:

```
Switch(config)#interface fa 0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#exit
```

IV.4. Programación Router

A continuación se muestras los comandos usados en esta sección:

```
Router(config)#interface fa 0/0
Router(config-if)#no shutdown

Router(config-if)#interface fa 0/0.10
Router(config-subif)#encapsulation dot1Q 10
Router(config-subif)#ip address 192.168.0.1 255.255.255.0
Router(config-subif)#exit
Router(config-if)#interface fa 0/0.20
Router(config-subif)#encapsulation dot1Q 20
Router(config-subif)#ip address 192.168.1.1 255.255.255.0
Router(config-subif)#exit
Router(config-if)#interface fa 0/0.30
Router(config-subif)#encapsulation dot1Q 30
Router(config-subif)#ip address 192.168.2.1 255.255.255.0
Router(config-subif)#exit
```

IV.5. Configuración de las direcciones IP y máscaras de red a cada dispositivo

Por ultimo, toca configurar cada uno de los dispositivos LAN (computadoras de escritorio) con una IP y mascara de red correspondiente a la que se le fue asignada a su subred.

IPv4 Address	192.168.0.2
Subnet Mask	255.255.255.0
Default Gateway	192.168.0.1
DNS Server	0.0.0.0

Figura 2: Configuración Dispositivo Red 1.

IPv4 Address	192.168.1.2
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1
DNS Server	0.0.0.0

Figura 3: Configuración Dispositivo Red 2.

IPv4 Address	192.168.2.2
Subnet Mask	255.255.255.0
Default Gateway	192.168.2.1
DNS Server	0.0.0.0

Figura 4: Configuración Dispositivo Red 3.

IV.6. Diseño final de la red

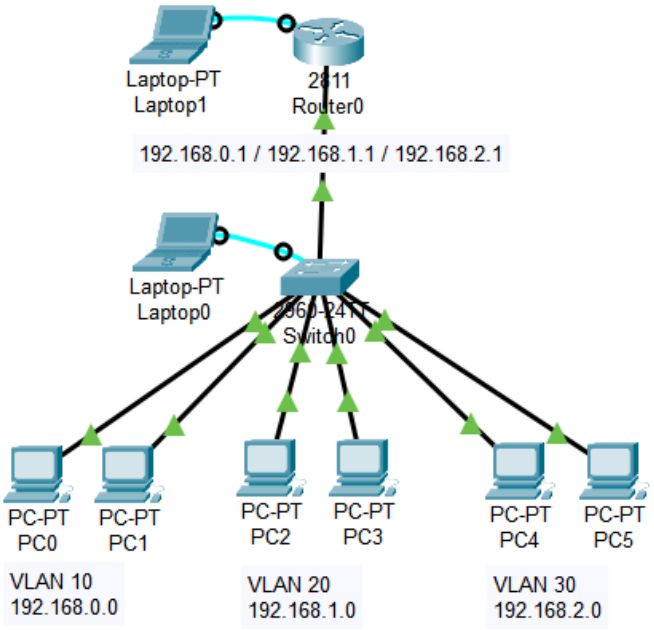

Figura 5: Diseño Final de la Red

IV.7. Pruebas de comunicación

```
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=1ms TTL=127
Reply from 192.168.1.2: bytes=32 time<1ms TTL=127
Reply from 192.168.1.2: bytes=32 time<1ms TTL=127
Reply from 192.168.1.2: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Figura 6: Comunicación Redes Tipo 1-2

```
C:\>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:

Reply from 192.168.2.2: bytes=32 time<1ms TTL=127
Reply from 192.168.2.2: bytes=32 time<1ms TTL=127
Reply from 192.168.2.2: bytes=32 time<1ms TTL=127
Reply from 192.168.2.2: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Figura 7: Comunicación Redes Tipo 1-3

```
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time<1ms TTL=127
Reply from 192.168.1.2: bytes=32 time<1ms TTL=127
Reply from 192.168.1.2: bytes=32 time<1ms TTL=127
Reply from 192.168.1.2: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Figura 8: Comunicación Redes Tipo 2-3

V. Conclusiones

La capacidad de crear segmentos de red mediante el uso de VLANs ofrece una gestión más efectiva de la red en su conjunto. Esto se debe a que cada segmento puede ser controlado de manera independiente, lo que resulta en una mejora del tráfico. Durante la transmisión de paquetes, estos no se difunden a todos los dispositivos de la red, sino únicamente a los dispositivos dentro de cada segmento. Es crucial destacar que, con las VLANs, se logra un fortalecimiento de la seguridad de la información, ya que cada

VLAN administra internamente sus propios datos y no se comunica con otras VLAN por defecto; esta comunicación solo se establece si así lo deseamos. De esta manera, se establece una barrera de seguridad entre los equipos de cada VLAN.

REFERENCIAS

[1] "Qué son las VLAN, para qué sirven y cómo funcionan con ejemplos de uso." [Online]. Available: https://www.redeszone.net/tutoriales/redes-cable/vlan-tipos-configuracion/

[2] L. G. Lorés, "Ventajas e inconvenientes de usar redes privadas virtuales," Sep. 2018. [Online]. Available: https://www.escueladeinternet.com/ventajas-y-limites-de-usar-redes-privadas-virtuales/