INSTITUTO POLITÉCNICO NACIONAL

ESCUELA SUPERIOR DE COMPUTO

INVESTIGACIÓN DE VLAN Y EJERCICIO DE VLSM

NOMBRE DEL ALUMNO: GARCÍA QUIROZ GUSTAVO IVAN

GRUPO: 5CV3

NOMBRE DEL PROFESOR: ALCARAZ TORRES JUAN JESUS

08/11/2023

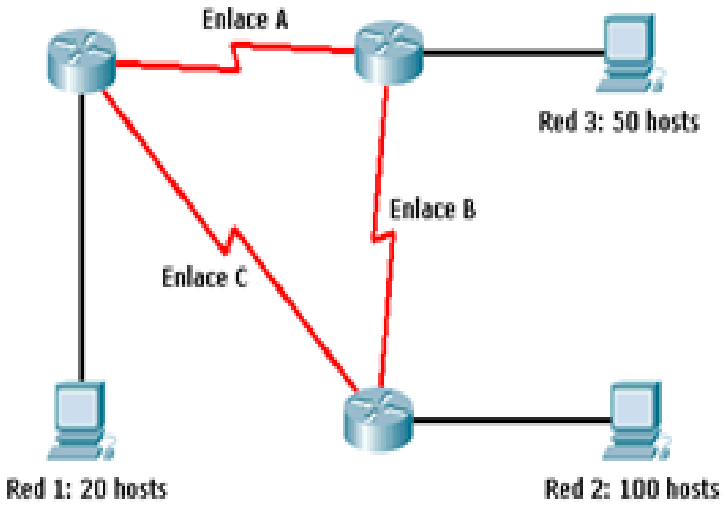
Índice

EJERCICIO

Ejercicio

Dada la siguiente topología y la dirección IP 148.204.1.0/24, se nos pide que por medio de subneteo con VLSM obtengamos direccionamiento IP para los hosts de las 3 subredes, las interfaces Ethernet de los routers que son los enlaces seriales entre los routers.

Calcular la cantidad de direcciones IP para toda la topología, llenar tabla correspondiente y justificar cálculos.



SubRed	IP de Inicio	IP Final	Broadcast	Direcciones por subred	Mascara de SubRed
148.204.1.0/25	148.204.1.1	148.204.1.126	148.204.1. 127	$2^7 - 2 = 128 - 2 = 126$	255.255.255.128
148.204.1.128/26	148.204.1.129	148.204.1.190	148.204.1.191	$2^6 - 2 = 64 - 2 = 62$	255.255.255.192
148.204.1.192/27	148.204.1.193	148.204.1.222	148.204.1. 223	$2^5 - 2 = 32 - 2 = 30$	255.255.255. 224
148.204.1.224/30	148.204.1.225	148.204.1.226	148.204.1.227	$2^2 - 2 = 4 - 2 = 2$	255.255.255.252
148.204.1.228/30	148.204.1.229	148.204.1.230	148.204.1.231	$2^2 - 2 = 4 - 2 = 2$	255.255.255.252
148.204.1.232/30	148.204.1.233	148.204.1.234	148.204.1.235	$2^2 - 2 = 4 - 2 = 2$	255.255.255.252

