**¿Cómo diferenciar los puertos de conmutación Ethernet de acuerdo con la arquitectura de la red?**

La arquitectura de red tradicional suele tener tres capas: la capa central, la capa de distribución y la capa de acceso. Por ende, los switches y puertos Ethernet también cuentan con estas características.

**Puerto de acceso**

El puerto de acceso se utiliza para conectar dispositivos como ordenadores de escritorio, portátiles, impresoras, etc., que sólo se encuentran disponibles en el enlace de acceso. Este tipo de puerto está vinculado a una red VLAN específica que envía y recibe tramas Ethernet regulares sin etiquetar; y por lo general, pertenece a una única red VLAN, es decir, a la VLAN de acceso, descartando todas las tramas que no estén clasificadas en la misma.

**Puerto Troncal**

El puerto troncal se utiliza entre los switches o el switch y los dispositivos de nivel superior, disponibles en el enlace troncal. Este permite la instalación de varias redes VLAN a través de la interfaz, y es capaz de transportar tráfico para numerosas redes VLAN simultáneamente. La diferencia principal entre un puerto troncal y un puerto de acceso es que el primero es un puerto de agregación de red VLAN conectado a otros puertos de un switch, y el segundo es un puerto que sirve para que el switch conecte el host con la red VLAN.

**Puerto Híbrido**

Un puerto híbrido sirve para conectar los dispositivos de red y los dispositivos de usuario. Soporta redes VLAN sin etiquetar a modo de puerto de acceso y redes VLAN etiquetadas a modo de puerto troncal. Asimismo, puede recibir datos de una o más redes VLAN. Estos puertos se asemejan a los puertos troncales en muchos aspectos, pero tienen otras características de configuración.

**Puerto QinQ**

La tunelización Q-in-Q y la traducción de VLAN permiten a los proveedores de servicios crear una conexión Ethernet de capa 2 entre dos sitios de cliente. Los proveedores pueden separar el tráfico de VLAN de diferentes clientes en un vínculo (por ejemplo, si los clientes usan identificadores de VLAN superpuestos) o agrupar VLAN de clientes diferentes en una VLAN de servicio único. Los centros de datos pueden usar la tunelización Q-in-Q y la traducción de VLAN para aislar el tráfico de clientes dentro de un solo sitio o para permitir los flujos de tráfico de clientes entre centros de datos en la nube en diferentes ubicaciones geográficas.



**Tipos de VLAN**

Existen diferentes tipos de redes VLAN, los cuales se utilizan en las redes modernas. Algunos tipos de VLAN se definen según las clases de tráfico. Otros tipos de VLAN se definen según la función específica que cumplen.

**VLAN de datos**

Una 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 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. Esto admite cualquier dispositivo conectado a cualquier puerto de switch para comunicarse con otros dispositivos en otros puertos de switch. La VLAN predeterminada para los switches Cisco es la VLAN 1. En la ilustración, se emitió el comando show vlan brief en un switch que ejecuta la configuración predeterminada. Observe que todos los puertos se asignan a la VLAN 1 de manera predeterminada.

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.

Las VLAN nativas se definen en la especificación IEEE 802.1Q a fin de mantener la compatibilidad con el tráfico sin etiquetar de modelos anteriores común a las situaciones de LAN antiguas. Una VLAN nativa funciona como identificador común en extremos opuestos de un enlace troncal.

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.

**VLAN de administración**

Una 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.

En el pasado, la VLAN de administración para los switches 2960 era la única SVI activa. En las versiones 15.x de IOS de Cisco para los switches de la serie Catalyst 2960, es posible tener más de una SVI activa. Con IOS de Cisco 15.x, se debe registrar la SVI activa específica asignada para la administración remota. Si bien, en teoría, un switch puede tener más de una VLAN de administración, esto aumenta la exposición a los ataques de red.

En la ilustración, actualmente todos los puertos están asignados a la VLAN 1 predeterminada. No hay ninguna VLAN nativa asignada explícitamente ni otras VLAN activas; por lo tanto, la VLAN nativa de la red que se diseñó es la VLAN de administración. Esto se considera un riesgo de seguridad.



