Tecnológico Nacional de México

Instituto Tecnológico de Reynosa

Redes VLAN

Carrera: TICS ***Fecha:*** 29/Ago/22
Materia: Redes emergentes

Docente: Enrique Guerrero Muñiz

Equipo 4 integrantes:
19580585 Bermúdez Domínguez Juan Carlos
19580589 Castillo Jr. Gregorio
19580595 Flores Acosta Sheila Lizeth
19580867 Morales Calixto Daniel Alexander
19580603 Góngora Raga Perla Elizabeth
19580633 Pérez Romero Julio Alberto

Índice

2 Redes VLAN

¿Qué son las vlan?

Las VLAN o también conocidas como «**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.

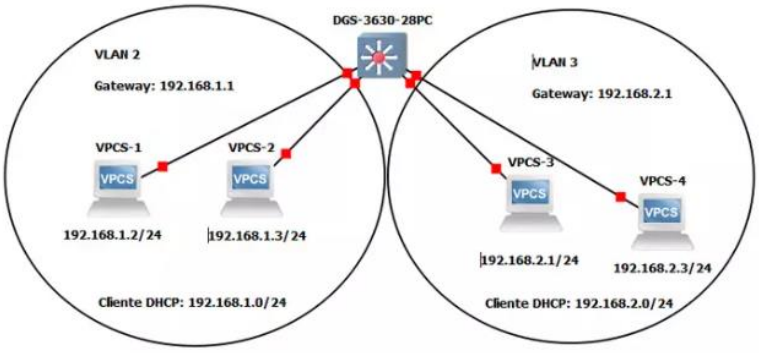
Características

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

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.

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.

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.



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.

Mejor eficiencia del personal de TI. Nos facilitarán el manejo de la red, debido a que diferentes usuarios pueden compartir una misma VLAN.

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.

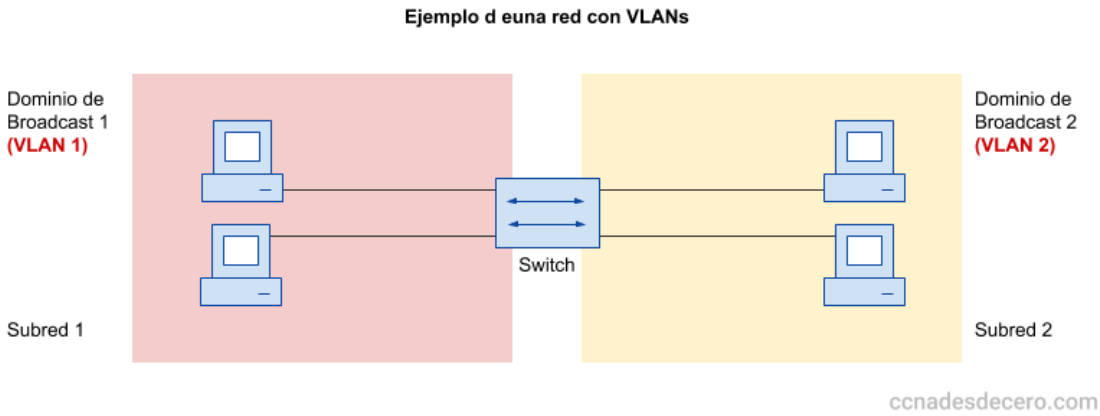
Las VLAN nos permiten **asociar lógicamente a los diferentes usuarios**, en base a etiquetas, puertos del switch, a su dirección MAC e incluso dependiendo de la autenticación que hayan realizado en el sistema. Las VLAN pueden existir en un solo switch gestionable, para asignar después a cada puerto el acceso a una determinada VLAN, pero también pueden existir en varios switches que están interconectados entre ellos

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.

Objetivo

El objetivo de usar VLAN en un entorno doméstico o profesional, es para segmentar adecuadamente la red y usar cada subred de una forma diferente, además, al segmentar por subredes usando VLANs se puede permitir o denegar el tráfico entre las diferentes VLAN gracias a un dispositivo L3 como un router o un switch multicapa L3.



- **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 mas 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.

Desventajas de las VLAN

Acabamos de ver todas las ventajas y beneficios de las VLAN, pero estas también tienen sus desventajas y limitaciones, las cuales se deben tener en cuenta a la hora de crear una. Todo esto con la intención de aprovechar mejor sus funcionalidades y rendimiento, ahorrar costes de instalación y mantenimiento posterior. Entre ellas, algunas de las más importantes son:

- **Administración compleja:** Si llegamos a tener varias VLAN, puede suponer el mismo o incluso más trabajo y coste que las redes LAN.
- **Aislamiento:** Si la red es muy grande, cabe la posibilidad de que sean necesarios varios router para poder comunicarse sin problema, por lo cual aumentaría el coste de instalación
- **Seguridad:** Si un virus llega a la red, se puede distribuir de forma relativamente sencilla por toda la red.
- **Latencia:** Este tipo de redes son más eficaces que las WAN, pero no lo son tanto como una red LAN.

¿Para que 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

2.1 Tipos de redes VLAN

Tipos de VLAN

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.

Cuando estamos usando el estándar 802.1Q y creamos las diferentes VLANs en un switch, podremos configurar los diferentes puertos como «tagged» o «untagged», es decir, con etiqueta o sin etiqueta.

- **VLAN tagged**: en las tramas Ethernet se incorpora el «tag» del VLAN ID que hayamos configurado, este tipo de VLANs son entendidas por todos los switches, por los puntos de acceso WiFi profesionales y por los routers. Se pueden configurar en modo «tagged» una o más VLANs en un determinado puerto. En los enlaces troncales (desde un router a un switch, de switch a switch y de switch a AP) se suelen configurar siempre como «tagged» para «enviarles» todas las VLANs.
- **VLAN untagged**: en las tramas Ethernet se retira el tag que hayamos configurado, este tipo de VLANs son entendidas por todos los dispositivos, pero principalmente se utilizan de cara a los equipos finales como ordenadores, portátiles, impresoras, cámaras IP y otro tipo de dispositivo. En un puerto en concreto solamente podremos configurar una VLAN como «untagged», no

podemos poner dos VLANs como «untagged» porque el equipo final no «entendería» nada.

Cuando estamos utilizando este estándar, los switches también permiten configurar los puertos físicos de diferentes formas:

- **Acceso**: son los puertos donde conectaremos los PC, impresoras, smartphones y los equipos finales, este puerto de acceso tendrá configurada una VLAN como «untagged».
- **Troncal o trunk**: lleva una o varias VLANs de un equipo a otro, por ejemplo, si queremos conectar un switch con otro switch y «pasarle» todas las VLANs o algunas de ellas, tendremos que configurarlo en modo troncal o trunk, y seleccionar las VLANs que queremos pasar como «tagged».
- **Dynamic**: dependiendo del tipo de paquete que reciba el switch, se pondrá como access o como trunk. No se recomienda configurar los puertos de un switch en modo dinámico por seguridad para evitar posibles ataques.

