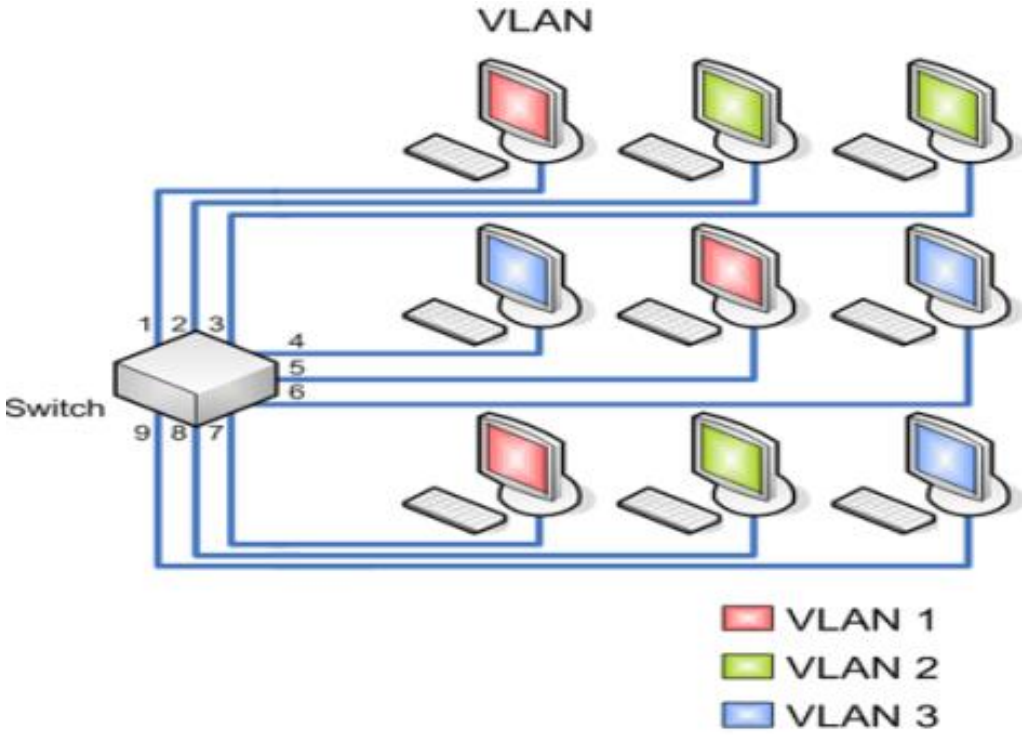
VLANs

Jhon Jairo Padilla Aguilar, PhD.

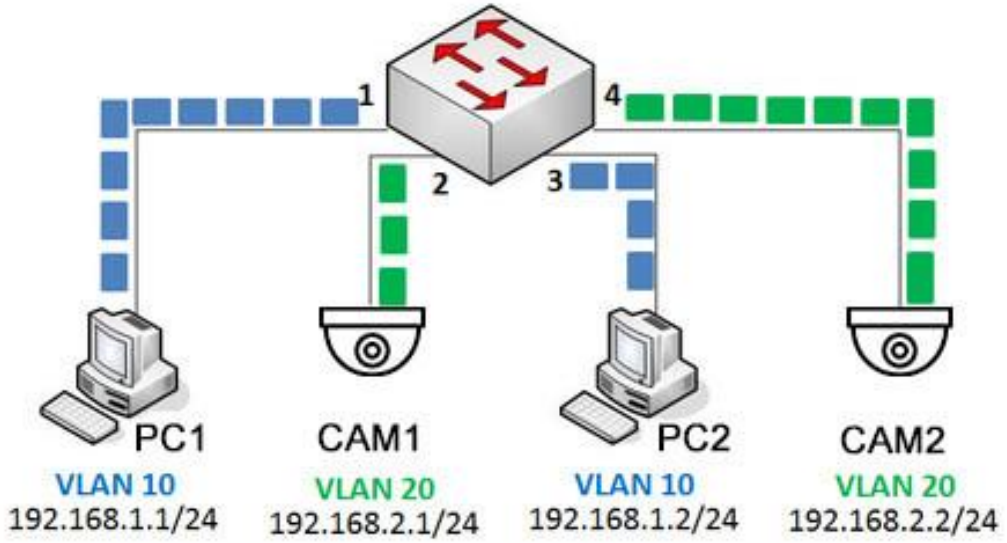
Definición de VLAN

- Una VLAN, acrónimo de virtual LAN (red de área local virtual), es un método para crear redes lógicas independientes dentro de una misma red física.
- Varias VLAN pueden coexistir en un único conmutador físico o en una única red física.
- Las VLAN son útiles para reducir el dominio de difusión (broadcast) y ayudan en la administración de la red, separando segmentos lógicos de una red de área local (los departamentos de una empresa, por ejemplo) que por seguridad no deberían intercambiar datos usando la red local.
- Una VLAN consiste en dos o más redes de computadoras que se comportan como si estuviesen conectados al mismo conmutador, aunque se encuentren físicamente conectados a diferentes segmentos de una red de área local.

