Sistemas de Computación 2

<< Redes >>

Virtual Local Area Network

VLAN

Una de las técnicas que contribuyen a mejorar el rendimiento de una red es la división de los grandes dominios de difusión en dominios más pequeños.

Por una cuestión de diseño, los routers bloquean el tráfico de difusión en una interfaz. Sin embargo, los routers generalmente tienen una cantidad limitada de interfaces LAN. La función principal de un router es trasladar información entre las redes, no proporcionar acceso a la red a las terminales.

La función de proporcionar acceso a una LAN suele reservarse para los switches de capa de acceso. Se puede crear una red de área local virtual (VLAN) en un switch de capa 2 para reducir el tamaño de los dominios de difusión, similares a los dispositivos de capa 3. Por lo general, las VLAN se incorporan al diseño de red para facilitar que una red dé soporte a los objetivos de una organización.

Las VLAN proporcionan la segmentación y la flexibilidad organizativa. Las VLAN proporcionan una manera de agrupar dispositivos dentro de una LAN.

Un grupo de dispositivos dentro de una VLAN se comunica como si estuvieran conectados al mismo cable. Las VLAN se basan en conexiones lógicas, en lugar de conexiones físicas.

Características de las VLAN

Las VLAN permiten que el administrador divida las redes en segmentos según factores como la función, el equipo de trabajo o área, sin tener en cuenta la ubicación física del usuario o del dispositivo.

Los dispositivos dentro de una VLAN funcionan como si estuvieran en su propia red independiente, aunque compartan una misma infraestructura con otras VLAN.

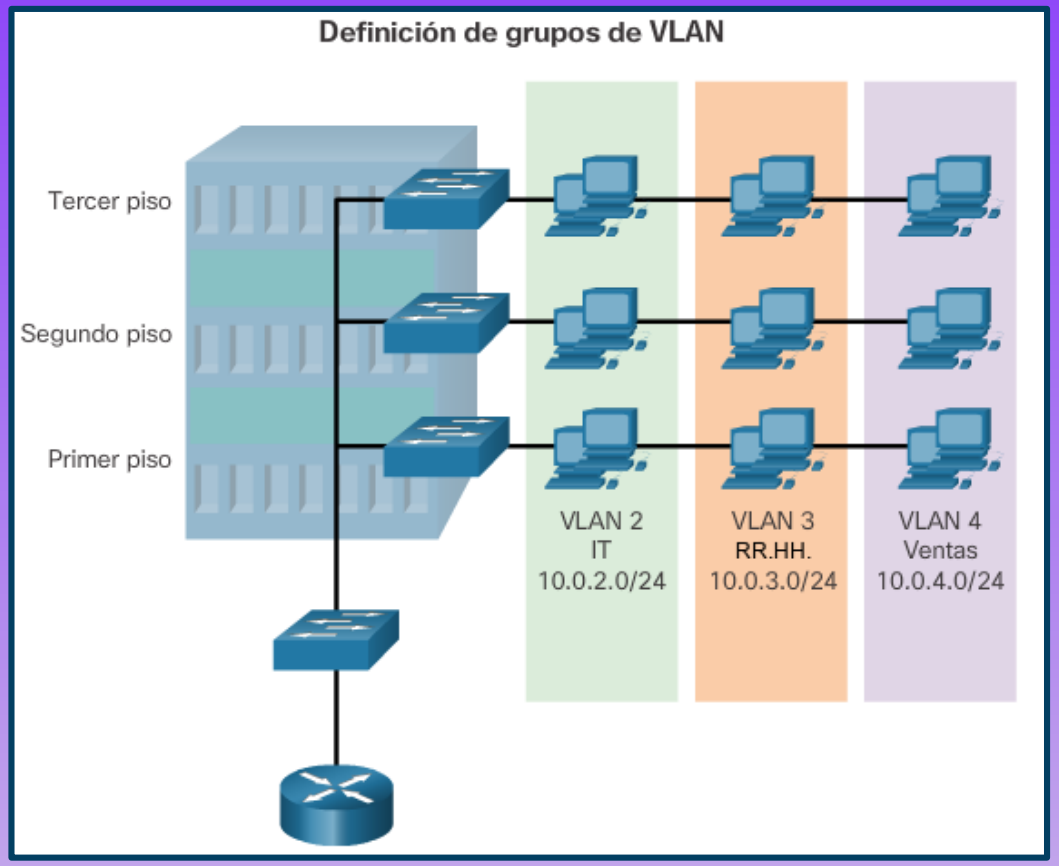
Cualquier puerto de switch puede pertenecer a una VLAN, y los paquetes de unidifusión, difusión y multidifusión se reenvían y saturan solo las estaciones terminales dentro de la VLAN donde se originan los paquetes.