INVESTIGACIÓN

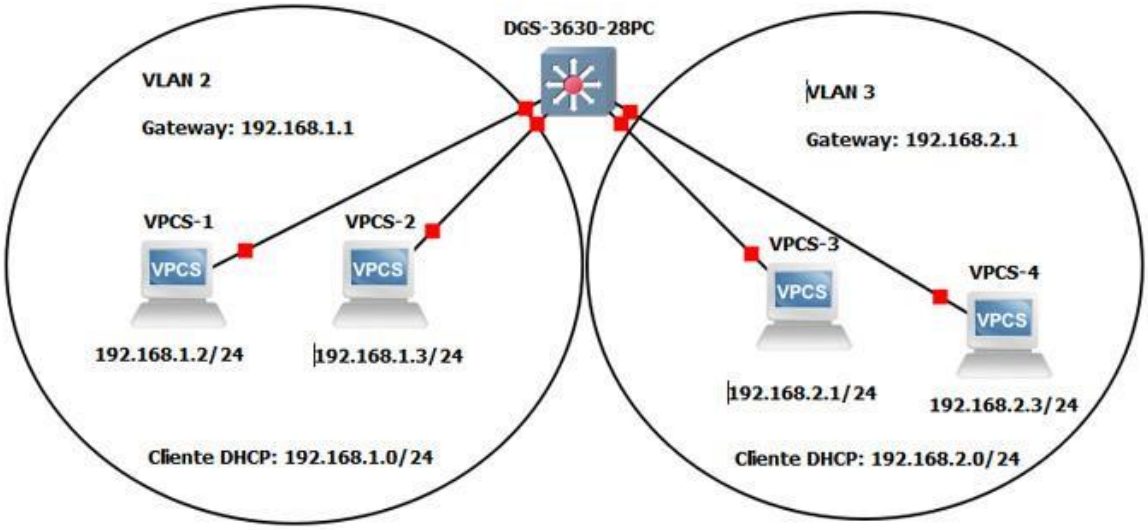
VLAN

¿Qué son las VLAN?

Las **VLAN o Virtual LAN** nos permite crear redes lógicamente independientes dentro de la misma red física, haciendo uso de switches gestionables que soportan VLANs para segmentar adecuadamente la red. También es muy importante que los routers que utilicemos soportan VLAN, de lo contrario, no podremos gestionarlas todas ni permitir o denegar la comunicación entre ellas. Actualmente la mayoría de routers profesionales e incluso sistemas operativos orientados a firewall/router como pfSense o OPNsense soportan VLAN porque es un estándar hoy en día. El uso de VLANs nos proporciona lo siguiente:

- **Seguridad**. Las VLAN nos permite **crear redes lógicamente independientes**, por tanto, podemos aislarlas para que solamente tengan conexión a Internet, y denegar el tráfico de una VLAN a otra. Por defecto no se permite a las VLANs intercambiar tráfico con otra VLAN, es totalmente necesario ascender a nivel de red (L3) con un router o un switch multicapa, con el objetivo de activar el inter-vlan routing, es decir, el enrutamiento entre VLANs para sí permitir la comunicación entre ellas siempre que lo necesitemos.
- **Segmentación**. Las VLAN nos permite **segmentar todos los equipos en diferentes subredes**, a cada subred le asignaremos una VLAN diferente. Por ejemplo, podremos crear una subred de gestión interna de todos los routers, switches y puntos de acceso, podremos crear una subred principal para los administradores, otra subred para dispositivos IoT y otra subred diferente para invitados. Es decir, podremos segmentar la red principal en subred con el objetivo de que cada subred haga uso de las comunicaciones como deseen. Gracias a la segmentación, podremos agrupar una gran cantidad de equipos dentro del mismo dominio de broadcast, aunque estén muy lejos físicamente.
- **Flexibilidad**. Gracias a las VLAN podremos colocar a los diferentes equipos en una subred o en otra, de manera fácil y rápida, y tener unas políticas de comunicación donde permitimos o denegamos el tráfico hacia otras VLANs o hacia Internet. Por ejemplo, si creamos una VLAN de invitados, podríamos prohibirles el uso de servicios de streaming de vídeo.
- **Optimización de la red**. Al tener subredes más pequeñas, en entornos donde tengamos cientos o miles de equipos conectados, contendremos el broadcast en dominios más pequeños, por tanto, el rendimiento de la red será óptimo, sin tener que transmitir los mensajes de broadcast a todos los equipos conectados, lo que haría que el rendimiento de la red baje

radicalmente e incluso podría llegar a colapsar. Al usar VLAN, tendremos varios dominios de difusión en el mismo switch. En redes donde el tráfico consiste en un alto porcentaje de transmisiones y multidifusiones, las VLAN pueden reducir la necesidad de enviar dicho tráfico a destinos innecesarios. Por ejemplo, en un dominio de transmisión que consta de 10 usuarios, si el tráfico de transmisión está destinado solo a 5 de los usuarios, colocar estos 5 usuarios en una VLAN separada puede reducir el tráfico. En comparación con los switches, los routers requieren más procesamiento del tráfico entrante, y a medida que aumenta el volumen de tráfico que pasa a través de los routers, también aumenta la latencia en dichos routers, lo que da como resultado un rendimiento reducido. El uso de VLAN reduce la cantidad de routers necesarios, ya que las VLAN crean dominios de transmisión utilizando switches en lugar de routers.