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. En estos casos, 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.

Cada una de estas redes de superposición, se conoce como segmento VXLAN, y se identifica mediante un identificador único de 24 bits. Este se denomina VXLAN Network Identifier (VNI). En cuanto a los dispositivos, solo pueden comunicarse entre sí si se encuentran dentro de la misma VXLAN.

Las ventajas que esta nos ofrece son:

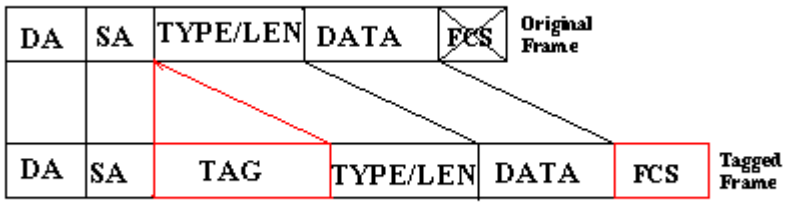
- Mayor escalabilidad en los entornos de nube virtualizados. Esto ocurre porque el ID de la VXLAN, es de 24 bits, lo cual le permite crear hasta un máximo de 16 millones de redes, las cuales estarían aisladas. Esto supera lo que de por sí proporcionan las VLAN, que cuentan con IDs de 12 bits, y permiten 4094 redes que también se encuentran aisladas.
- Mayor flexibilidad a la hora de gestionar toda la conexión.
- Facilita la opción de dar uso de **funciones de capa 3** en las redes subyacentes.
- La red virtual que se encuentra en la **capa 2, se abstrae** de toda la red subyacente en formato físico. Esto da como resultado que la red virtual no será visible para la red física, lo cual a su vez proporciona algunos beneficios como por ejemplo, eliminar las necesidades de contar con una infraestructura física añadida, y reducen la duplicación de direcciones MC en las VM que se encuentran en el mismo segmento de la VSLAN.

2.2 Protocolos de enlace VLAN

IEEE 802.1Q

Inicialmente creado para desarrolla un mecanismo que permita a múltiples redes interconectadas con puentes o switches para compartir transparentemente el mismo medio físico sin problemas de interferencia entre las redes que comparten el medio

Actualmente se usa para definir el protocolo de encapsulamiento usado para implementar este mecanismo en redes ethernet y también 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.

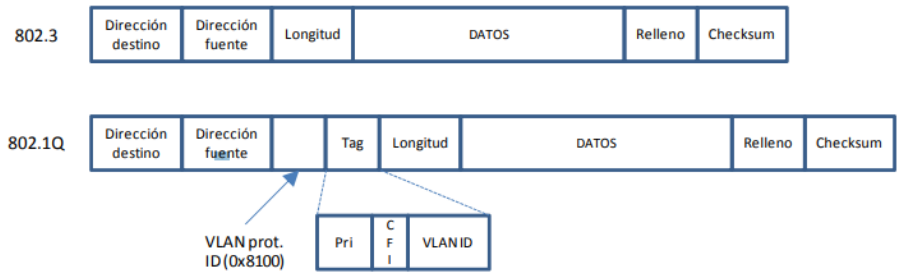


Características

- Se encarga del etiquetado de las tramas que es asociada inmediatamente con la información de la VLAN
- Es el más común para el etiquetado de las VLANs
- Se caracteriza por un formato de trama similar a 802.3(Ethernet)
- Este protocolo es un estándar internacional y por lo dicho anteriormente es compatible con bridges y switches sin capacidad de VLAN

Formato de forma

El protocolo 802.1Q propone añadir 4 bytes 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.



Como se puede apreciar en la Figura 1, la VLAN tag se inserta en la trama Ethernet entre el campo “Dirección fuente” y “Longitud. 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.

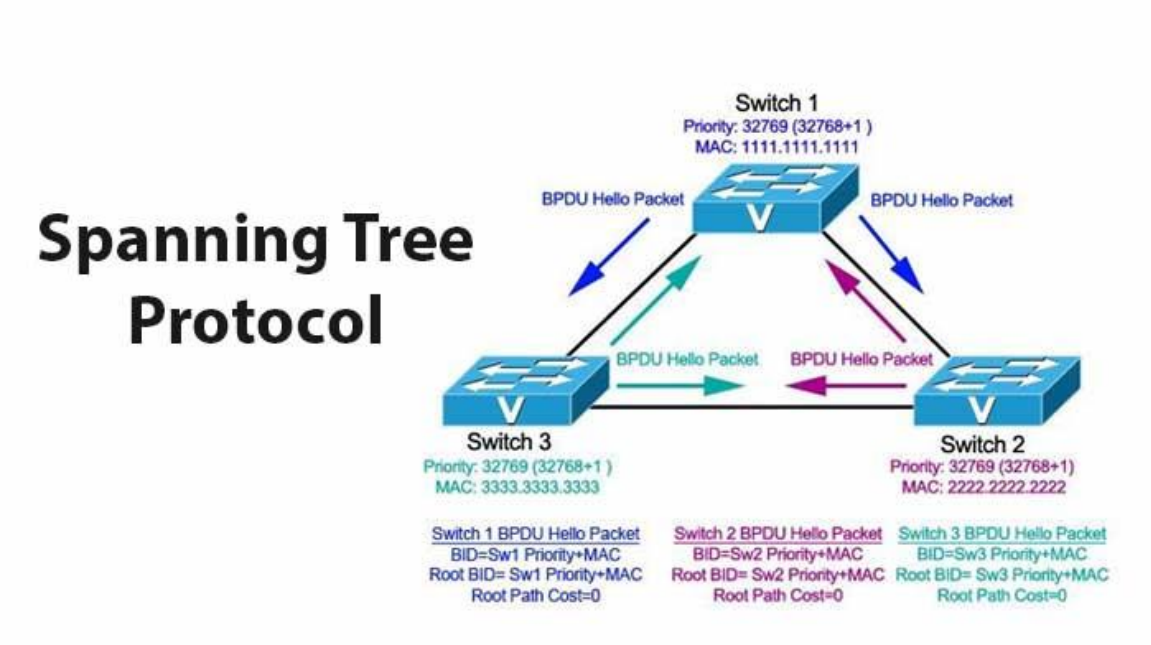
STP (Spanning tree protocol): Evita la aparición de bucles lógicos para que haya un solo camino entre dos nodos

El STP, definido por el estándar IEEE 802.1d es un protocolo que funciona en el **nivel de la capa 2** del modelo OSI y su principal objetivo es controlar los enlaces redundantes, asegurando el rendimiento de una red.

Como ya se sabe, los switches no filtran los broadcasts y tal situación hace que todos los broadcasts recibidos a una interfaz de un switch sean enviados por otras interfaces, excepto por la interfaz que se ha recibido (flooding), creándose así una tormenta de difusión.