Cada VLAN se considera una red lógica independiente, y los paquetes destinados a las estaciones que no pertenecen a la VLAN se deben reenviar a través de un dispositivo que admita el routing.

Las VLAN habilitan la implementación de las políticas de acceso y de seguridad según grupos específicos de usuarios.

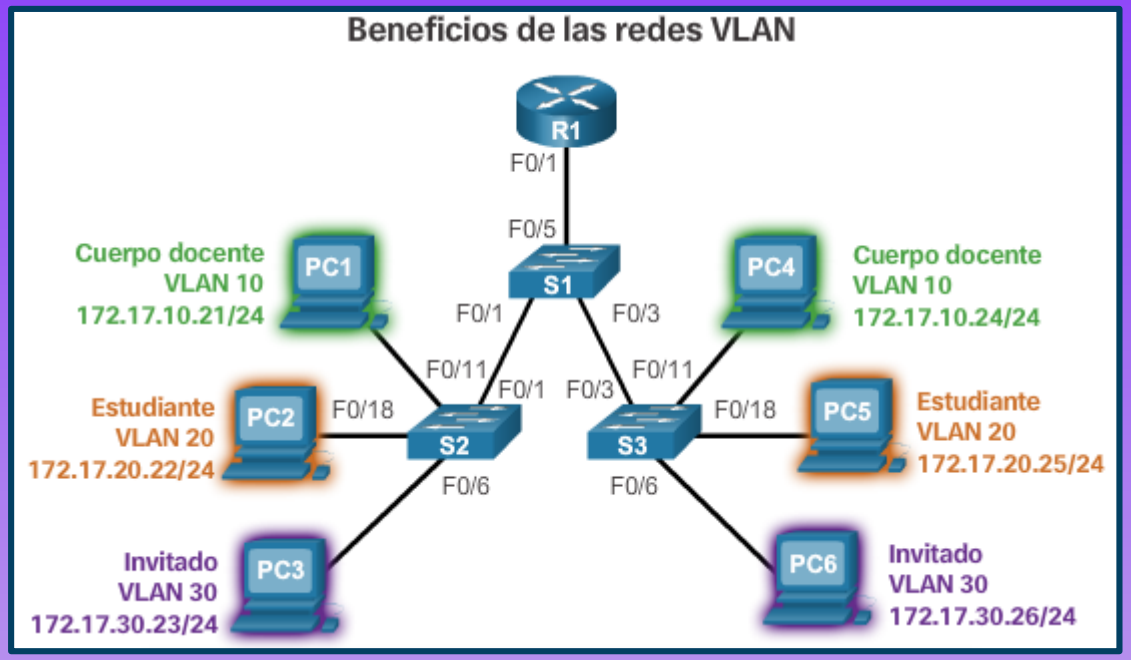
Cada puerto de un switch se puede asignar a una sola VLAN (a excepción de un puerto conectado a un teléfono IP o a otro switch).

Beneficios de las VLAN



- Seguridad: los grupos que tienen datos sensibles se separan del resto de la red, lo que disminuye las posibilidades de que ocurran violaciones de información confidencial.
- Reducción de costos: el ahorro de costos se debe a la poca necesidad de actualizaciones de red costosas y al uso más eficaz de los enlaces y del ancho de banda existentes.
- Mejor rendimiento: la división de las redes planas de capa 2 en varios grupos de trabajo lógicos (dominios de difusión) reduce el tráfico innecesario en la red y mejora el rendimiento.
- Dominios de difusión reducidos: la división de una red en redes VLAN reduce la cantidad de dispositivos en el dominio de difusión.

Beneficios de las VLAN



- Mayor eficiencia del personal de IT: las VLAN facilitan el manejo de la red debido a que los usuarios con requerimientos similares de red comparten la misma VLAN. Cuando se dispone de un switch nuevo, se implementan todas las políticas y los procedimientos que ya se configuraron para la VLAN específica cuando se asignaron los puertos. También es fácil para el personal de IT identificar la función de una VLAN proporcionándole un nombre.
- Administración más simple de aplicaciones y proyectos: las VLAN agregan dispositivos de red y usuarios para admitir los requisitos geográficos o comerciales. Al tener características diferentes, se facilita la administración de un proyecto o el trabajo con una aplicación especializada; un ejemplo de este tipo de aplicación es una plataforma de desarrollo de aprendizaje por medios electrónicos para el cuerpo docente.