- **Reducción de costes.** Debido a la poca necesidad de actualizaciones de red que son demasiado costosas, y gracias a un uso más eficaz de los enlaces y del ancho de banda disponible, es posible reducir costes al realizar este tipo de redes. Las VLAN se pueden usar para crear dominios de transmisión que eliminan la necesidad de costosos routers, lo cual ayuda aún más a reducir dichos costes.
- **Mejor eficiencia del personal de TI.** Nos facilitarán el manejo de la red, debido a que diferentes usuarios pueden compartir una misma VLAN. Cuando implementamos un nuevo switch, este implantará todas las políticas y procedimientos que tiene prestablecidos la VLAN. También hará más sencillo identificar la función de una VLAN en concreto, al poder proporcionarle un nombre.
- **Administración de aplicaciones y proyectos simples.** Estas redes pueden agregar dispositivos y usuarios para admitir ciertos requisitos

geográficos o de tipo comercial. Como tienen características diferentes, se facilita mucho la administración de una aplicación concreta, o albergando proyectos diferentes. El setenta por ciento de los costos de la red son el resultado de adiciones, movimientos y cambios de usuarios en la red, cada vez que un usuario se mueve en una LAN, se hace necesario volver a cablear, direccionar nuevas estaciones y reconfigurar los concentradores y routers. Algunas de estas tareas se pueden simplificar con el uso de VLAN, por lo que, si un usuario se mueve dentro de una VLAN, no es necesaria la reconfiguración de los routers. Además, según el tipo de VLAN, se pueden reducir o eliminar otros trabajos, sin embargo, todo el poder de las VLAN solo se sentirá realmente cuando se creen buenas herramientas de administración que permitan a los administradores de red arrastrar y colocar usuarios en diferentes VLAN o configurar alias, a pesar de este ahorro, las VLAN agregan una capa de complejidad administrativa, ya que ahora es necesario administrar grupos de trabajo virtuales.

Las VLAN nos permiten **asociar lógicamente a los diferentes usuarios**, en base a etiquetas, puertos del switch, a su dirección MAC e incluso dependiendo de la autenticación que hayan realizado en el sistema. Las VLAN pueden existir en un solo switch gestionable, para asignar después a cada puerto el acceso a una determinada VLAN, pero también pueden existir en varios switches que están interconectados entre ellos, por tanto, las VLAN pueden extenderse por diferentes switches a través de los enlaces troncales. Esto nos permite tener las VLAN en diferentes switches y asignar una determinada VLAN en cualquiera de estos switches o en varios simultáneamente.

Cuando creamos y configuramos las VLAN en un router no se pueden comunicar entre ellas, la única forma de que se puedan comunicar las VLAN es ascendiendo a nivel de red (L3), esto lo podemos hacer de diferentes formas:

- Usar un **router/firewall con soporte para el estándar de VLANs**. El switch pasará un troncal con todas las VLANs y el router/firewall dará de alta en su firmware o sistema operativo las diferentes VLANs, y permitirán el enrutamiento inter-vlan. Es posible que, por defecto, este enrutamiento esté activado, pero por reglas en el firewall se deniegue la comunicación entre las VLAN, hasta que permitamos el acceso.
- Usar un **switch gestionable L3**. Los switches gestionables L3 nos permiten crear interfaces IPv4 y IPv6, por lo que podremos crear una interfaz por cada VLAN que tengamos configurada en el switch y activar el enrutamiento inter-vlan. Esto es una opción muy buena para intercomunicar las VLANs sin necesidad de que el router se encargue de todo, generalmente estos switches L3 están en el Core de la red.