**Puertos de tipo Access**

La principal utilidad que se les da a este tipo de puertos es para conectar equipos finales, los puertos de acceso solo transportan tráfico de una sola vlan y aunque los puertos de acceso también se pueden utilizar para conectar switches no es recomendable ya que una implementación de este tipo no es escalable.



Tomando como referencia la topología anterior, cuando una pc manda un paquete, dicho paquete no lleva ningún identificador ni sabe a que vlan pertenece y sera el switch quien le asigne el identificador de la vlan a la que este asociado el puerto.

A continuación se muestra la configuración que se debe aplicar en los puertos para ponerlos como acceso.



**Puerto de tipo IEEE 802.1Q (dot1q)**

El protocolo IEEE 802.1Q, también conocido como dot1Q, fue un proyecto del grupo de trabajo 802 de la IEEE para desarrollar un mecanismo que permita a múltiples redes compartir de forma transparente el mismo medio físico, sin problemas de interferencia entre ellas (Trunking). Es también el nombre actual del estándar establecido en este proyecto y se usa para definir el protocolo de encapsulamiento usado para implementar este mecanismo en redes Ethernet. Todos los dispositivos de interconexión que soportan VLAN deben seguir la norma IEEE 802.1Q que especifica con detalle el funcionamiento y administración de redes virtuales. \*Shortest Path Bridging (SPB) Incorporado al IEEE 802.1Q-2014[1](https://es.wikipedia.org/wiki/IEEE_802.1Q#cite_note-1)​

Formato de la trama



Insertion of 802.1Q tag in an Ethernet frame

802.1Q en realidad no encapsula la trama original sino que añade 4 bytes al encabezado Ethernet original. El valor del campo EtherType se cambia a 0x8100 para señalar el cambio en el formato de la trama.

Debido a que con el cambio del encabezado se cambia la trama, 802.1Q fuerza a un recálculo del campo "FCS".

**VLAN nativas**

No se etiquetan con el ID de VLAN cuando se envían por el trunk. Y en el otro lado, si a un puerto llega una trama sin etiquetar, la trama se considera perteneciente a la VLAN nativa de ese puerto. Este modo de funcionamiento fue implementado para asegurar la interoperabilidad con antiguos dispositivos que no entendían 802.1Q.

La VLAN nativa es la vlan a la que pertenecía un puerto en un switch antes de ser configurado como puerto trunk o como puerto acceso. Solo se puede tener una VLAN nativa por puerto.

Para establecer un trunking 802.1Q a ambos lados deben tener la misma VLAN nativa porque la encapsulación todavía no se ha establecido y los dos switches deben hablar sobre un link sin encapsulación (usan la native VLAN) para ponerse de acuerdo en estos parámetros. En los equipos de Cisco Systems la VLAN nativa por defecto es la VLAN 1. Por la VLAN 1 además de datos, se manda información sobre PAgP, CDP, VTP.

* La VLAN nativa no debe ser la de gestión.
* Cambiar la VLAN nativa de la 1 a cualquier otra como medida de seguridad.
* Todos los switches en la misma VLAN nativa.
* Usuarios y servidores en sus respectivas VLANs.
* El tráfico entre switches debe ser el único que no se encapsule en enlaces trunk. El resto del tráfico, incluyendo la VLAN de gestión debe ir encapsulado por los trunks. Si no estamos encapsulando cualquiera puede conectar un equipo que no hable 802.1Q (switches y hubs) y funcionará sin nuestro control.

**Puerto de tipo Híbrido**

Una VLAN híbrida es una red virtual que se crea por medio de dos sistemas: uno basado en etiquetas y otro basado en puertos. Para entender mejor en qué consiste la VLAN híbrida y por qué es uno de los métodos más usados, explicaremos en qué consiste cada uno de los dos sistemas que la componen.