Tipos de VLAN

VLAN predeterminada:Todos los puertos de switch se vuelven parte de la VLAN predeterminada después del arranque inicial de un switch que carga la configuración predeterminada. Los puertos de switch que participan en la VLAN predeterminada forman parte del mismo dominio de difusión. La VLAN 1 tiene todas las características de cualquier VLAN, excepto que no se le puede cambiar el nombre ni se puede eliminar. Todo el tráfico de control de capa 2 se asocia a la VLAN 1 de manera predeterminada.

VLAN nativa: Una VLAN nativa está asignada a un puerto troncal 802.1Q. Los puertos de enlace troncal son los enlaces entre switches que admiten la transmisión de tráfico asociado a más de una VLAN. Los puertos de enlace troncal 802.1Q admiten el tráfico proveniente de muchas VLAN (tráfico con etiquetas), así como el tráfico que no proviene de una VLAN (tráfico sin etiquetar). El tráfico con etiquetas hace referencia al tráfico que tiene una etiqueta de 4 bytes insertada en el encabezado de la trama de Ethernet original, que especifica la VLAN a la que pertenece la trama. El puerto de enlace troncal 802.1Q coloca el tráfico sin etiquetar en la VLAN nativa, que es la VLAN 1 de manera predeterminada.

Se recomienda configurar la VLAN nativa como VLAN sin utilizar, independiente de la VLAN 1 y de otras VLAN. De hecho, es común utilizar una VLAN fija para que funcione como VLAN nativa para todos los puertos de enlace troncal en el dominio conmutado.

Tipos de VLAN

VLAN de datos: es una VLAN configurada para transportar tráfico generado por usuarios. Una VLAN que transporta tráfico de administración o de voz no sería una VLAN de datos. Es una práctica común separar el tráfico de voz y de administración del tráfico de datos. A veces a una VLAN de datos se la denomina VLAN de usuario. Las VLAN de datos se usan para dividir la red en grupos de usuarios o dispositivos.

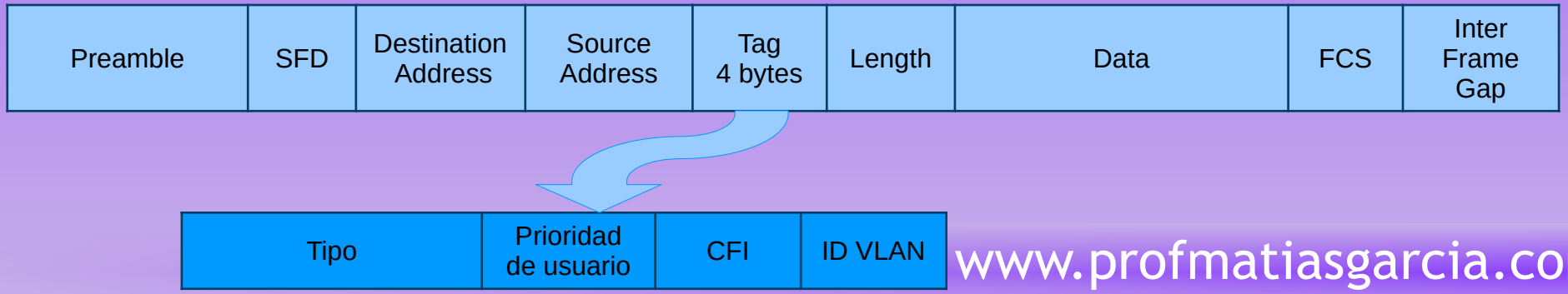
VLAN de administración: es cualquier VLAN que se configura para acceder a las capacidades de administración de un switch. La VLAN 1 es la VLAN de administración de manera predeterminada. Para crear la VLAN de administración, se asigna una dirección IP y una máscara de subred a la interfaz virtual de switch (SVI) de esa VLAN, lo que permite que el switch se administre mediante HTTP, Telnet, SSH o SNMP. Dado que en la configuración de fábrica de un switch Cisco la VLAN 1 se establece como VLAN predeterminada, la VLAN 1 no es una elección adecuada para la VLAN de administración.