Funcionamiento del STP

El protocolo STP elimina lógicamente caminos de comunicación. Para ello el este crea un árbol de switches presentes en la red y elige el switch de referencia, a partir del cual se creará el árbol.



Bajo el protocolo STP, este switch se llama **root bridge**. La elección del root bridge es hecha con base en una prioridad y también con base en la dirección MAC. En una red sólo puede haber un root bridge.

En términos de configuración el STP es un protocolo relativamente simple pero en la teoría hay algunos conceptos que son necesarios aprender bien. En un próximo tutorial seguiré hablando de algunos protocolos bastante usados en esta área.

VTP

VTP (VLAN Trunking Protocol): Protocolo propietario de Cisco que permita una gestión centralizada de todas las VLANs.

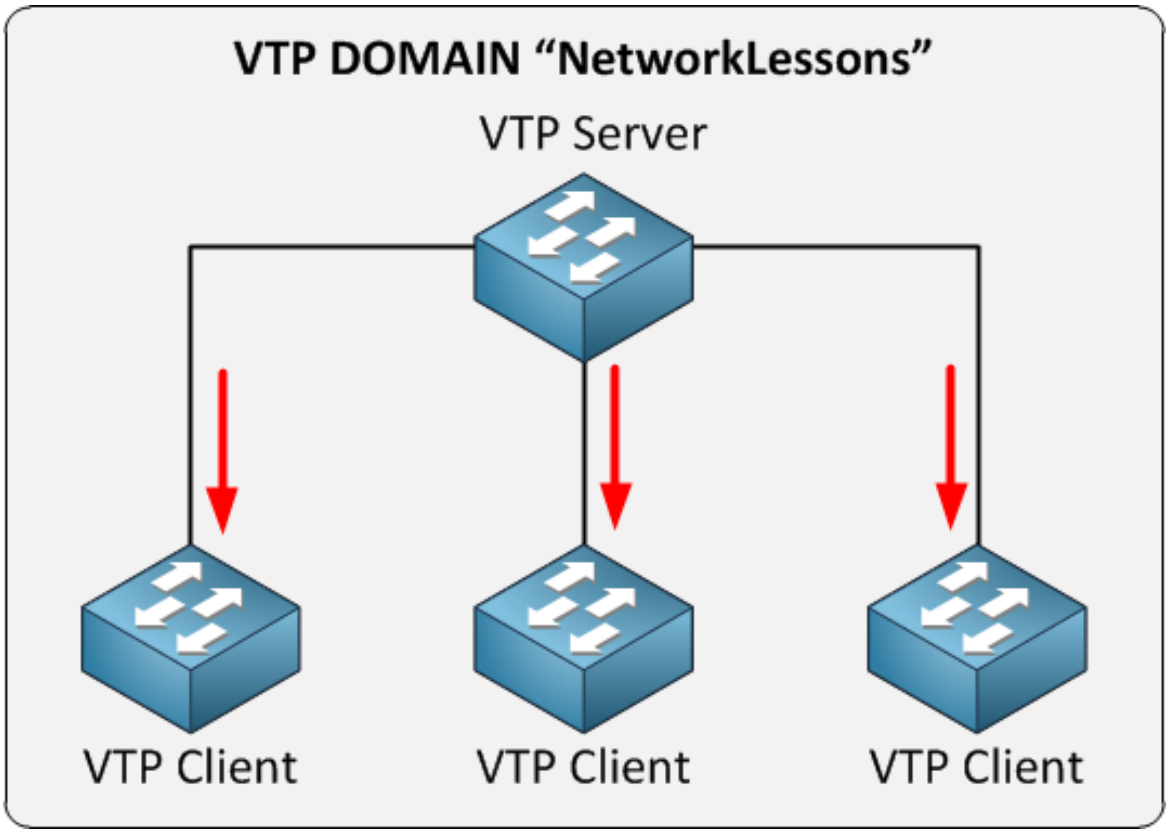
Este protocolo reduce la administración en una red de switch. Al configurar una VLAN nueva en un servidor VTP, se distribuye la VLAN a través de todos los switches del dominio. Esto reduce la necesidad de configurar la misma VLAN en todas partes. VTP es un protocolo de propiedad de Cisco que está disponible en la mayoría de los productos de la serie Cisco Catalyst.

Este permite centralizar y simplificar la administración en un dominio de Vlans, pudiendo crear, borrar y renombrar las mismas, reduciendo asu la misma VLAN en todos los nodos

El protocolo VTP nace como una herramienta para redes de asministracion para redes de cierto tamaño, donde la gestión manual se vuelve inabordable.

VTP opera en 3 modos distintos

- Servidor
- Cliente
- transparente



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.

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.

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.

2.3 Enrutamiento inter VLAN

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.

El enrutamiento entre vlans o inter vlan routing, resulta necesario una vez que se posee una infraestructura de red con vlan implementadas, debido a que los usuarios necesitaran intercambiar información de una red a otra.

Es importante recordar que cada VLAN es un dominio de broadcast único. Por lo tanto, de manera predeterminada, las computadoras en VLAN separadas no pueden comunicarse.

Existe una manera para permitir que estas estaciones finales puedan comunicarse; esta manera se llama enrutamiento entre vlan (Inter vlan routing).

El enrutamiento entre VLAN es un proceso que permite reenviar el tráfico de la red desde una VLAN a otra mediante un enrutador. Las VLAN están asociadas a subredes IP únicas en la red. Esta configuración de subred facilita el proceso de enrutamiento en un entorno de múltiples VLAN.

Tradicionalmente, el enrutamiento de la LAN utiliza enrutadores con interfaces físicas múltiples. Es necesario conectar cada interfaz a una red separada y configurarla para una subred diferente.

En una red tradicional que utiliza múltiples VLAN para segmentar el tráfico de la red en dominios de broadcast lógicos, el enrutamiento se realiza mediante la conexión de diferentes interfaces físicas del enrutador a diferentes puertos físicos del switch. Los puertos del switch conectan al enrutador en modo de acceso; en este modo,

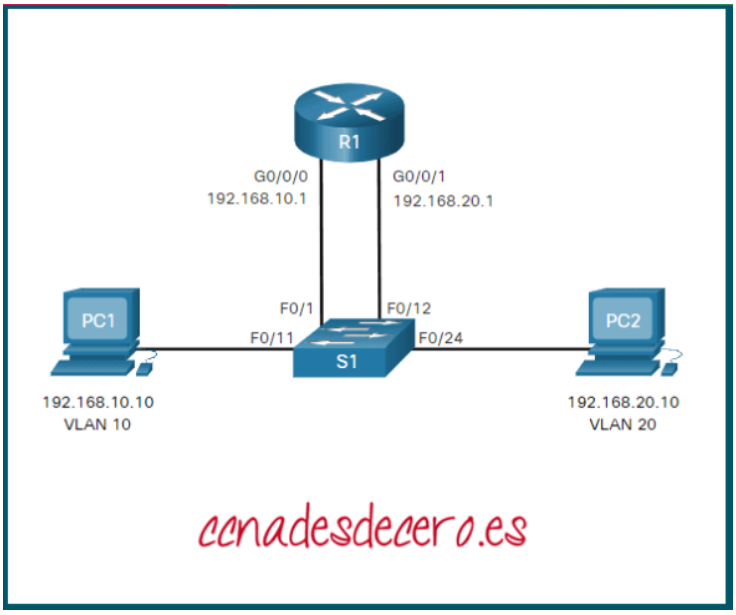
diferentes VLAN estáticas se asignan a cada interfaz del puerto. Cada interfaz del switch estaría asignada a una VLAN estática diferente. Cada interfaz del enrutador puede entonces aceptar el tráfico desde la VLAN asociada a la interfaz del switch que se encuentra conectada y el tráfico puede enrutarse a otras VLAN conectadas a otras interfaces.