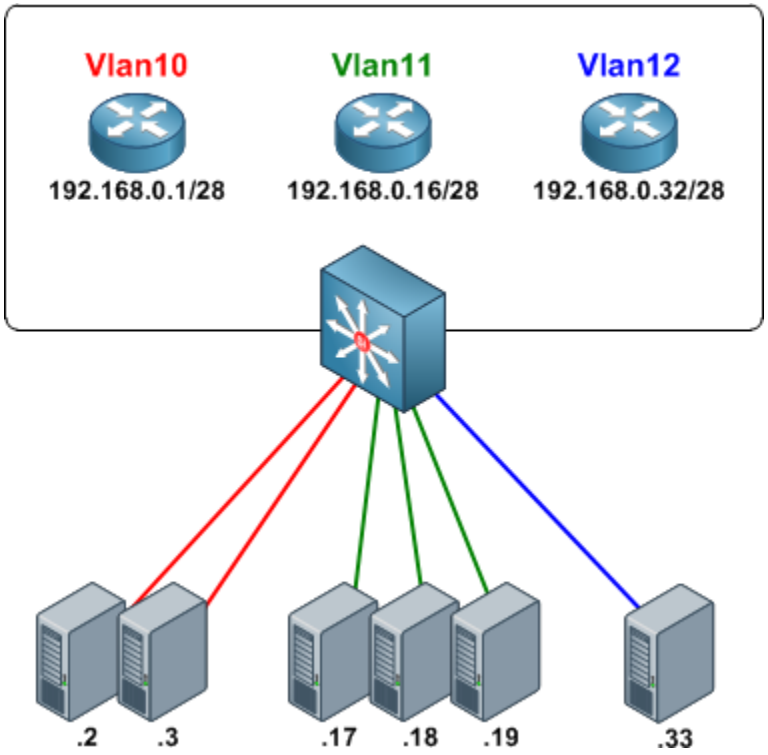
Para permitir la comunicación o la no comunicación de las VLAN se deben hacer uso de **ACL (Listas de Control de Acceso)**, o configurar el firewall

correspondiente para permitir o denegar el tráfico. Por ejemplo, se podría permitir la comunicación de una VLAN 2 a una VLAN 3, pero no al revés, por tanto, configurando correctamente el firewall y los estados de conexión, se podría ajustar la comunicación a los requisitos de la empresa.

¿Para qué sirven las VLAN?

Cuando configuramos una red de área local, ya sea en un entorno doméstico donde queramos segmentar los diferentes dispositivos a conectar, o en un entorno profesional, hacemos uso de VLANs para tener diferentes subredes. Imaginemos que somos los administradores de redes de un colegio, podemos crear diferentes VLANs para diferentes usos y realizar una administración mucho más sencilla de la red, además, seremos capaces de «contener» los mensajes de broadcast en dominios de difusión más pequeños, es decir, tendremos subredes pequeñas para proporcionar direccionamiento a las decenas de equipos que tengamos, y no solamente una subred donde haya cientos de dispositivos conectados. En este escenario de un colegio, podríamos tener perfectamente las siguientes VLANs:

- VLAN de gestión: podremos crear una VLAN de gestión para acceder al router, firewall, a todos los switches repartidos por todo el colegio y también los puntos de acceso WiFi que tengamos, los sistemas de monitorización también estarán en esta VLAN para monitorizar continuamente los diferentes equipos de red.
- VLAN de administración del colegio: en esta VLAN estarán todos los PC del director, secretario del colegio, profesores y demás personal.
- VLAN de alumnos: en esta VLAN estarán todos los equipos de los alumnos, ya sean los equipos cableados en las aulas o vía WiFi con un determinado SSID asociado a una VLAN.
- VLAN de invitados: en esta VLAN se podrían conectar los diferentes smartphones y tablets de los propios alumnos, los padres cuando hacen visitas etc.



Tal y como podéis ver, una VLAN nos va a permitir segmentar la red local en varias subredes más pequeñas, enfocadas específicamente a una tarea en cuestión, además, podremos proporcionar seguridad porque las VLAN entre ellas no se podrán comunicar (o sí, dependiendo de la configuración de las ACL que nosotros queramos). Gracias a las VLAN el rendimiento general de la red mejorará, porque estaremos conteniendo el broadcast en dominios de difusión más pequeños.

Tipos de VLANs

Actualmente existen varios **tipos de VLANs** que podemos utilizar en los diferentes equipos, es decir, en los switches y puntos de acceso WiFi. Las diferentes VLANs que existen son las basadas en el estándar 802.1Q VLAN Tagging basado en etiquetas, las VLAN basadas en puerto, las VLAN basadas en MAC, las VLAN basadas en aplicaciones, aunque esta última no suele utilizarse habitualmente.