Etiquetado VLAN

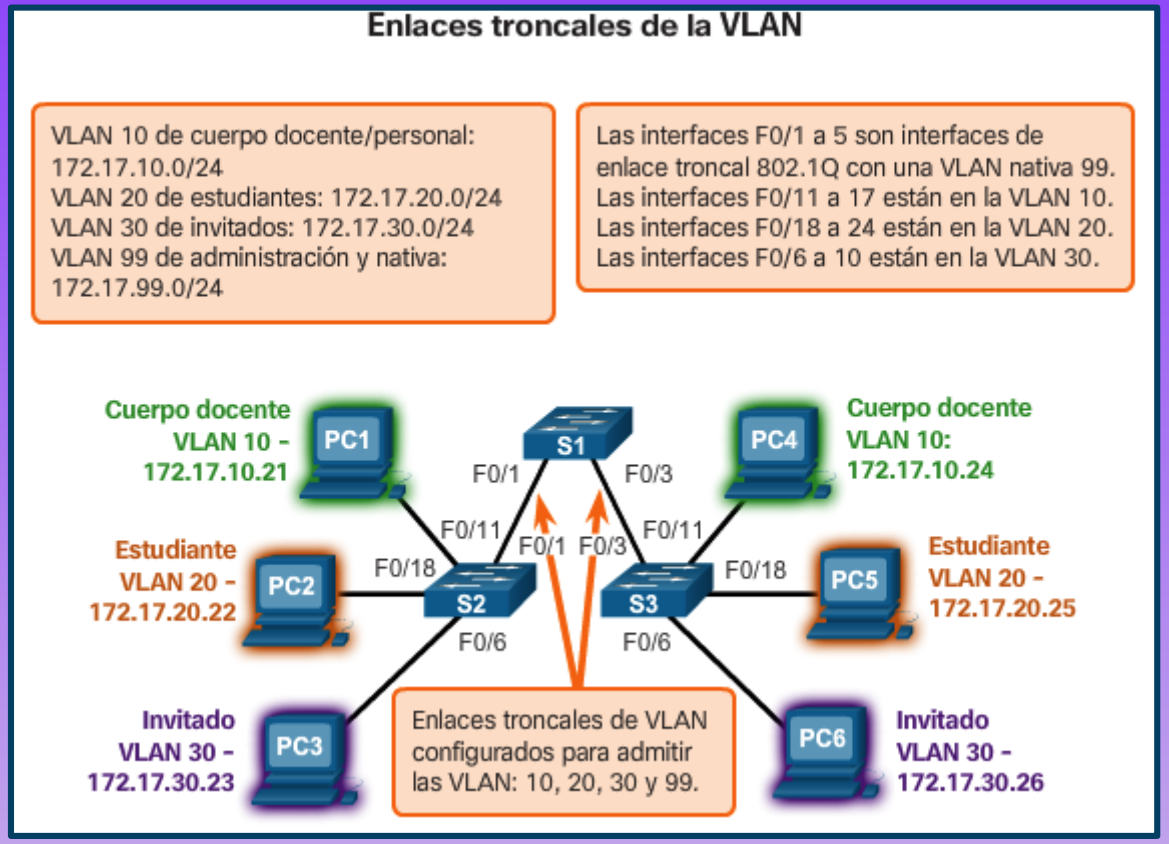
El campo de etiqueta de la VLAN consta de un campo de tipo, un campo de prioridad, un campo de identificador de formato canónico y un campo de ID de la VLAN:

- Tipo: es un valor de 2 bytes denominado “ID de protocolo de etiqueta” (TPID). Para Ethernet, este valor se establece en 0x8100 hexadecimal.
- Prioridad de usuario: es un valor de 3 bits que admite la implementación de nivel o de servicio.
- Identificador de formato canónico (CFI): es un identificador de 1 bit que habilita las tramas Token Ring que se van a transportar a través de los enlaces Ethernet.
- ID de VLAN (VID): es un número de identificación de VLAN de 12 bits que admite hasta 4096 ID de VLAN.

Una vez que el switch introduce los campos Tipo y de información de control de etiquetas, vuelve a calcular los valores de la FCS e inserta la nueva FCS en la trama.



VLAN en entornos computados



Un enlace troncal es un enlace punto a punto entre dos dispositivos de red que llevan más de una VLAN. Un enlace troncal de VLAN amplía las VLAN a través de toda la red. Cisco admite IEEE 802.1Q para coordinar enlaces troncales en las interfaces Fast Ethernet, Gigabit Ethernet y 10-Gigabit Ethernet.

Los enlaces troncales de VLAN permiten que se propague todo el tráfico de VLAN entre los switches, de modo que los dispositivos que están en la misma VLAN pero conectados a distintos switches se puedan comunicar sin la intervención de un router.