El enrutamiento entre VLAN tradicional requiere de interfaces físicas múltiples en el enrutador y en el switch. Sin embargo, no todas las configuraciones del enrutamiento entre VLAN requieren de interfaces físicas múltiples.

1. Enrutamiento Inter-VLAN 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.

Por ejemplo, consulta la topología donde R1 tiene dos interfaces conectadas al switch S1.



Nota en la tabla de direcciones MAC de ejemplo de S1 se rellena de la siguiente manera:

- El puerto Fa0/1 está asignado a la VLAN 10 y está conectado a la interfaz R1 G0/0/0.
- El puerto Fa0/11 está asignado a la VLAN 10 y está conectado a PC1.
- El puerto Fa0/12 está asignado a la VLAN 20 y está conectado a la interfaz R1 G0/0/1.
- El puerto Fa0/11 está asignado a la VLAN 20 y está conectado a PC2.

Tabla de direcciones MAC para S1		
Puerto	Dirección MAC	VLAN
F0/1	R1 G0/0/0 MAC	10
F0/11	PC1 MAC	10
F0/12	R1 G0/0/1 MAC	20

Cuando PC1 envía un paquete a PC2 en otra red, lo reenvía a su puerta de enlace predeterminada 192.168.10.1. R1 recibe el paquete en su interfaz G0/0/0 y examina la dirección de destino del paquete. R1 luego enruta el paquete hacia fuera de su interfaz G0/0/1 al puerto F0/12 en la VLAN 20 en S1. Finalmente, S1 reenvía la trama a PC2.

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.

En nuestro ejemplo, R1 requería dos interfaces Ethernet separadas para enrutar entre la VLAN 10 y la VLAN 20. ¿Qué ocurre si hubiera seis (o más) VLAN para interconectar? Se necesitaría una interfaz separada para cada VLAN. Obviamente, esta solución no es escalable.

2. Enrutamiento Inter-VLAN Router-on-a-Stick

El método de enrutamiento inter-VLAN ‘router-on-a-stick’ supera la limitación del método de enrutamiento inter-VLAN heredado. Solo requiere una interfaz Ethernet física para enrutar el tráfico entre varias VLAN de una red.

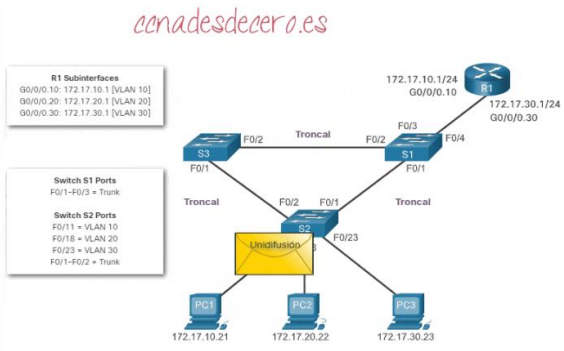
Es un tipo de configuración de router en la cual una interfaz física única enruta el tráfico entre múltiples VLAN en una red.

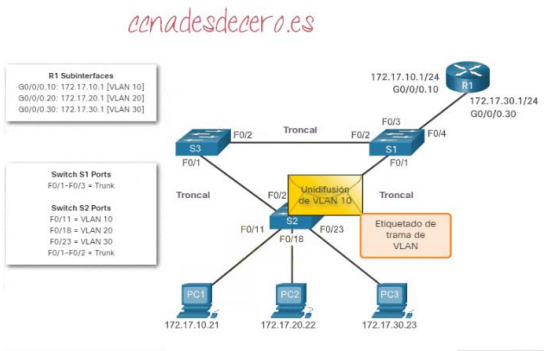
El router realiza el enrutamiento inter VLAN al aceptar el tráfico proveniente del switch adyacente y reenvía el tráfico enrutado de la VLAN etiquetada para la VLAN destino, por la misma interfaz física.

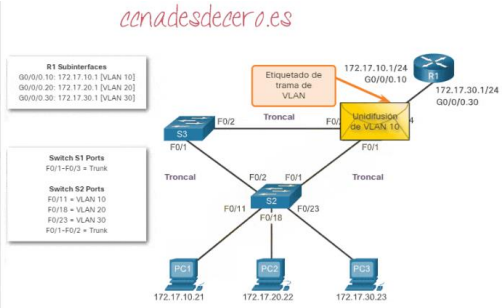
El router realiza el enrutamiento al conectar cada una de sus interfaces físicas a una VLAN única.

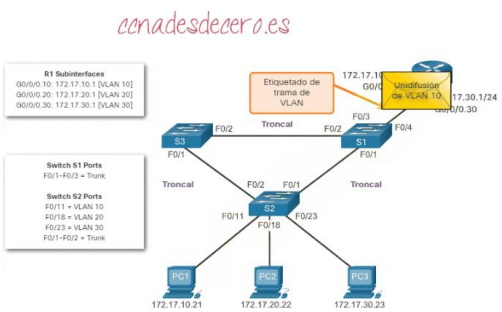
Para este tipo de enrutamiento, se hace uso de subinterfaces, que son interfaces virtuales virtuales múltiples, asociadas a una interfaz física. Cada subinterfaz se configura con su propia dirección IP, máscada de subred y asignación de VLAN única.