Aplicación de las VLAN



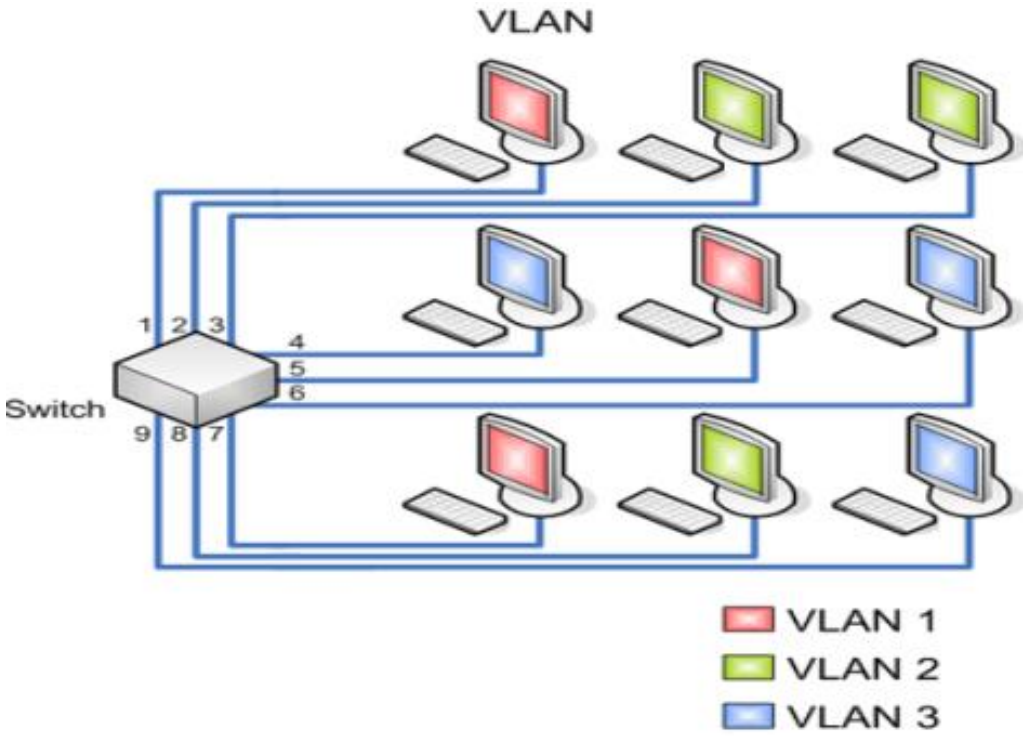
Segmentación de la red usando VLANs



Ejemplo de uso de VLANs para separar usuarios de diferentes tipos

Beneficios de las VLANs

- Control de broadcast:
  - Aisla el dominio de colisiones
- Seguridad:
  - Restricción de tráfico
  - Comunicación entre VLAN (capa 3)
- Rendimiento:
  - El tráfico generado por un grupo no afecta a otro.
- Administración de la red:
  - Facilidad ante cambios



Tipos de VLAN

Tipos de VLAN	Descripción
Basado en puerto	• Método de configuración más común • Los puertos se asignan individualmente, en grupos, en filas o en 2 o más switches • Uso sencillo • Se implementa a menudo donde el Protocolo de Control de Host Dinámico (DHCP) se usa para asignar las direcciones IP a los hosts de red
Dirección MAC	• Se implementa con escasa frecuencia hoy en día • Es necesario introducir y configurar cada dirección de forma individual • Los usuarios lo consideran útil • Administración, diagnóstico de fallas y gestión difíciles
Basado en protocolo	• Se configuran como las direcciones MAC, pero usan una dirección lógica o IP • Ya no son comunes debido a DHCP

VLAN estáticas y dinámicas

VLAN Estáticas

- Las VLAN estáticas también se denominan VLAN basadas en el puerto.

- Las asignaciones en una VLAN estática se crean mediante la asignación de los puertos de un switch o conmutador a dicha VLAN. Cuando un dispositivo entra en la red, automáticamente asume su pertenencia a la VLAN a la que ha sido asignado el puerto. Si el usuario cambia de puerto de entrada y necesita acceder a la misma VLAN, el administrador de la red debe cambiar manualmente la asignación a la VLAN del nuevo puerto de conexión en el switch.

VLAN Dinámicas:

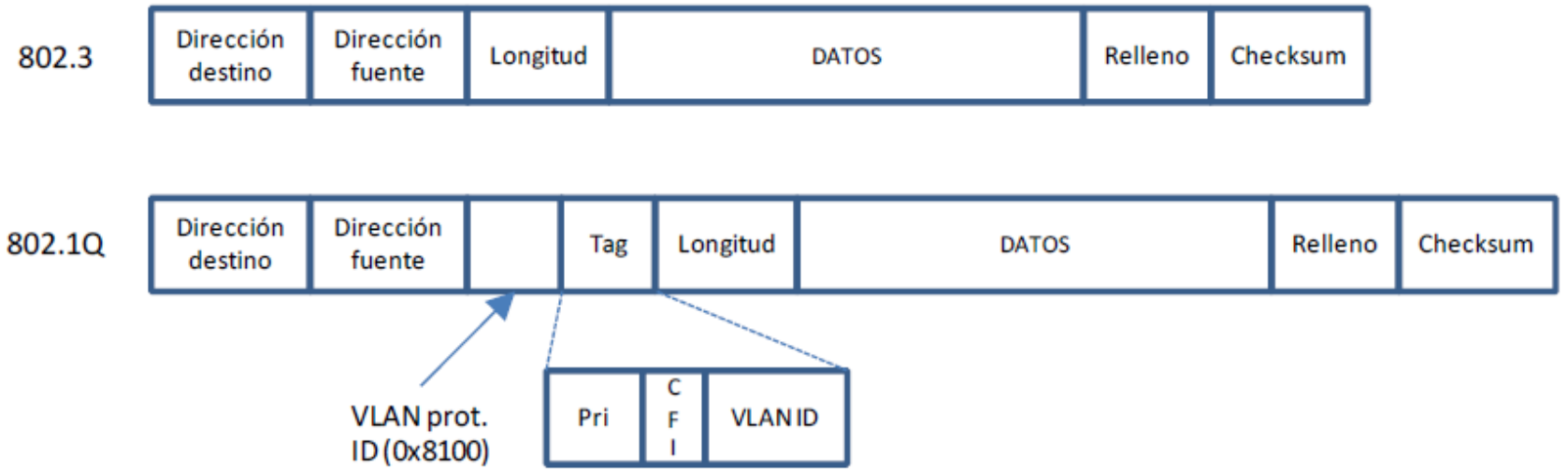
- En las VLAN dinámicas, la asignación se realiza mediante paquetes de software.
- Con el VMPS (acrónimo en inglés de VLAN Management Policy Server o Servidor de Gestión de Directivas de la VLAN), el administrador de la red puede asignar los puertos que pertenecen a una VLAN de manera automática basándose en información tal como la dirección MAC del dispositivo que se conecta al puerto o el nombre de usuario utilizado para acceder al dispositivo.
- En este procedimiento, el dispositivo que accede a la red, hace una consulta a la base de datos de miembros de la VLAN. Se puede consultar el software FreeNAC para ver un ejemplo de implementación de un servidor VMPS.