Asignación de VLAN

Los distintos switches admiten diversas cantidades de VLAN. La cantidad de VLAN que admiten es suficiente para satisfacer las necesidades de la mayoría de las organizaciones. Las VLAN de rango normal en estos switches se numeran del 1 al 1005, y las VLAN de rango extendido se numeran del 1006 al 4094.

VLAN de rango normal

- Se utiliza en redes de pequeños y medianos negocios y empresas.
- Se identifica mediante un ID de VLAN entre 1 y 1005.
- Los ID de 1002 a 1005 se reservan para las VLAN Token Ring y FDDI.
- Los ID 1 y 1002 a 1005 se crean automáticamente y no se pueden eliminar.
- Las configuraciones se almacenan en un archivo de base de datos de VLAN, denominado vlan.dat. El archivo vlan.dat se encuentra en la memoria flash del switch.
- El protocolo de enlace troncal de VLAN (VTP), que permite administrar la configuración de VLAN entre los switches, solo puede descubrir y almacenar redes VLAN de rango normal.

VLAN de rango extendido

- Posibilita a los proveedores de servicios que amplíen sus infraestructuras.
- Las configuraciones no se escriben en el archivo vlan.dat, sino en un archivo en ejecución
- Admiten menos características que las VLAN de rango normal.

Enlaces troncales de VLAN

Un enlace troncal de VLAN es un enlace entre dos switches que transporta el tráfico para todas las VLAN (a menos que se restrinja la lista de VLAN permitidas de manera manual o dinámica). Para habilitar los enlaces troncales, configure los puertos en cualquier extremo del enlace físico con conjuntos de comandos paralelos.

Un enlace troncal no pertenece a una VLAN específica. Es más bien un conducto para las VLAN entre los switches y los routers.

Para configurar un puerto de switch en un extremo de un enlace troncal, utilice el comando `switchport mode trunk`. Con este comando, la interfaz cambia al modo de enlace troncal permanente.

El puerto establece una negociación de protocolo de enlace troncal dinámico (DTP) para convertir el enlace en un enlace troncal, incluso si la interfaz conectada a este no acepta el cambio.

Utilice el comando `switchport trunk allowed vlan lista-vlan` para especificar la lista de VLAN que se permiten en el enlace troncal.

Enrutamiento entre VLAN

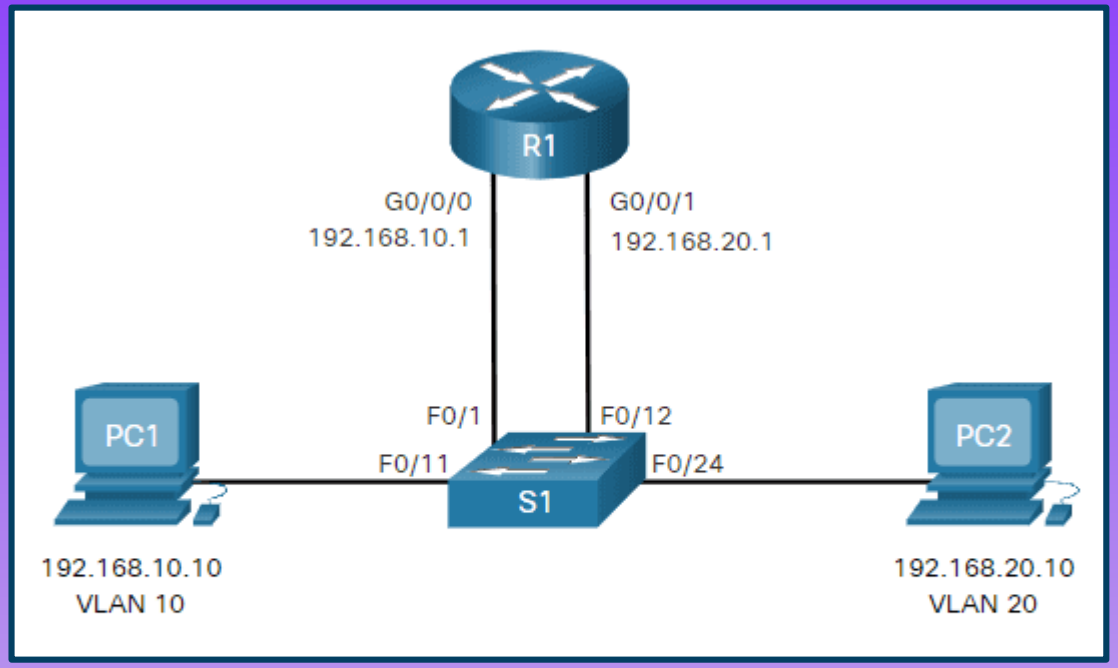
Las VLAN se utilizan para segmentar las redes de switch de Capa 2 por diversas razones. Independientemente del motivo, los hosts de una VLAN no pueden comunicarse con los hosts de otra VLAN a menos que haya un router o un switch de capa 3 para proporcionar servicios de enrutamiento.