**VLAN basada en etiquetas**

Una VLAN híbrida incluye un sistema basado en etiquetas, que sirve para crear redes virtuales de una manera muy sencilla y eficiente. Este sistema consiste en incluir códigos numéricos (por ejemplo: 0, 1, 100 o 200) en los paquetes de datos que gestiona una red. De esta manera, es posible segmentar el tráfico que se gestiona y se crean redes virtuales con conexiones limitadas, más seguras y eficientes.

Las VLAN basadas en etiquetas son las más utilizadas a la hora de crear redes virtuales. Sin embargo, existe otra manera para dividir el tráfico y los dominios de difusión de una red, el cual veremos a continuación.

**VLAN basada en puerto**

Una VLAN basada en puerto es una red virtual que se crea por medio de una gestión de las conexiones entre los puertos de los dispositivos conectados a una red. De esta manera, se puede asignar deliberadamente un límite para la conexión entre determinados dispositivos. A pesar de que es un método menos utilizado que la VLAN basada en etiquetas y la VLAN híbrida, este tipo de red virtual también es eficiente y, ahora, veremos por qué es útil combinarlo con los que hemos descrito anteriormente.

**¿Por qué utilizar una VLAN híbrida?**

El propósito de todas las VLAN es el mismo: crear divisiones dentro de la red para mitigar el daño ante un ciberataque y, a la vez, aumentar el nivel de organización y flujo de tráfico de una red. El tipo de VLAN indicado para cada red depende de sus propias condiciones y cada método es válido, según responda a sus necesidades. Sin embargo, la VLAN híbrida permite hacer conexiones de redes virtuales más complejas y aumentar el control sobre el esquema de la red.

**Puerto de tipo** [**QinQ**](https://community.fs.com/es/blog/qinq-vs-vlan-vs-vxlan.html)

El QinQ (también conocido como apilamiento VLAN) está estandarizado por el IEEE 802.1ad. Encapsula la etiqueta VLAN con dos capas: una etiqueta interior (de una red privada) y una etiqueta exterior (de la red pública). Como hay una creciente cantidad de usuarios en las redes, también ha aumentado el número de IDs de VLAN necesarios. El etiquetado VLAN tradicional que utiliza el IEEE 802.1Q es incapaz de identificar y aislar los datos de los usuarios en las obras crecientes de Metro Ethernet. La tecnología QinQ se utiliza para ampliar la cantidad VLANs hasta 4096×4096, de este modo se podrán ahorrar ID de VLAN públicas.

Los paquetes QinQ tienen un formato fijo. Normalmente, un paquete etiquetado 802.11Q se encapsula en otra etiqueta 802.1Q, de la que deriva el nombre «Q-in-Q». Durante la transmisión, los paquetes se reenvían en función de la etiqueta VLAN exterior en la red pública, se interpreta que la etiqueta forma parte de los datos, por lo que esta también se transmite en la red pública. Como contienen esta forma de doble etiqueta, los paquetes QinQ tienen cuatro bytes más que los paquetes comunes con etiqueta VLAN 802.1Q.



Hay dos tipos de implementaciones de QinQ: QinQ básico y QinQ selectivo.

El QinQ básico es un tipo de etiquetado basado en el puerto. Cuando un paquete llega a la interfaz que tiene activada la VLAN VPN (red privada virtual), el switch etiqueta el paquete con su etiqueta VLAN por defecto. No importa si el paquete entrante está etiquetado o no. Si ha sido etiquetado, entonces tendrá doble etiqueta VLAN; si no, tendrá una sola etiqueta VLAN con el puerto del switch.

El QinQ selectivo posee las funciones del QinQ básico, pero es más flexible. Identifica la etiqueta VLAN interna de los paquetes según la dirección MAC, el protocolo IP, la dirección IP de origen y la etiqueta VLAN, y luego determina qué etiqueta hay que añadir.

**Referencias**

https://es.wikipedia.org/wiki/IEEE\_802.1Q

https://www.reuter.com.ar/CCNA/CCNA2/mod3\_ccna2/

https://ccnadesdecero.com/curso/enrutamiento-intra-vlan/

https://keepcoding.io/blog/que-es-una-vlan-hibrida/