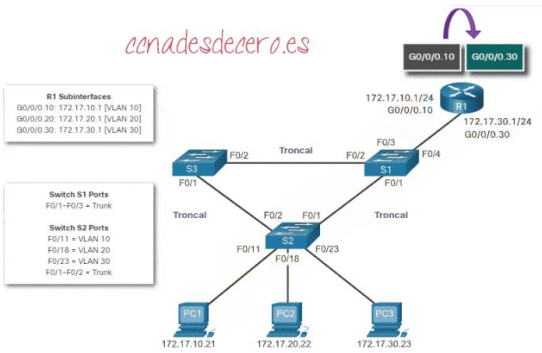
Las subinterfaces configuradas son interfaces virtuales basadas en software. Cada uno está asociado a una única interfaz Ethernet física. Estas subinterfaces se configuran en el software del router. Cada una se configura de forma independiente con sus propias direcciones IP y una asignación de VLAN.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

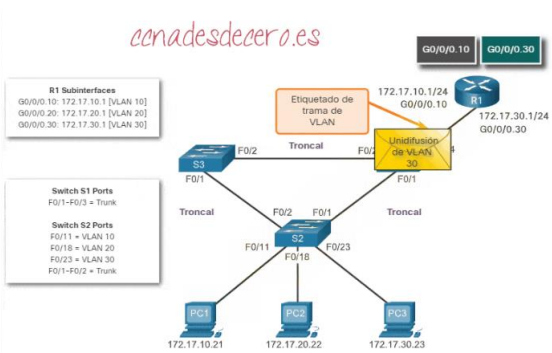


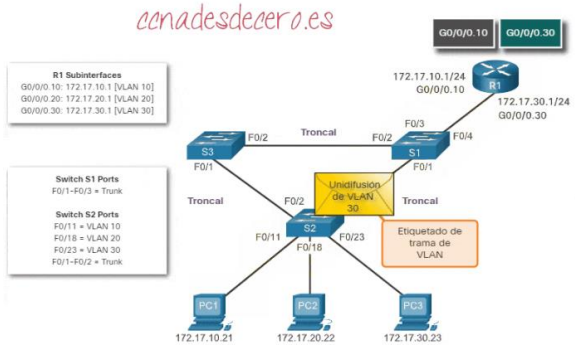


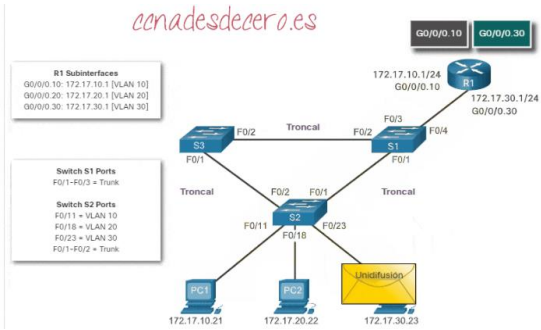


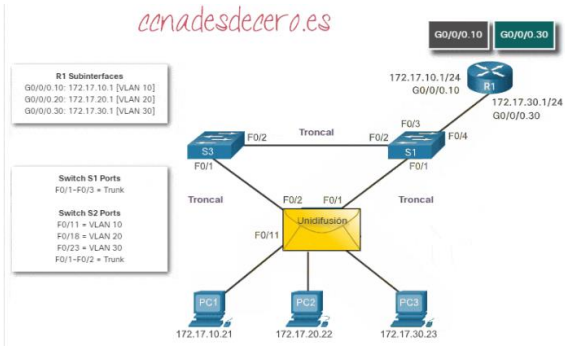


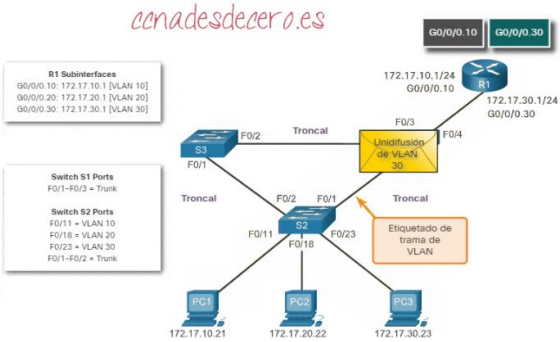

ccnadesdecero.es
G0/0/0.10
G0/0/0.30
R1 Subinterfaces
G0/0/0.10: 172.17.10.1 [VLAN 10]
G0/0/0.20: 172.17.20.1 [VAN 20]
G0/0/0.30: 172.17.30.1 [VLAN 30]
172.17.10.1/24
G0/0/0.10
172.17.30.1/24
G0/0/0.30
R1
S3
S1
S2
F0/1
F0/2
F0/3
F0/4
F0/11
F0/18
F0/23
Troncal
Switch S1 Ports
F0/1-F0/3 = Trunk
Switch S2 Ports
F0/11 = VLAN 10
F0/18 = VLAN 20
F0/23 = VLAN 30
F0/1-F0/2 = Trunk
PC1
PC2
PC3
172.17.10.21
172.17.20.22
172.17.30.23

