VLAN Management

Transcribed on July 29, 2025 at 9:49 PM by Minutes AI

Speaker 1 (00:04)

Bienvenidos a esta nueva sesión.

En esta sesión vamos a tratar el tema de las VLAN más en profundidad.

Ya hemos hablado de forma breve de la segmentación tipo VLAN, pero esta vez nos centraremos en las diferentes técnicas y operaciones para configurarlas.

De nuevo es importante antes de sentarse a configurar la segmentación, un estudio previo de las redes que tenemos y su direccionamiento, aunque ya sabemos lo que es una VLAN.

Una VLAN significa Virtual Local Area Network y aquí lo vamos a ver más en profundidad.

Pues bien, a modo de repaso sabemos que es una tecnología que nos permite segmentar una red física dentro de otras redes lógicas, lo que crea un aislamiento que se puede dividir en grupos, departamentos o incluso dependiendo del tipo de tráfico, y esto convierte a las VLAN en una técnica realmente efectiva a la hora de hacer un hardening o una securización de una red de datos.

Bien, al hablar de VLAN tenemos que hablar de switches gestionados, ya que estos son los elementos encargados de gestionar y configurar las VLANs.

No todos los switches son gestionados, los que solemos tener en casa no suelen ser switches que se puedan gestionar, que se puedan crear VLAN, con lo cual estamos hablando de un nivel superior de este tipo de hardware o dispositivos.

Estos nos permiten configurar a veces desde una línea de comandos o desde una web todo tipo de configuraciones.

El primer paso será identificar físicamente los puertos que se van a utilizar para cada VLAN y después cada cable irá conectado a un puerto concreto del switch, por lo que es necesario una buena fase de planificación y localización de los usuarios físicamente dentro de la organización.

Aquí podéis ver un gráfico en el que a la izquierda tenéis un esquema de cómo sería esa configuración y cómo estaría interconectada y su reflejo directo en el hardware.

Cada color corresponde a una VLAN y es ahí donde conectaríamos a los usuarios físicos que queramos que tengan acceso a las diferentes VLAN.

En este punto quiero destacar que es muy importante realizar una buena selección del dispositivo que se va a util, hay que mirar sus características, pero sobre todo su posibilidad de escalabilidad, porque es muy habitual cambiar de ubicación a los usuarios, cambiar de planta, etc.

En el ejemplo que podéis ver en la diapositiva a la derecha, en el switch físico podéis ver perfectamente cuál sería la ubicación, por ejemplo en verde podría ser perfectamente el departamento de recursos humanos, el amarillo podría ser el de Haití, etcétera.

Cualquier equipo conectado a uno de estos switches, a uno de estos puertos que están asignados en la VLAN, tendría acceso a una cantidad determinada de recursos.

Aquí os quiero recordar que los switches trabajan en la capa 2 OSI, que es la de Data Link.

Por este motivo tenéis que saber que el switch distingue a nivel de paquete y es capaz de leer etiquetas que lo identifican, esta trama o estos paquetes.

Y aquí podemos definir dentro de esa trama o esos paquetes hay etiquetas que son las que definen a qué VLAN corresponde.

La identificación de los frames del paquete Ethernet, o sea, identificador VLAN, está especificado por un estándar que es el Q.

Bien, pues antes hemos comentado que los puertos Ethernet del switch se agrupan en esos grupos de colores que hemos visto que corresponden a las VLANs.

Entonces aquí se pueden conectar todo tipo de dispositivos, una impresora, cualquier cosa que tenga tarjeta de red podría estar asignada a una VLAN.

Pero claro, como he comentado antes, debe ser dinámico y escalable, ya que puede haber cambios de ubicación, puede llegar nuevos usuarios que queramos añadirlo a esa VLAN, etc.

Entonces aquí es donde aparece un puerto, un puerto llamado trunk.

Estos puertos tienen la misión de transmitir la información de las VLAN entre los otros switches de la misma empresa u organización.

De esta forma podemos extender una VLAN a otros switches dentro de la misma red.

Por lo tanto es una forma de crear lo que se llaman pilas o stack de diferentes servidores interconectados entre todos ellos.

Aquí podéis ver un ejemplo de esa conexión por los trunks.

El puerto trunk sería aquello que veis en forma de círculo con el color correspondiente a su VLAN y serían los puertos que interconectan los diferentes aparatos, en este caso los switches, de forma física a través de un cable.

En otras palabras, es como si extendiéramos nuestra VLAN simplemente haciendo un puente entre cada uno de los switches.

Y aquí quiero hacer hincapié en la seguridad de esos puertos, ya que tienen una importancia crítica en la infraestructura.

Algunos tipos de switches pueden establecer políticas de seguridad que se asocian al tipo de puerto que hemos utilizado.

Esto se llama en el argot el Port Security.

De esta forma es posible aplicar una política de seguridad al puerto trunk, por ejemplo, limitando por ejemplo el número de Macs que pueden circular por las VLANs, y también incluso podemos filtrarlas o incluso si vemos que hay un tipo de actividad extraña, podemos activar una acción de desconexión directa del puerto trunk y a su vez enviar algún tipo de alerta usando el protocolo, por ejemplo SMNP como una alerta de seguridad.

El protocolo encargado de transmitir la información entre las diferentes VLANs a través de los puertos tipo trunk se llama VTP o VLAN Trunk Protocol.

Cada VLAN debe tener asignado también su propio rango de direcciones IP, tal y como hemos visto en anteriores capítulos que hablaban sobre el direccionamiento.

El router lo que hará será identificar las diferentes VLANs que conforman el switch o los switches para de esta forma enrutar la información.

El servidor DHCP debe ser el encargado de asignar las direcciones IP para cada VLAN.