IEEE 802.1Q

- Es una modificación al estándar de Ethernet.
- El protocolo IEEE 802.1Q [3] fue un proyecto del grupo de trabajo 802 de IEEE para desarrollar un mecanismo que permita a múltiples redes interconectadas con puentes o switches compartir transparentemente el mismo medio físico sin problemas de interferencia entre las redes que comparten el medio (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.
- Permite identificar a una trama como proveniente de un equipo conectado a una red determinada.
- Una trama perteneciente a una VLAN sólo se va a distribuir a los equipos que pertenezcan a su misma VLAN, de forma que se separan dominios de broadcast.

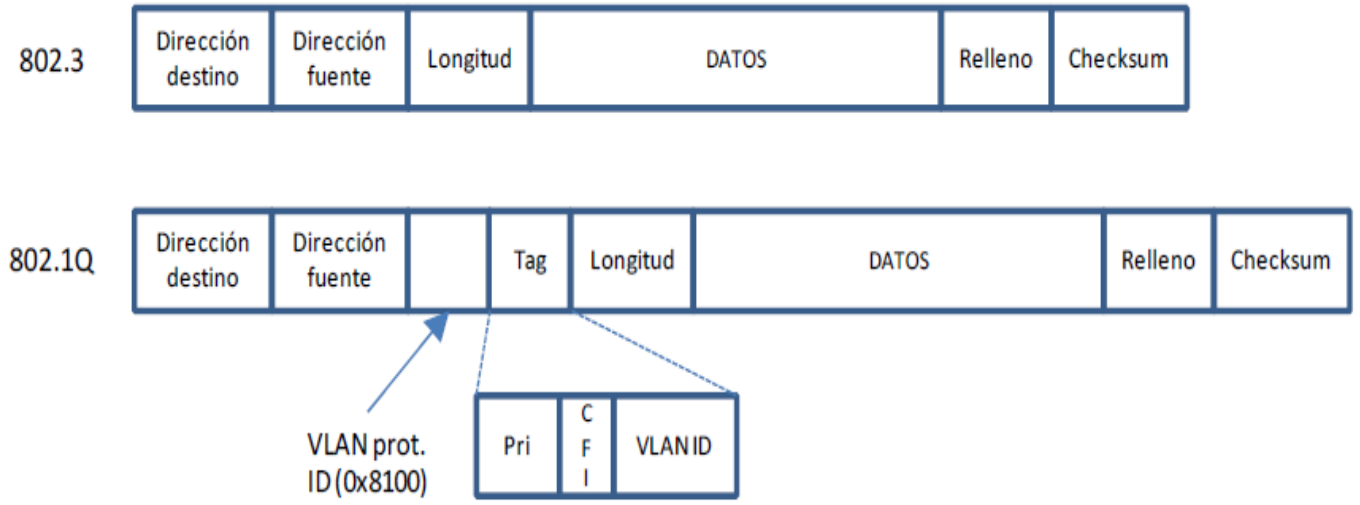
Formato de las tramas

- El protocolo 802.1Q propone añadir 4 bytes (VLAN Tag) al encabezado Ethernet original en lugar de encapsular la trama original. El valor del campo EtherType se cambia a 0x8100 para señalar el cambio en el formato de la trama.