El Enrutamiento Entre VLAN (Inter-VLAN Routing) es el proceso de reenviar el tráfico de red de una VLAN a otra VLAN.

Hay tres opciones de Enrutamiento inter-VLAN:

- Inter-VLAN Routing heredado – Esta es una solución antigua. No escala bien
- Router-on-a-stick – Esta es una solución aceptable para una red pequeña y mediana.
- Switch de capa 3 con interfaces virtuales (SVIs) : esta es la solución más escalable para organizaciones medianas y grandes.

Inter-VLAN Routing heredado



La primera solución de enrutamiento inter-VLAN se basó en el uso de un router con múltiples interfaces Ethernet. Cada interfaz del router estaba conectada a un puerto del switch en diferentes VLAN. Las interfaces del router sirven como puertas de enlace predeterminada para los hosts locales en la subred de la VLAN.

El enrutamiento entre VLAN heredado usando interfaces físicas funciona, pero tiene una limitación significativa. No es razonablemente escalable porque los routers tienen un número limitado de interfaces físicas. Requerir una interfaz física de router por VLAN agota rápidamente la capacidad de interfaz física de un router.

Enrutamiento router-on-a-stick’

Solo requiere una interfaz Ethernet física para enrutar el tráfico entre varias VLAN de una red.

Una interfaz Ethernet del router se configura como un troncal 802.1Q y se conecta a un puerto troncal en un switch de capa 2. Específicamente, la interfaz del router se configura mediante subinterfaces para identificar VLAN enrutables.

Las subinterfaces configuradas son interfaces virtuales basadas en software. Cada uno está asociado a una única interfaz Ethernet física. Estas subinterfaces se configuran en el software del router. Cada una se configura de forma independiente con sus propias direcciones IP y una asignación de VLAN. Las subinterfaces se configuran para subredes diferentes que corresponden a su asignación de VLAN. Esto facilita el enrutamiento lógico.

Cuando el tráfico etiquetado de VLAN entra en la interfaz del router, se reenvía a la subinterfaz de VLAN. Después de tomar una decisión de enrutamiento basada en la dirección de red IP de destino, el router determina la interfaz de salida del tráfico. Si la interfaz de salida está configurada como una subinterfaz 802.1q, las tramas de datos se etiquetan con la nueva VLAN y se envían de vuelta a la interfaz física.

Enrutamiento con switch capa 3

El método moderno para realizar inter-VLAN routing es utilizar switches de capa 3 e interfaces virtuales del switch (SVI). Una SVI es una interfaz virtual configurada en un switch de capa 3.

Los SVIs entre VLAN se crean de la misma manera que se configura la interfaz de VLAN de administración. El SVI se crea para una VLAN que existe en el switch. Aunque es virtual, el SVI realiza las mismas funciones para la VLAN que lo haría una interfaz de router. Específicamente, proporciona el procesamiento de Capa 3 para los paquetes que se envían hacia o desde todos los puertos de switch asociados con esa VLAN.

ventajas del uso de switches de capa 3 para el enrutamiento inter-VLAN:

- Es mucho más veloz que router-on-a-stick, porque todo el switching y el routing se realizan por hardware.
- El routing no requiere enlaces externos del switch al router para el enrutamiento.
- No se limitan a un solo enlace porque los EtherChannels de Capa 2 pueden ser usados como enlaces troncales entre los switches para aumentar el ancho de banda.
- La latencia es mucho más baja, dado que los datos no necesitan salir del switch para ser enrutados a una red diferente.
- Se implementan con mayor frecuencia en una LAN de campus que en routers.

La única desventaja es que son más caros.

Bibliografía & Licencia

- CCNA 2 (2017). Switching, Routing and Wireless Essentials. Cisco Press.
- Textos tomados, corregidos y modificados de diferentes páginas de Internet, tutoriales y documentos.

- Autor:

Matías E. García

Prof. & Tec. en Informática Aplicada

www.profmatiasgarcia.com.ar

info@profmatiasgarcia.com.ar