De esta forma conseguimos dividir más la infraestructura y automatizar el proceso de asignación de IPs, el cual incluso se podría hacer más seguro utilizando alguna de las técnicas que ya hemos visto anteriormente.

Y aquí quiero hablar de un pequeño detalle que suele pasar desapercibido y es que hay que configurar todos y cada uno de los puertos del switch, tanto si lo utilizamos como no.

Si no lo utilizamos tenemos que deshabilitarlo.

Esto es un problema que va asociado a la seguridad física, con lo cual es importante que los puertos que no utilicemos estén deshabilitados para que nadie pueda poner un cable y conectarse a esa VLAN.

Existen varios tipos de VLAN o VLANs, por ejemplo tenemos la VLAN por defecto, que es la de default, esta es la configuración base, aquí es donde se crea una VLAN que agrupa a todos los puertos, es la VLAN que viene por defecto, suele ser la VLAN 1 o VLAN 0 en algunos casos, y es la que se encarga del control de todo el tráfico, con lo cual cualquier switch lleva ya pre configurada una VLAN aunque esté en todos los puertos, que es la VLAN 0 o VLAN 1, que es la VLAN por defecto.

Las siguientes son las VLAN nativa o Native VLAN Aquí se permite el tráfico de cualquier tipo de paquetes o de frames, es decir, ni etiquetados ni nada, es decir, cualquier tipo de tráfico de red.

Esta configuración se suele utilizar básicamente para solucionar problemas de compatibilidad con otro tipo de redes, pero claro, no se puede securizar ni casi se puede procesar o gestionar, por eso es un tipo de red exclusivamente para hacer testeo o pruebas.

Después tenemos la VLAN de Gestión o de Management, la función de este tipo de VLAN es dar acceso directo a la gestión de los switches, por norma o de forma o por defecto está en la misma VLAN que la VLAN 1, o sea la VLAN por defecto VLAN 1 o VLAN 0, y esto es una mala práctica de seguridad, ya que supondría o digamos que expondría los puertos de gestión al resto de usuarios, y eso no queremos, no queremos que cualquier usuario acceda al puerto de gestión, por ese motivo es una buena práctica definir esta VLAN, la que vamos a utilizar para la gestión, fuera de la que viene por defecto.

Después tenemos la de Voz, las VLAN para Voz o las voip voip.

Estos puertos soportan este tipo de tráfico, lo que implica que van a mayor velocidad, los dispositivos VoIP tienen mayor prioridad de tráfico dentro de la red, además no les hace falta mucho más ancho de banda, por ese motivo es necesario configurarlas siempre para que solo funcionen para esta función de Voz IP, es decir, si tenemos que montar Voz IP hay que montar una VLAN dedicada exclusivamente para ello.

Y aquí os quiero recordar que un dispositivo Voz IP no es más que un aparato de red, tiene una IP y tiene una Mac.

Por este motivo se pueden aplicar todas las técnicas que hemos descrito hasta ahora de protección, porque no es más que otro elemento dentro de la arquitectura.

Y por último tenemos la VLAN para Datos o Data VLAN, y aquí es donde se va a generar el mayor tráfico de la red, ya que es por donde va a circular todos los paquetes que se han generado por los diferentes usuarios, dispositivos, etc.

Y estos puertos se pueden securizar de forma individual o colectiva, o sea, podemos securizar un puerto concreto o podemos securizar toda la OBLAN.

Bien, pues aquí tenéis un pequeño listado que resume algunas de las buenas prácticas que intentan mitigar en lo posible problemas e incidentes que están asociados con la seguridad de las VLANs.

Bien, algunos son obvios, como el primero que es no usar la configuración por defecto, que te desconectes tío.

Ahora bien, las VLAN, por ejemplo un ID por departamento, desconectar los puertos que no usamos, desactivar los puertos trunk que no usamos.

También es súper importante crear una VLAN de gestión de Management, este punto también es muy importante, permitir solo acceso SSH a esta red de gestión, esto quiere decir que podemos configurar puertos para que sólo gestionen un tipo de protocolo y esto es muy muy interesante.

Después tenemos el crear siempre una VLAN para invitados, no meter equipos que no están controlados por nosotros dentro de la red corporativa.

Lo que dije antes también de la voz IP que debe estar en una VLAN diferente a la de datos.

Y el siguiente punto es obvio, filtrar, filtrar siempre los puertos, sino utilizar siempre los puertos que necesitamos, ni uno más ni uno menos.

Y ya por último tenemos que evitar crear reglas del tipo VLAN to VLAN a no ser que que no sea, vamos, que sea estrictamente necesario.

Para hacer esto lo que podemos hacer son utilizar reglas que van de VLAN to Host o de Host to VLAN.

Esto es una técnica un poco más específica pero que sepáis que existe y que se puede hacer y la clave está en evitar siempre las reglas de VLAN a VLAN.

Y por último una técnica que ya conocéis bien que es la de ACL o las listas de acceso, que funciona exactamente igual que lo que hemos hablado hasta ahora sobre las reglas, que básicamente lo que hace es permitir o no el tráfico entre las diferentes VLANs.

En conclusión, hemos demostrado y hemos visto que es fundamental utilizar las VLANs o las VLANs como un elemento básico en lo que es la protección de nuestra arquitectura de red de datos.

Aquí aparece la figura de los switches gestionados y su gran importancia al poder segmentar redes sociales físicas en redes lógicas.

Por este motivo esta técnica se convierte en una técnica crítica que tenemos que utilizar sí o sí en cualquier arquitectura que pretendemos que tenga un nivel alto de seguridad.

Llegamos al final de la sesión, os esperamos en el siguiente vídeo.