Formato de las tramas

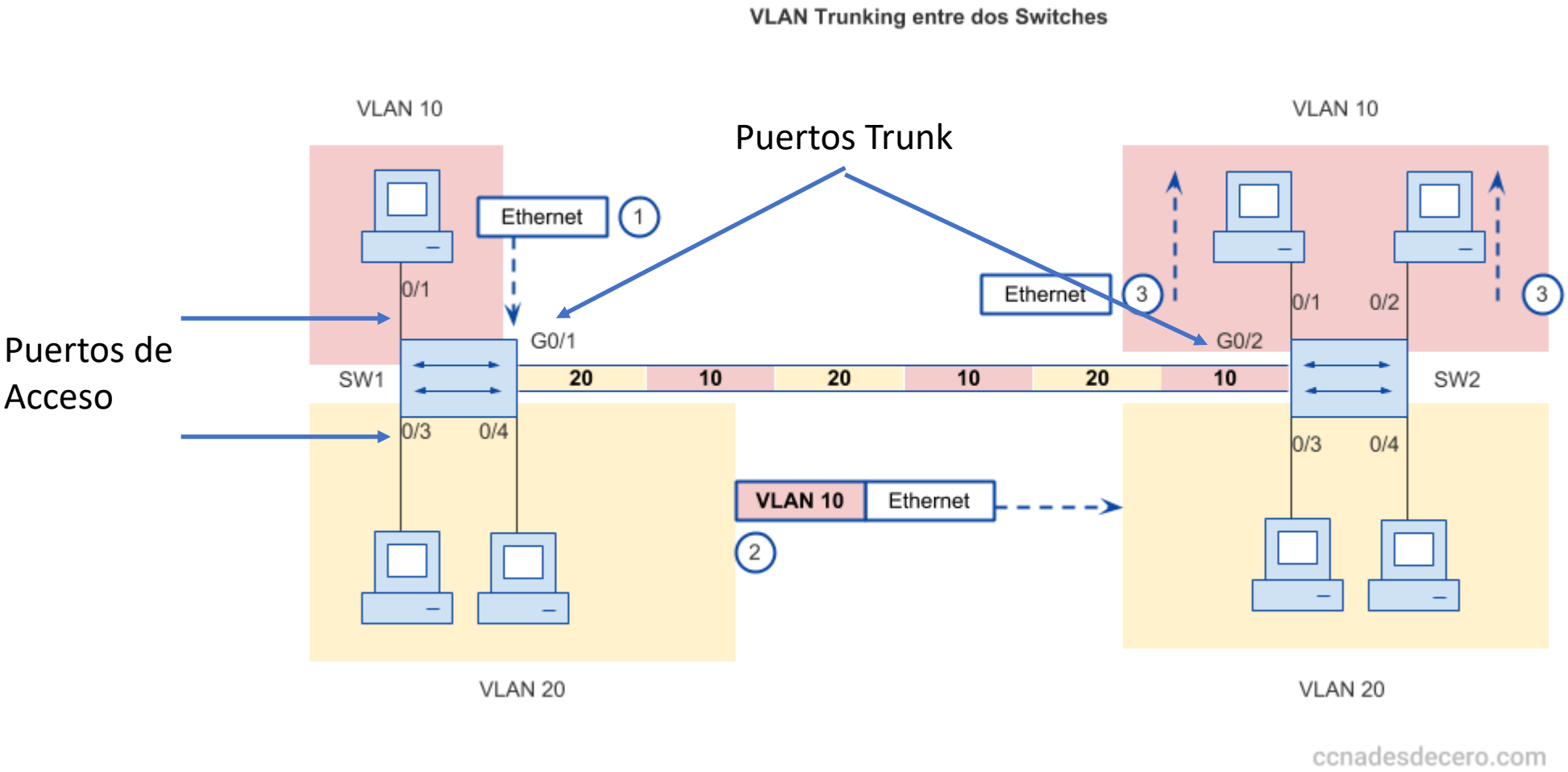
- Los primeros 2 bytes del VLAN tag consisten en el “Tag Type" (tipo de tag) de 802.1Q y siempre está puesto a 0x8100.
- Los últimos 2 bytes contienen la siguiente información:
  - Los primeros 3 bits son el campo User Priority Field que pueden ser usados para asignar un nivel de prioridad.
  - El próximo bit es el campo Canonical Format Indicator (CFI) usado para indicar la presencia de un campo Routing Information Field (RIF).
  - Los restantes 12 bits son el VLAN Identifier (VID) que identifica de forma única a la VLAN a la cual pertenece la trama Ethernet.



Tipos de Puertos en los Switches

- Puertos de acceso:
  - Se conectan los Host directamente.
  - Mapean el puerto a una VLAN programada previamente.
  - Cuando entra una trama Ethernet se le añade el TAG de 802.1Q. Cuando sale una trama 802.1Q se le quita el TAG, para que llegue a la estación correspondiente con el formato IEEE 802.3 original.
- Puertos 1Q Trunk:
  - Se utilizan para conectar Switches entre si y que pase el tráfico de diferentes VLANs a través de ellos. Las tramas que le llegan y que salen llevan el Tag 802.1Q.

Tipos de puertos, etiquetado



VLAN nativa

- Las tramas pertenecientes a las VLAN nativas no se modifican cuando se envían por medio del trunking.
- Las VLAN nativas también se conocen con el nombre de "VLAN de administración", dado que desde los computadores conectados a dichas VLANs será desde los que configuraremos los switches y podremos administrar las VLANs.
- Los fabricantes generalmente distribuyen sus equipos con la VLAN id 1 configurada como VLAN nativa, VLAN por defecto y VLAN de administración.
- Esto quiere decir que por defecto, todos los puertos del Switch pertenecen a la VLAN 1. Si un puerto lo añadimos a otra VLAN creada posteriormente, dejará por tanto de pertenecer a la VLAN de administración. Solo se puede tener una VLAN nativa por puerto.