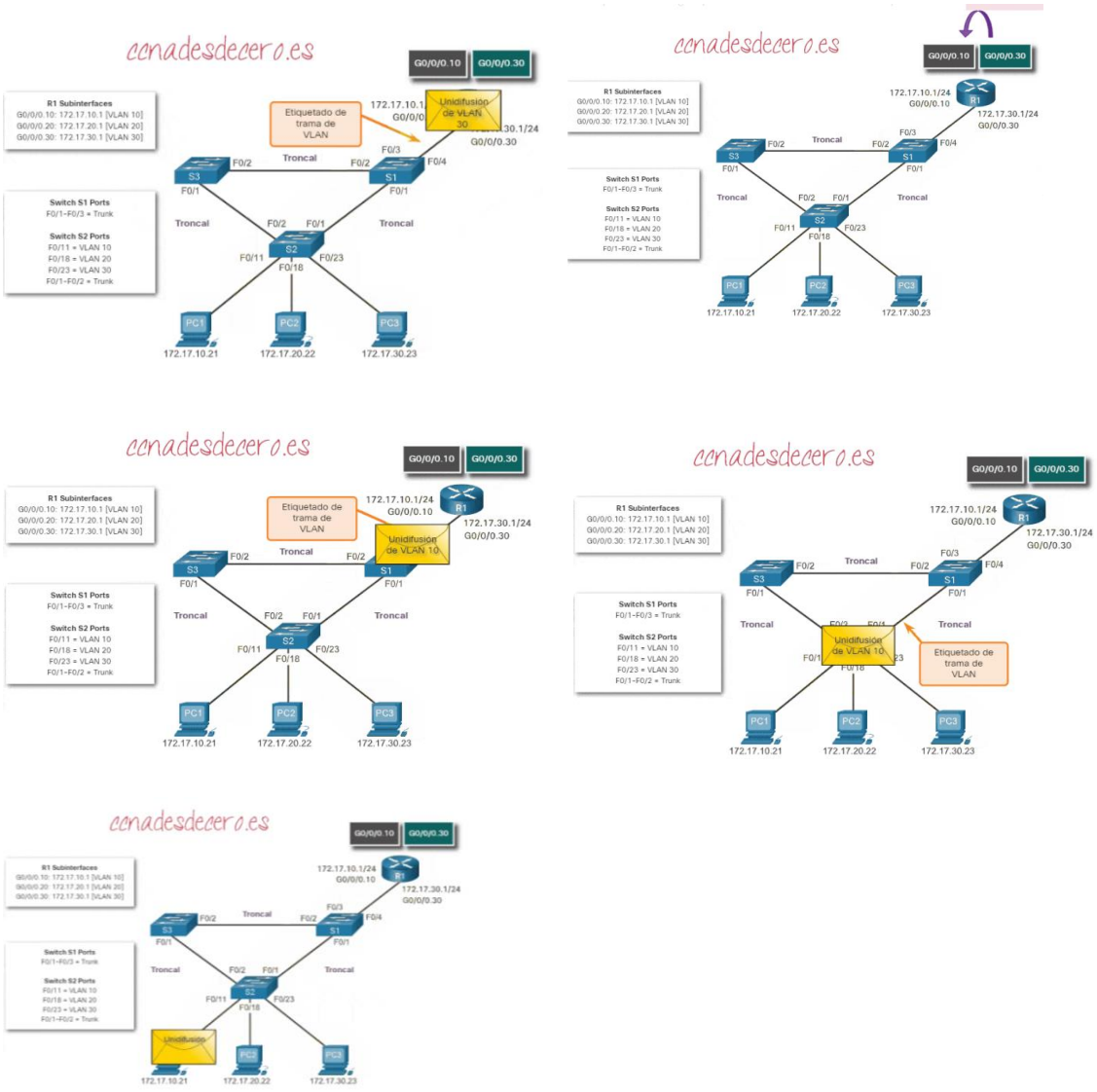

ccnadesdecero.es
G0/0/0.10
G0/0/0.30
R1 Subinterfaces
G0/0/0.10: 172.17.10.1 [VLAN 10]
G0/0/0.20: 172.17.20.1 [VLAN 20]
G0/0/0.30: 172.17.30.1 [VLAN 30]
Etiquetado de trama de VLAN
Unidifusión de VLAN 30
172.17.10.1/24
G0/0/0.10
172.17.30.1/24
G0/0/0.30
R1
S3
S2
F0/1
F0/2
F0/11
F0/18
F0/23
Troncal
Switch S1 Ports
F0/1-F0/3 = Trunk
Switch S2 Ports
F0/11 = VLAN 10
F0/18 = VLAN 20
F0/23 = VLAN 30
F0/1-F0/2 = Trunk
PC1
PC2
PC3
172.17.10.21
172.17.20.22
172.17.30.23


ccnadesdecero.es
G0/0/0.10
G0/0/0.30
R1 Subinterfaces
G0/0/0.10: 172.17.10.1 [VLAN 10]
G0/0/0.20: 172.17.20.1 [VLAN 20]
G0/0/0.30: 172.17.30.1 [VLAN 30]
172.17.10.1/24
G0/0/0.10
172.17.30.1/24
G0/0/0.30
R1
S3
S1
S2
F0/1
F0/2
F0/3
F0/4
F0/11
F0/18
F0/23
Troncal
Unidifusión de VLAN 30
Etiquetado de trama de VLAN
Switch S1 Ports
F0/1-F0/3 = Trunk
Switch S2 Ports
F0/11 = VLAN 10
F0/18 = VLAN 20
F0/23 = VLAN 30
F0/1-F0/2 = Trunk
PC1
PC2
PC3
172.17.10.21
172.17.20.22
172.17.30.23


ccnadesdecero.es
G0/0/0.10
G0/0/0.30
R1 Subinterfaces
G0/0/0.10: 172.17.10.1 [VLAN 10]
G0/0/0.20: 172.17.20.1 [VLAN 20]
G0/0/0.30: 172.17.30.1 [VLAN 30]
172.17.10.1/24
G0/0/0.10
172.17.30.1/24
G0/0/0.30
R1
S3
S1
S2
F0/1
F0/2
F0/3
F0/4
F0/11
F0/18
F0/23
Troncal
Switch S1 Ports
F0/1-F0/3 = Trunk
Switch S2 Ports
F0/11 = VLAN 10
F0/18 = VLAN 20
F0/23 = VLAN 30
F0/1-F0/2 = Trunk
Unidifusión
PC1
PC2
PC3
172.17.10.21
172.17.20.22
172.17.30.23


ccnadesdecero.es
G0/0/0.10
G0/0/0.30
R1 Subinterfaces
G0/0/0.10: 172.17.10.1 [VLAN 10]
G0/0/0.20: 172.17.20.1 [VLAN 20]
G0/0/0.30: 172.17.30.1 [VLAN 30]
172.17.10.1/24
G0/0/0.10
172.17.30.1/24
G0/0/0.30
R1
S3
S1
S2
F0/1
F0/2
F0/3
F0/4
F0/11
F0/18
F0/23
Troncal
Unidifusión
Switch S1 Ports
F0/1-F0/3 = Trunk
Switch S2 Ports
F0/11 = VLAN 10
F0/18 = VLAN 20
F0/23 = VLAN 30
F0/1-F0/2 = Trunk
PC1
PC2
PC3
172.17.10.21
172.17.20.22
172.17.30.23

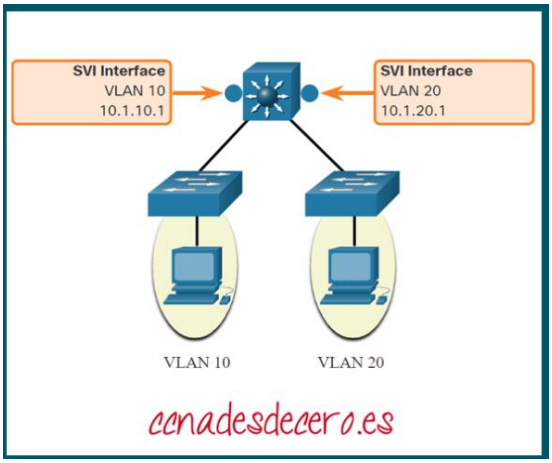

ccnadesdecero.es
G0/0/0.10
G0/0/0.30
R1 Subinterfaces
G0/0/0.10: 172.17.10.1 [VLAN 10]
G0/0/0.20: 172.17.20.1 [VLAN 20]
G0/0/0.30: 172.17.30.1 [VLAN 30]
172.17.10.1/24
G0/0/0.10
172.17.30.1/24
G0/0/0.30
R1
S3
S2
F0/1
F0/2
F0/3
F0/4
F0/11
F0/18
F0/23
Troncal
Unidifusión de VLAN 30
Etiquetado de trama de VLAN
Switch S1 Ports
F0/1-F0/3 = Trunk
Switch S2 Ports
F0/11 = VLAN 10
F0/18 = VLAN 20
F0/23 = VLAN 30
F0/1-F0/2 = Trunk
PC1
PC2
PC3
172.17.10.21
172.17.20.22
172.17.30.23



Como se ve en la animación, PC1 en la VLAN 10 se comunica con PC3 en la VLAN 30. El router R1 acepta el tráfico de unidifusión etiquetado en la VLAN 10 y lo enruta a la VLAN 30 mediante sus subinterfaces configuradas. El switch S2 elimina la etiqueta de la VLAN de la trama de unidifusión y reenvía la trama a PC3 en el puerto F0/23.