802.1Q VLAN Tagging

Es el tipo de VLAN más utilizada, hace uso del **estándar 802.1Q** para etiquetas o quitar la etiqueta a las VLANs. Este estándar consiste en introducir una cabecera 802.1Q dentro de la trama Ethernet que todos conocemos, con el objetivo de diferenciar las diferentes VLANs que tengamos configuradas. Este estándar no encapsula la trama original de Ethernet, sino que añade 4 bytes al encabezado

Ethernet original, además, el cambio de «EtherType» se cambia al valor 0x8100 para señalar que se ha cambiado el formato de la trama.

VLAN basadas en puerto

También conocida como Port Switching en los menús de **configuración de los routers y switches,** se trata de la más extendida y utilizada por switches de gama muy baja. Cada puerto se asigna a una VLAN y los usuarios que estén conectados a ese puerto pertenecen a la VLAN asignada. Los usuarios dentro de una misma VLAN poseen visibilidad los unos sobre los otros, aunque no a las redes locales virtuales vecinas.

El único inconveniente es que no permite dinamismo a la hora de ubicar los usuarios, y en el caso de que el usuario cambie de emplazamiento físicamente se debería reconfigurar la VLAN. En las VLANs basadas en puerto la decisión y reenvío se basa en la dirección MAC de destino y puerto asociado, es la VLAN más simple y común, por este motivo los switches de gama baja suelen incorporar VLAN basada en puerto y no basada en el estándar 802.1Q.

VLAN basadas en MAC

El razonamiento es similar a la anterior, salvo que en vez de ser una asignación a nivel de puerto lo es a nivel de dirección MAC del dispositivo. La ventaja es que permite movilidad sin necesidad de que se tengan que aplicar cambios en la configuración del switch o del router. El problema parece bastante claro: añadir todos los usuarios puede resultar tedioso. Solamente los switches de gama más alta permiten VLAN basada en MAC, cuando el switch detecta que se ha conectado una determinada dirección MAC le colocará automáticamente en una **VLAN específica**, esto es muy útil en los casos en los que queremos movilidad.

Imaginemos que nos conectamos con nuestro ordenador portátil en varios puertos Ethernet por nuestra oficina, y queremos que siempre nos asigne la misma VLAN, en este caso con las VLANs basadas en MAC sí es posible hacerlo sin tener que reconfigurar el switch. En grandes entornos empresariales esta funcionalidad es muy habitual para segmentar correctamente los equipos.

VLAN etiquetadas

Aquí veremos el etiquetado 802.1q que se define en el **estándar IEE 802.1q**. Permite a un dispositivo en red, agregar información a una trama en la capa 2, de forma que puede identificar la pertenencia a VLAN del marco. Este etiquetado permite que los entornos en red tengan VLAN, la cual abarca varios dispositivos. Un solo dispositivo recibe el paquete, lee la etiqueta y reconoce la VLAN a la que pertenece la trama. En algunos dispositivos, no se admite la recepción de paquetes etiquetados y no etiquetados en la misma interfaz de red. Si sucede

esto, debemos contactar con los administradores para que solucionen el problema.

En cuanto a la interfaz, esta puede ser un miembro del etiquetado o no etiquetado en una VLAN. Cada una de estas interfaces de red, es un miembro sin etiqueta de VLAN únicamente. En este caso, esta interfaz de red se encarga de transmitir las tramas de la VLAN nativa como tramas sin etiquetar. Pero una interfaz de red puede formar parte de diferentes VLAN, sin que las otras se encuentren etiquetadas.

Cuando configuramos un etiquetado, debemos asegurarnos de que este coincide con la configuración asignada a la VLAN en todos sus extremos. Y el puerto al que nos conectamos, debe estar en la misma VLAN que la interfaz. También debemos saber que, si la **configuración de la VLAN** no está sincronizada y propagada, se tiene que realizar la configuración en todas las unidades de forma independiente.

VXLAN

Se trata de una red de área local virtual extensible. **Esta superpone redes de capa 2**, en una infraestructura de capa 3, encapsulando tramas de capa 2 en paquetes UDP.

Bibliografía

De Luz, S. (2021, agosto 12). *VLANs: Qué son, tipos y para qué sirven*. RedesZone. https://www.redeszone.net/tutoriales/redes-cable/vlan-tipos-configuracion/

Peterson, L. L., & Davie, B. S. (2011). *Computer Networks: A Systems Approach* (5a ed.). Morgan Kaufmann.