VTP- VLAN Trunking Protocol

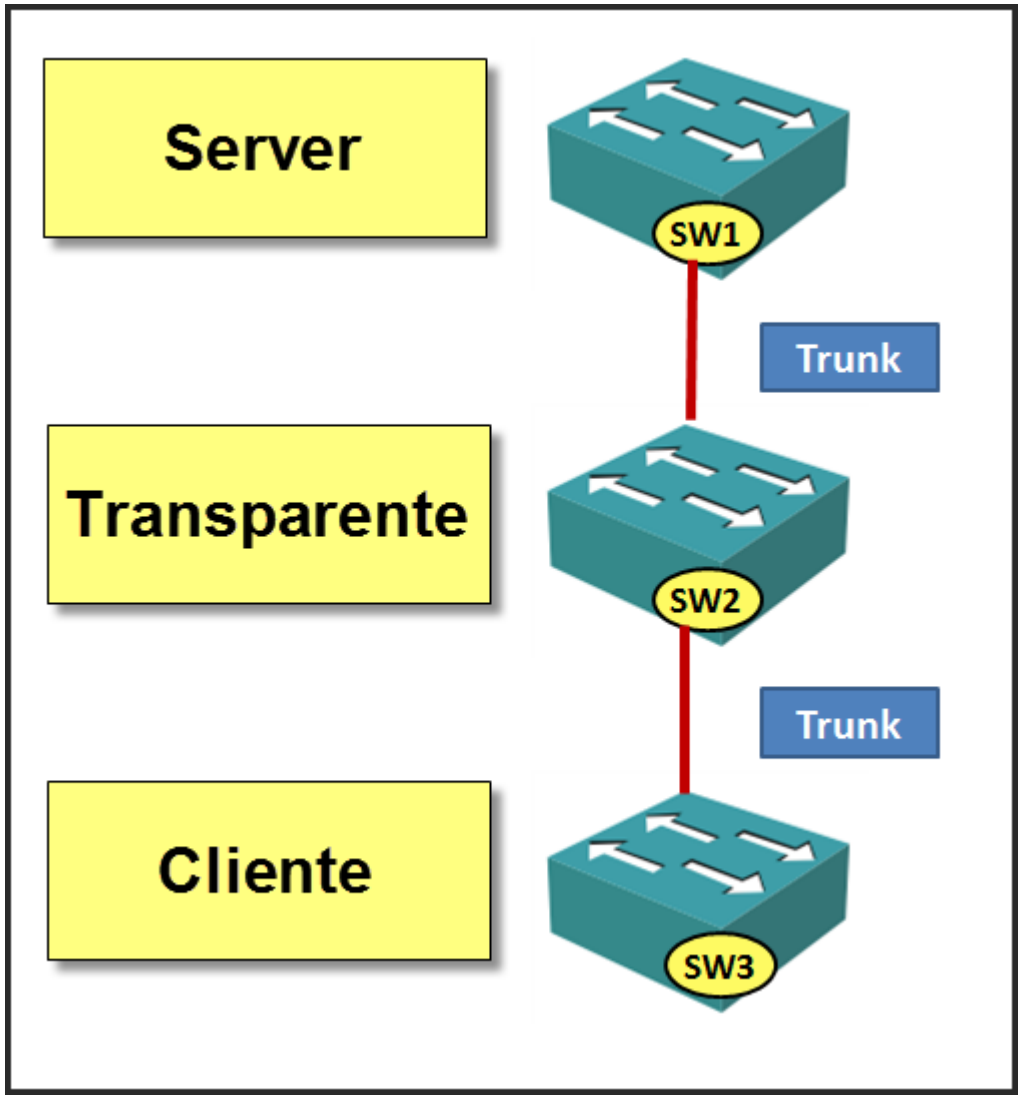
- VTP es un protocolo de mensajes de nivel 2 usado para configurar y administrar VLANs en equipos Cisco.
- Permite centralizar y simplificar la administración en un dominio de VLANs, pudiendo crear, borrar y renombrar las mismas, reduciendo así la necesidad de configurar la misma VLAN en todos los nodos.
- El protocolo VTP nace como una herramienta de administración para redes de cierto tamaño, donde la gestión manual se vuelve inabordable.

VTP- Modos de Operación

- VTP opera en 3 modos distintos:
  - Servidor
  - Cliente
  - Transparente

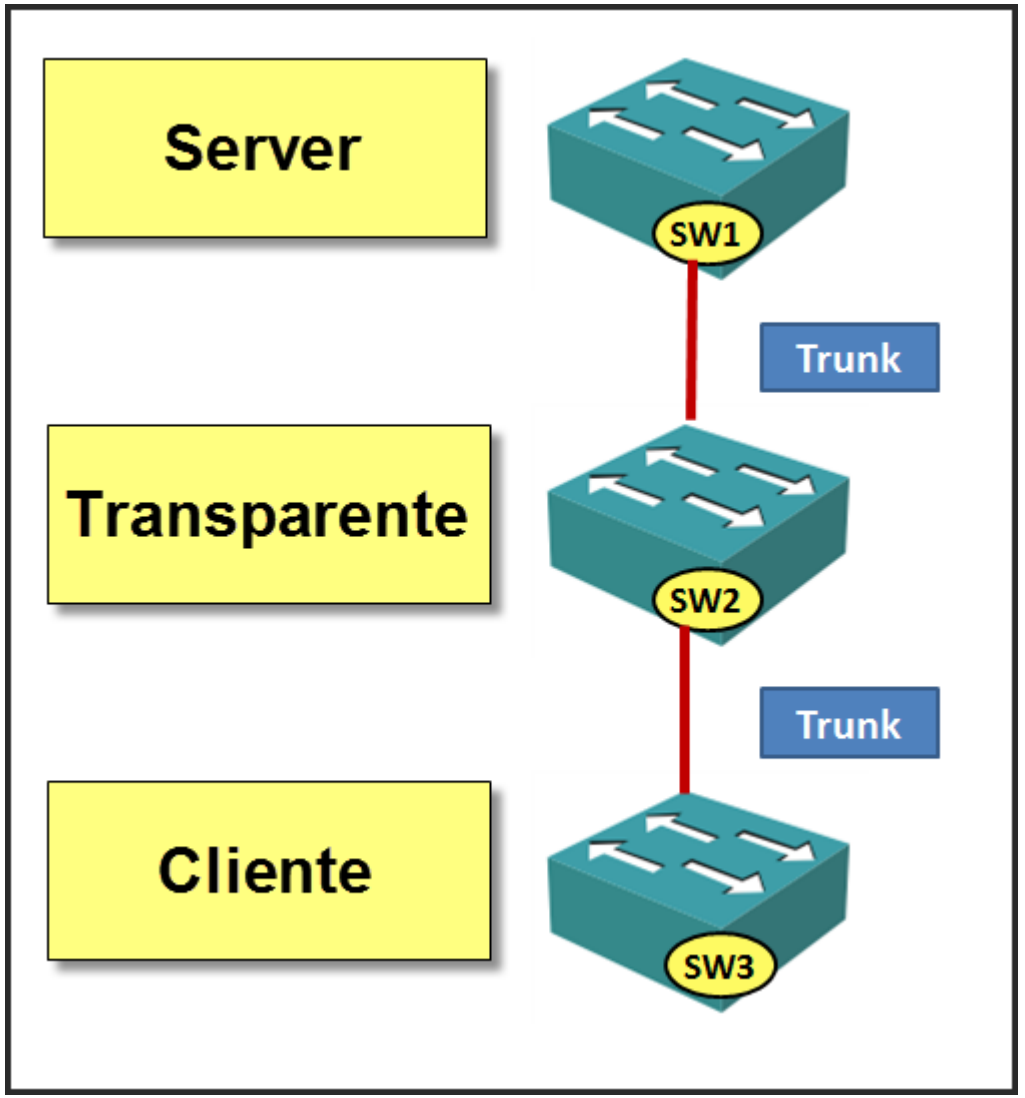
Modos de Operación de VTP

- Servidor:
  - Es el modo por defecto.
  - Desde él se pueden crear, eliminar o modificar VLANs.
  - Su cometido es anunciar su configuración al resto de switches del mismo dominio VTP y sincronizar dicha configuración con la de otros servidores, basándose en los mensajes VTP recibidos a través de sus enlaces trunk.
  - Debe haber al menos un servidor. Se recomienda autenticación MD5.