3. Enrutamiento Inter-VLAN en 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.

A continuación se presentan las 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 los switches de capa 3 son más caros.

DIFERENCIAS

MÉTODO ANTIGUO	ROUTER-ON-STICK	SWITCH CAPA 3
Una interfaz por VLAN	Una interfaz física para muchas VLAN	Se minimizan fallas al reducir de dos a un solo equipo
No existe contención de ancho de banda	Contención de ancho de banda	El proceso de enrutamiento es más rápido, ya que solo revisa una tabla.
Conectado para acceder al modo puerto de switch	Conectado para establecer el enlace troncal en el modo puerto de switch	La seguridad de la red se ve mejorada
Más costoso	Menos costoso que el método antiguo	Menos costoso que los otros métodos
Configuración de la conexión más compleja	Configuración de la conexión menos compleja	

2.4 Resolución de problema VLAN

Una de las tareas frecuentes de los administradores de red es resolver problemas de formación de enlaces troncales o de enlaces que se comportan incorrectamente como enlaces troncales. En ocasiones, un puerto de switch se puede comportar como puerto de enlace troncal, incluso si no se configuró como tal. Por ejemplo, un puerto de acceso puede aceptar tramas de redes VLAN distintas de la VLAN a la cual se asignó. Esto se conoce como “filtración de VLAN”.

Se muestra un diagrama de flujo de las pautas generales de resolución de problemas de enlaces troncales.

Para resolver problemas de enlaces troncales que no se forman o de filtración de VLAN, proceda de la siguiente manera:

Paso 1: Utilice el comando **show interfaces trunk** para verificar si hay coincidencia entre la VLAN nativa local y peer. Si la VLAN nativa no coincide en ambos extremos, hay una filtración de VLAN.

Paso 2: Utilice el comando **show interfaces trunk** para verificar si se estableció un enlace troncal entre los switches. Configure estáticamente los enlaces troncales siempre que sea posible. Los puertos de los switches Cisco Catalyst utilizan DTP de manera predeterminada e intentan negociar un enlace troncal.

Para mostrar el estado del enlace troncal, la VLAN nativa utilizada en ese enlace troncal y verificar el establecimiento del enlace troncal, utilice el comando show interfaces trunk. En el ejemplo de la figura 2, se muestra que la VLAN nativa en un extremo del enlace troncal se cambió a la VLAN 2. Si un extremo del enlace troncal se configura como VLAN 99 nativa y el otro extremo como VLAN 2 nativa, las tramas que se envían desde la VLAN 99 en un extremo se reciben en la VLAN 2 en el otro extremo. La VLAN 99 se filtra en el segmento VLAN 2.

CDP muestra un aviso de incompatibilidad de VLAN nativa en un enlace troncal con este mensaje:

*Mar 1 06:45:26.232: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/1 (2), with S2 FastEthernet0/1 (99).

Si existe una incompatibilidad de VLAN nativa, se producen problemas de conectividad en la red. El tráfico de datos para las VLAN distintas de las dos VLAN nativas configuradas se propaga correctamente a través del enlace troncal, pero los datos relacionados con cualquiera de las VLAN nativas no se propagan correctamente a través del enlace troncal.

Como se muestra en la figura 2, los problemas de incompatibilidad de la VLAN nativa no impiden que se forme el enlace troncal. Para resolver una incompatibilidad de VLAN nativa, configure la VLAN nativa para que sea la misma VLAN en ambos lados del enlace.

2.5 Seguridad en VLAN

Todo buen administrador de redes sabe que seguramente el próximo ataque a sus sistemas provenga de su red. Por malicia o desconocimiento, los usuarios que se encuentran del lado interno tienen mucho más poder destructivo que los externos y eso es así gracias a los administradores confiados.

La red puede ser una de las partes más vulnerables de un sistema. La red de máquinas virtuales necesita tanta protección como una red física. La utilización de VLAN puede mejorar la seguridad de las redes del entorno.

Las VLAN se encuentran en un esquema de redes estándar IEEE, con métodos de etiquetado específicos que permiten el enrutamiento de los paquetes únicamente hacia los puertos que forman parte de la VLAN. Cuando se las configura correctamente, las VLAN constituyen un medio confiable para proteger un conjunto de máquinas virtuales contra intrusiones accidentales o maliciosas.

Las VLAN permiten segmentar una red física de modo que dos máquinas de la red no puedan transmitirse paquetes entre ellas a menos que formen parte de la misma VLAN. Por ejemplo, las transacciones y los registros contables son algunos de los datos internos más confidenciales de una empresa. En una empresa cuyos empleados de los departamentos de ventas, envíos y contabilidad utilizan máquinas virtuales en la misma red física, es posible proteger las máquinas virtuales del departamento contable mediante la configuración de las VLAN.

Empresas de diversos sectores, aseguran sus redes e infraestructuras con la idea de que los ataques siempre vendrán desde el exterior y olvidan que desde dentro de la misma puede sufrir la mayoría de ataques ya sean intencionados o no.

Todo aspecto a recalcar siempre podrá quedarse corto a la hora de tener cubiertas nuestras espaldas dado que con las nuevas tecnologías tanto de ataque como de defensa no podemos tener opciones de quedarnos rezagados a la hora de implementar y de corregir nuestros sistemas.

Asegurar es una opción ineludible, delicada y sobre todo inaplazable porque los ataques pueden producirse de un momento a otro.

Ejemplo de seguridad de VLANs sería que un empleado conecta un SWITCH al cable rj45 que viene asignado a su pc. Así como si estaría activando un servicio DHCP daría direcciones IP a todo nuevo host que se conecte o una conexión WIFI.

Consejos

Si configuras una red de área local virtual (VLAN), recuerda que las VLAN comparten el ancho de banda de la red y requieren medidas de seguridad adicionales.

- Al usar VLAN, separe los clusters sensibles de sistemas del resto de la red. De esta manera, se reduce la probabilidad de que los usuarios tengan acceso a la información almacenada en esos clientes y servidores.
- Asigne un número de VLAN nativo único a los puertos de enlace troncal.
- Limite las VLAN que se pueden transportar mediante un enlace troncal a las que son estrictamente necesarias.
- Desactive el protocolo de enlace troncal (VTP) de VLAN, si es posible. De lo contrario, configure lo siguiente para el VTP: dominio de gestión, contraseña y eliminación. A continuación, defina VTP en modo transparente.
- Utilice configuraciones de VLAN estáticas, cuando sea posible.
- Desactive los puertos de conmutador no utilizados y asígneles un número de VLAN que no esté en uso.