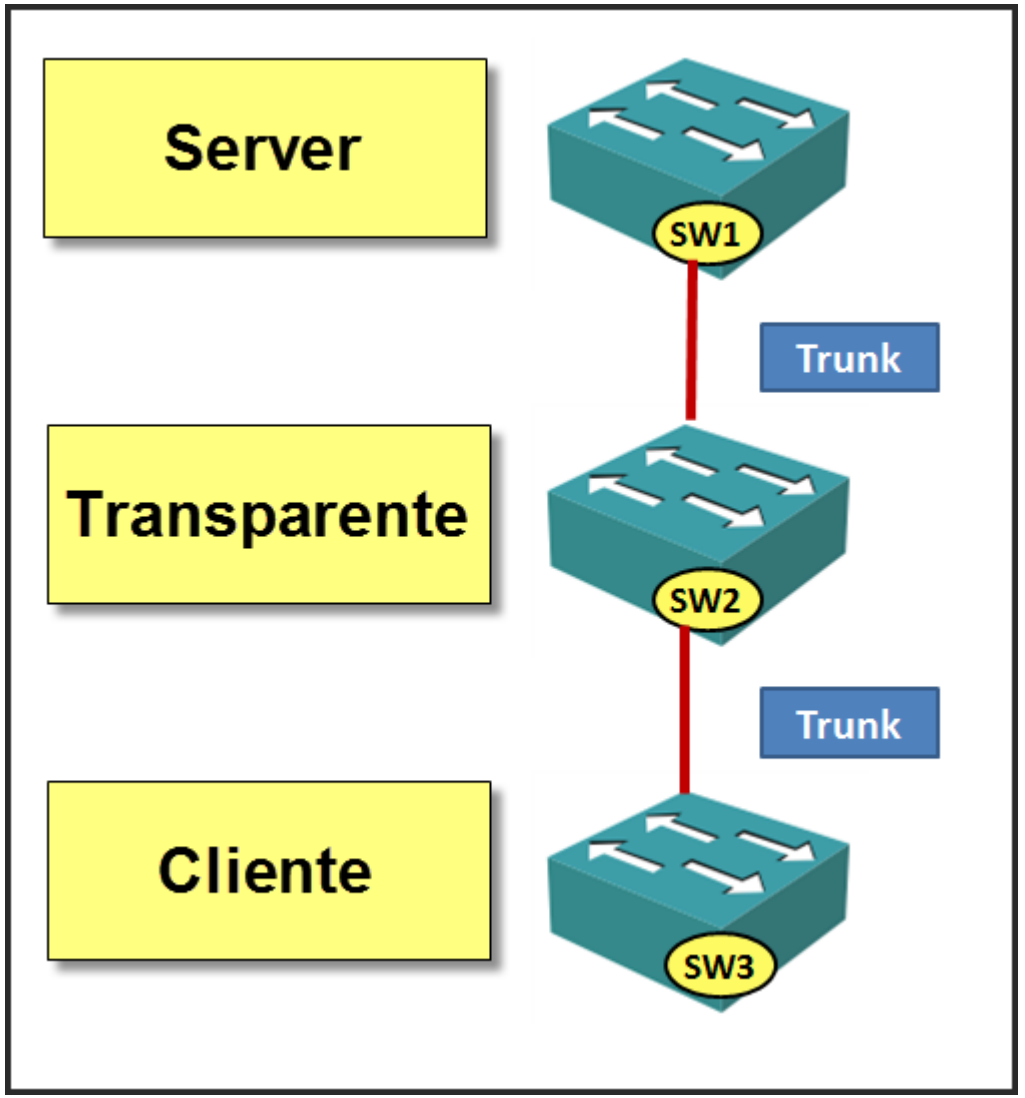
Modos de Operación de VTP

- Cliente:
  - En este modo no se pueden crear, eliminar o modificar VLANs, tan sólo sincronizar esta información basándose en los mensajes VTP recibidos de servidores en el propio dominio.
  - Un cliente VTP sólo guarda la información de la VLAN para el dominio completo mientras el switch está activado. Un reinicio del switch borra la información de la VLAN.