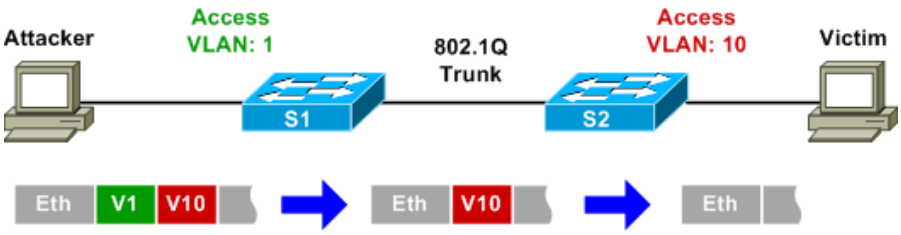
Tipos de ataques

VLAN HOPPING

Es una vulnerabilidad de seguridad que puede aparecer en entornos LAN, donde los Switch están conectados por puertos troncales.

Un atacante intenta obtener acceso a una VLAN no autorizada mediante la adición de dos etiquetas en los paquetes salientes desde el cliente, esto se llama doble etiquetado. Estas etiquetas se agregan a los paquetes que identifican a qué VLAN pertenecen (VLAN ID).

La primera etiqueta (802.1Q) es leída por el puerto de línea externa en el primer switch al que el cliente-atacante está conectado, donde es eliminada y no se vuele a etiquetar por otra y la envía al siguiente switch, en el segundo troncal se lee la segunda etiqueta que envía tráfico desde el atacante a los clientes con el mismo ID de VLAN como la segunda etiqueta y por ende estos datos serán reenviados.



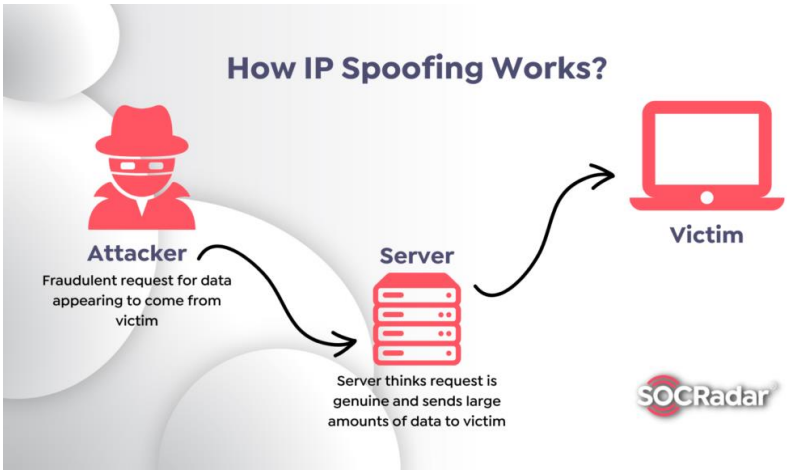
SPOOFING ATTACK

Estos ataques pueden ocurrir sobre varios protocolos permitiendo a un atacante realizar ataques de man-in-the-middle (MITM), de tal manera que tras el ataque todo el tráfico fluye por el equipo del atacante antes de enviárselo al router, switch o equipo de destino.

Donde el atacante adquiere control y permisos para leer, insertar y modificar las comunicaciones.

El ataque de DHCP Spoofing lo podremos evitar mediante la característica DHCP Snooping de Cisco, mientras que los ataques de ARP Spoofing los podremos evitar mediante las técnicas de inspección dinámica ARP que viene por defecto en los nuevos switches.

Ataques de IP Spoofing los podremos evitar configurando IP Source Guard que uniéndolo a DHCP Snooping el switch conocerá la asociación IP – MAC por puerto, evitando los ataques MitM.



Bibliografia

Access Denied. (s. f.). Vmware. Recuperado 3 de septiembre de 2022, de https://docs.vmware.com/es/VMware-vSphere/6.0/com.vmware.vsphere.security.doc/GUID-3887738A-3F3C-4438-B1E7-E35F2A38D94F.html

Unidad ll. (s. f.). pdf. Recuperado 3 de septiembre de 2022, de http://www.itpn.mx/recursositics/7semestre/redesemergentes/Unidad%20II.pdf

Zamorano, J. (2016, 28 marzo). Seguridad en VLANs y sus tipos de ataques. TechClub Tajamar. Recuperado 3 de septiembre de 2022, de https://techclub.tajamar.es/seguridad-vlans-tipos-ataques/

Seguridad de VLAN - Sun Blade X4-2B. (2014, 13 agosto). ORACLE. Recuperado 3 de septiembre de 2022, de https://docs.oracle.com/cd/E50696_01/html/E50091/gmpfo.html

de Luz, S. (2022, 1 septiembre). *VLANs: Qué son, tipos y para qué sirven*. RedesZone. Recuperado 3 de septiembre de 2022, de https://www.redeszone.net/tutoriales/redes-cable/vlan-tipos-configuracion/

colaboradores de Wikipedia. (2022, 18 febrero). *IEEE 802.1Q*. Wikipedia, la enciclopedia libre. https://es.wikipedia.org/wiki/IEEE_802.1Q

Walton, A. (2018, 1 agosto). *Spanning Tree Protocol (STP): Qué hace y cómo funciona »*. CCNA desde Cero. https://ccnadesdecero.es/spanning-tree-protocol-stp-como-funciona/#:%7E:text=El%20STP%2C%20definido%20por%20el,el%20rendimiento%20de%20una%20red

Cómo Comprender VLAN Trunk Protocol (VTP). (2022, 16 marzo). Cisco. https://www.cisco.com/c/es_mx/support/docs/lan-switching/vtp/10558-21.html

4.1 Que es el VTP? - Redes 3. (s. f.). Google docs. https://sites.google.com/site/redes3isi/unidad-4/4-1-que-es-el-vtp

3.2.4.3 Introducción a la resolución de problemas de enlaces troncales. (s/f). Sapalomera.cat. Recuperado el 5 de septiembre de 2022, de https://www.sapalomera.cat/moodlecf/RS/2/course/module3/3.2.4.3/3.2.4.3.html.

Resolución de problemas de VLAN con LinkIQ. (2021, mayo 26). Fluke Networks. https://es.flukenetworks.com/blog/vlan-troubleshooting.

Soporteavanzado, B. (2018, octubre 29). Solución de problemas de VLAN con MS. Soporteavanzado.com; SoporteAvanzado. https://www.soporteavanzado.com/solucion-de-problemas-de-vlan-con-ms/

Unidad II.pdf. (s. f.). .itpn. http://www.itpn.mx/recursositics/7semestre/redesemergentes/Unidad%20II.pdf

Walton, A. (2020, 10 junio). Funcionamiento de Enrutamiento Entre VLAN ». CCNA desde Cero. Recuperado 5 de septiembre de 2022, de https://ccnadesdecero.es/funcionamiento-enrutamiento-entre-vlan/#:%7E:text=El%20Enrutamiento%20Entre%20VLAN%20(Inter,Esta%20es%20una%20soluci%C3%B3n%20antigua.