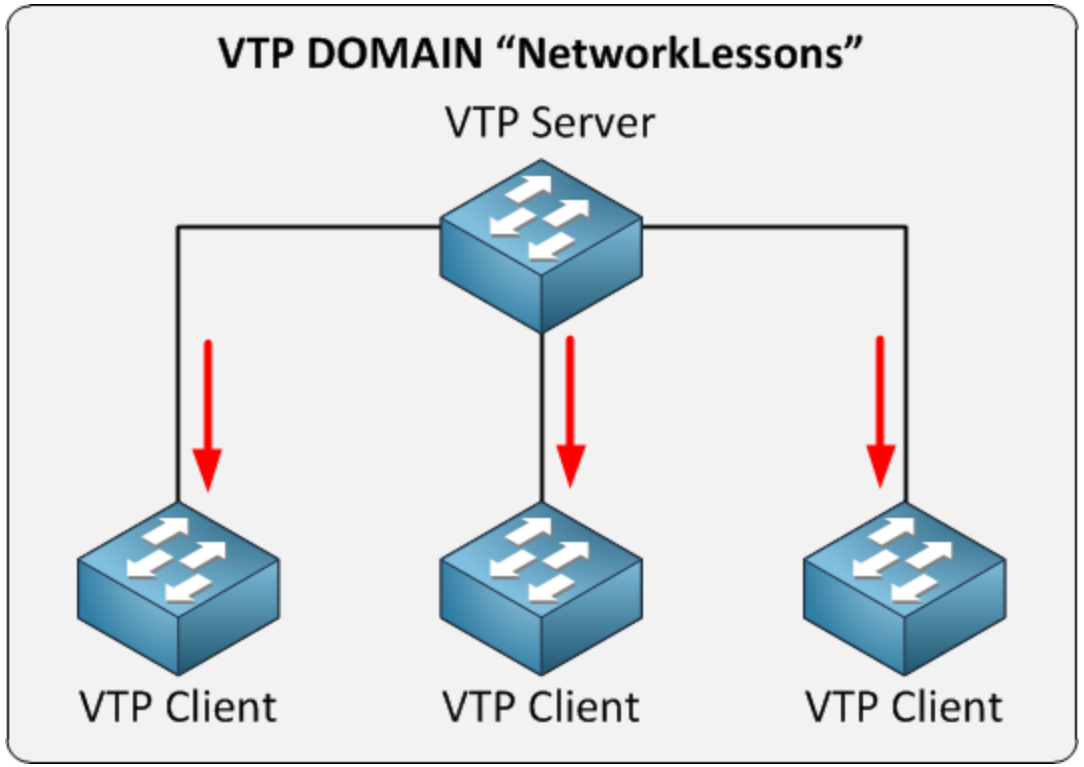
Modos de Operación de VTP

- Transparente:
  - Desde este modo tampoco se pueden crear, eliminar o modificar VLANs que afecten a los demás switches.
  - La información VLAN en los switches que trabajen en este modo sólo se puede modificar localmente.
  - Su nombre se debe a que no procesa las actualizaciones VTP recibidas, tan sólo las reenvía a los switches del mismo dominio.



Modos de Operación de VTP

- Para que dos equipos que utilizan VTP puedan compartir información sobre VLAN, es necesario que pertenezcan al mismo dominio. Los switches descartan mensajes de otro dominio VTP.



Recomendaciones

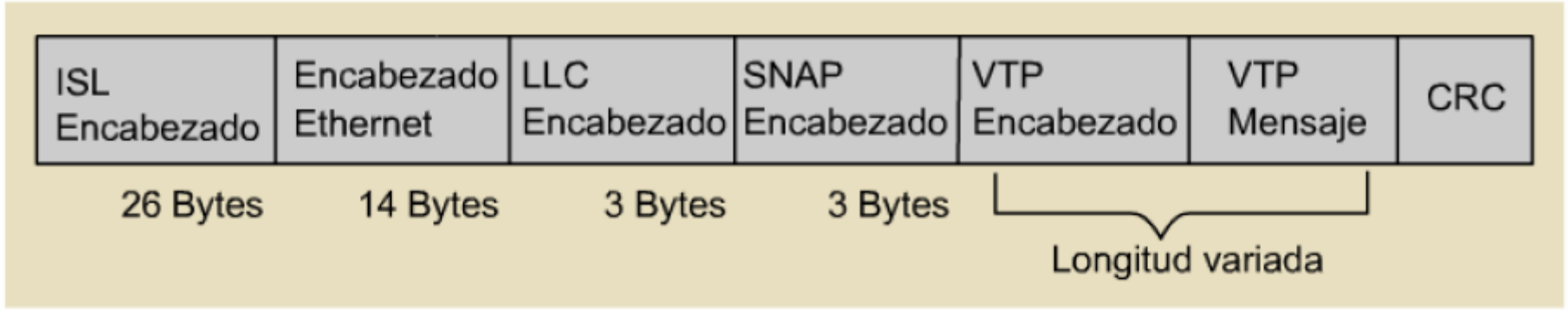
- Los administradores cambian la configuración de las VLANs en el switch que opera en modo servidor.
- Después de realizar cambios, estos son distribuidos a todos los demás dispositivos en el dominio VTP a través de los enlaces permitidos en el *trunk* (VLAN 1, por defecto), lo que minimiza los problemas causados por las configuraciones incorrectas y las inconsistencias.
- Si no se tiene VTP operando en la red, se deben cambiar las configuraciones de VLAN manualmente en cada switch!

Formato Paquetes VTP

- Los paquetes VTP se envían en las tramas de Inter-Switch Link (ISL) o en las tramas de IEEE 802.1Q (dot1q).
- Estos paquetes se envían a la dirección MAC de destino 01-00-0C-CC-CC-CC con un código de control de link lógico (LLC) de Subnetwork Access Protocol (SNAP) (AAAA) y un tipo de 2003 (en el encabezado SNAP).

Formato Paquetes VTP

- A continuación, se presenta el formato de un paquete VTP encapsulado en tramas ISL:

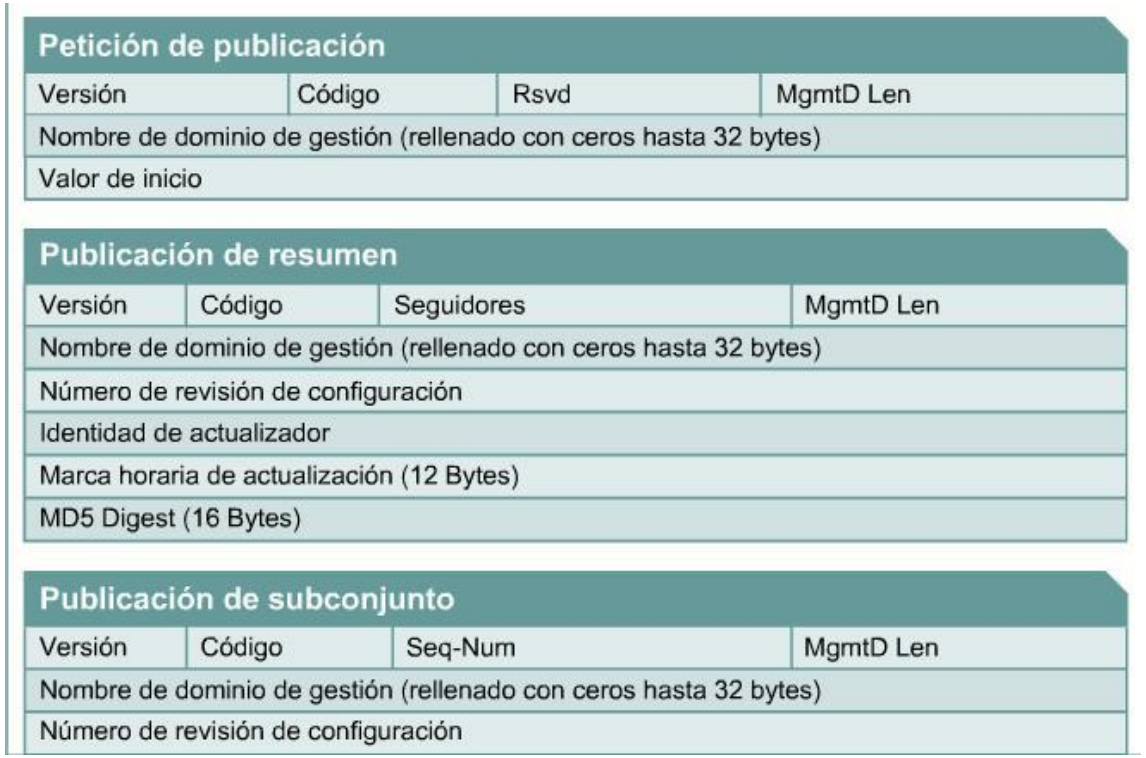


Especificaciones de trama ISL:

- El encabezado ISL tiene 26 bytes de largo.
- El CRC se calcula después de la encapsulación

Formato de un mensaje VTP

- El formato de encabezado VTP puede variar, en función del tipo de mensaje VTP. Pero, todos los paquetes VTP contienen estos campos en el encabezado:
  - Versión del protocolo VTP: 1, 2, o 3
  - Tipos de mensaje VTP: Anuncios de resumen, Anuncio de subgrupos, Solicitudes de anuncio, Mensajes de unión VTP
- Extensión del dominio de administración
- Nombre de dominio de administración



Número de Revisión de Configuración

- El número de revisión de configuración es un número de 32 bit que indica el nivel o versión de revisión para un paquete VTP.
- Cada dispositivo VTP rastrea el número de revisión de configuración VTP que se asigna a él.
- La mayor parte de los paquetes VTP contienen el número de revisión de la configuración VTP del remitente.
- ***Esta información se usa para determinar si la información recibida es más reciente que la versión actual. Cada vez que modifica la VLAN en un dispositivo VTP, la revisión de la configuración se incrementa en uno.***
- Para reiniciar la revisión de configuración en un switch, cambie el nombre del dominio VTP y después vuelva a cambiarlo e ingrese el nombre original.

Mensajes de Anuncios de Resumen

- Los switches Catalyst emiten *anuncios de resumen* en períodos de 5 minutos de forma predeterminada.
- Los Anuncios de Resumen le informan a los Catalyst adyacentes el nombre de dominio VTP actual y el número de revisión de la configuración.
- Cuando el switch recibe un paquete de anuncio de resumen sigue estos pasos:
  - El switch compara el nombre de dominio VTP con su propio nombre de dominio VTP.
  - Si el nombre es diferente, el switch simplemente ignora el paquete.
  - Si el nombre es el mismo, el switch compara la revisión de la configuración con su propia revisión:
    - Si su revisión de configuración es más alta o igual, se ignora el paquete.
    - Si es inferior, se envía una solicitud de anuncio.

Mensajes de Anuncios de subgrupos

- Cuando agrega, elimina o cambia una VLAN en un Catalyst, el servidor Catalyst aumenta la revisión de configuración donde ser realizaron los cambios y emite un anuncio de resumen, seguido de uno o varios anuncios de subconjuntos.
- Un anuncio de subconjuntos contiene una lista de información VLAN.
- Si existen varias VLAN, es posible que se requiera más de un anuncio de subgrupos para anunciar todas las VLAN.

Solicitudes de anuncio

- Un switch requiere una solicitud de anuncio de VTP en las siguientes situaciones:
  - El switch fue restablecido.
  - Se ha cambiado el Domain Name VTP.
  - El switch ha recibido un anuncio de resumen VTP con una revisión de la configuración mayor.
- Cuando se recibe una solicitud de anuncio, un dispositivo VTP envía un anuncio de resumen. Uno o varios anuncios de subgrupos siguen el anuncio de resumen.

Versiones de VTP

- VTP V2 y VTP V1 no son muy diferentes. La diferencia principal es que VTP V2 introduce el soporte para las VLAN de Token Ring. Si utiliza las VLAN de Token Ring, debe habilitar VTP V2.
- De otra manera, no hay razón para usar VTP V2.
- Cambiar la versión de VTP de 1 a 2, no hará que switch se recargue.

Versiones de VTP

- Esta descripción no trata la Versión 3 de VTP.
- La versión 3 difiere de la Versión 1 de VTP (V1) y la Versión 2 (V2) de VTP y solo está disponible en Catalyst OS (CatOS) 8.1(1) o posterior.
- La Versión 3 de VTP incorpora muchos cambios de V1 y V2 de VTP.
- Asegúrese de que comprende las diferencias entre la Versión 3 de VTP y las versiones anteriores antes de modificar su configuración de red.