Saturación de unidifusión en redes de oficinas centrales conmutadas

Contenido

Introducción

Este documento trata de las posibles causas y las consecuencias de la inundación del paquete unicast en las redes de switch.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

Convenciones

Para obtener más información sobre las convenciones del documento, consulte Convenciones de Consejos Técnicos de Cisco.

Definición del problema

Los switches LAN utilizan tablas de reenvío (tablas de Capa 2 [L2], tablas de Memoria de direccionable por contenido [CAM]) para dirigir el tráfico a puertos específicos, según el número de VLAN y la dirección MAC de destino de la trama. Cuando en la VLAN entrante no hay una

entrada que corresponda con la dirección MAC de destino de la trama, la trama (de unidifusión) será enviada a los puertos de reenvío dentro de la VLAN respectiva, lo que causa la inundación.

La inundación limitada es parte del proceso de conmutación normal. Sin embargo, hay ciertas situaciones en las que las inundaciones constantes pueden ocasionar efectos negativos en el rendimiento de la red. Este documento explica qué problemas pueden surgir debido a la saturación y los motivos más frecuentes de por qué cierto tráfico podría saturarse constantemente.

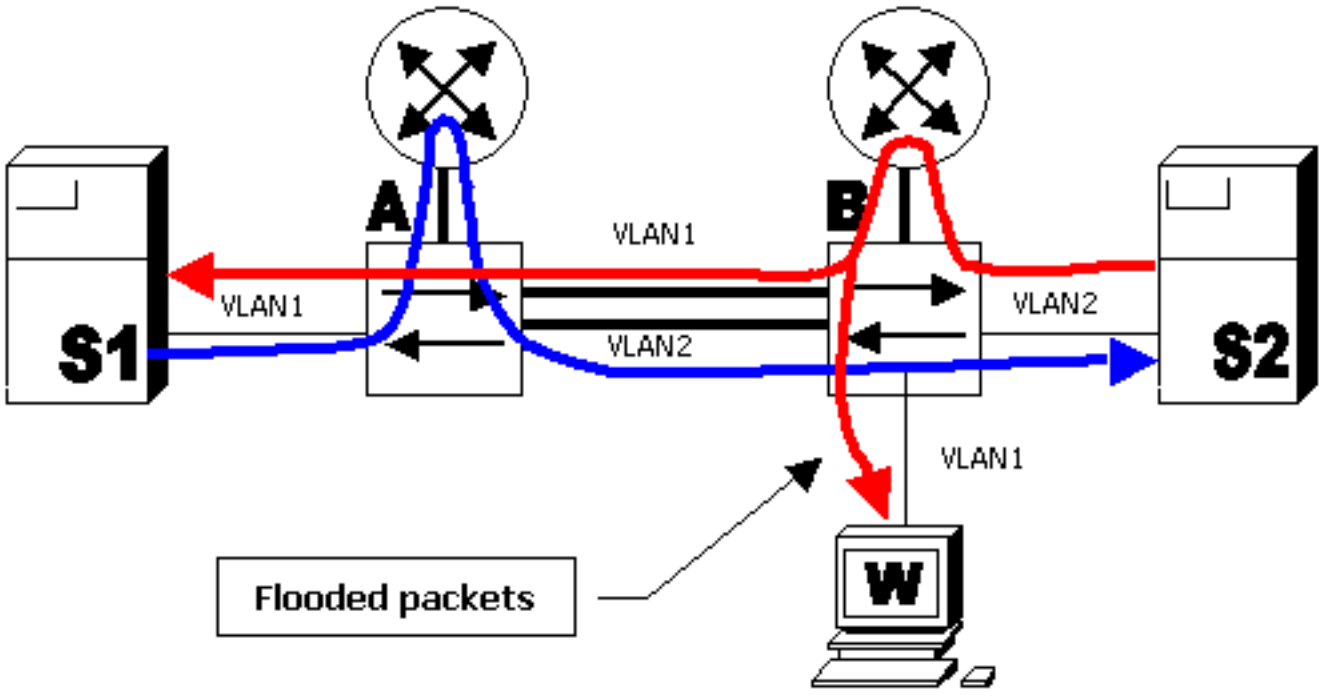
Tenga en cuenta que la mayor parte de los switches modernos, incluidos los switches Catalyst de las series 2900 XL, 3500 XL, 2940, 2950, 2970, 3550, 3750, 4500/4000, 5000 y 6500/6000, mantienen tablas de reenvío L2 por VLAN.

Causas de inundación

La causa de inundación más frecuente es que la dirección MAC de destino del paquete no está en la tabla de reenvío L2 del switch. En este caso, el paquete será inundado fuera de todos los puertos de reenvío a su VLAN (excepto el puerto en el que se recibió). Los siguientes casos prácticos muestran la mayoría de las razones comunes por las cuales el switch no conoce la dirección MAC de destino.

Causa 1: Ruteo Asimétrico

Grandes cantidades de tráfico inundado pueden saturar los links de ancho de banda bajo y causar problemas en el funcionamiento de la red o completar la interrupción de la conectividad en dispositivos conectados a través de tales links de ancho de banda bajo. Tenga en cuenta el siguiente diagrama:



En el diagrama anterior, el servidor S1 en la VLAN 1 está ejecutando una copia de seguridad (transferencia masiva de datos) hacia el servidor S2 en la VLAN 2. El servidor S1 tiene su gateway predeterminado que señala a la interfaz VLAN 1 del router A. El servidor S2 tiene su

gateway predeterminado que señala a la interfaz VLAN2 del router B. Los paquetes desde S1 a S2 seguirán este trayecto:

- S1—VLAN 1—switch A—router A—VLAN 2—switch B—VLAN 2—S2 (línea azul)

Los paquetes de S2 a S1 siguen el siguiente trayecto:

- S2—VLAN 2—switch B—router B—VLAN 1—switch A—inundado a VLAN 1—S1 (línea roja)

Note que con esta distribución, el switch A no "verá" el tráfico desde la dirección S2 MAC en VLAN 2 (dado que la dirección de origen MAC será reescrita por el router B y el paquete sólo llegará en VLAN 1). Esto significa que cada vez que el switch A necesite enviar el paquete a la dirección MAC S2, el paquete será inundado a la VLAN2. La misma situación se producirá con la dirección MAC S1 en el switch B.

Este comportamiento se llama Ruteo Asimétrico. Los paquetes siguen diferentes trayectos que dependen de la dirección. El ruteo asimétrico es una de las dos causas más comunes de inundación.

Impacto de inundación Unicast

Si retomamos el ejemplo anterior, el resultado es que los paquetes de la transferencia de datos entre el S1 y S2 serán inundados principalmente a la VLAN2 en el switch A y a la VLAN1 en el switch B. Esto significa que cada puerto conectado (estación de trabajo W en este ejemplo) en la VLAN1 en el switch B recibirá todos los paquetes de conversación entre el S1 y el S2. Suponga que el respaldo del servidor utiliza 50 Mbps de ancho de banda. Esta cantidad de tráfico saturará los links de 10 Mbps. Esto provocará una interrupción completa de la conectividad a las PC o disminuirá la velocidad de éstas considerablemente.

Esta inundación se debe al ruteo asimétrico y puede detenerse cuando el servidor S1 envía un paquete de difusión (por ejemplo, Protocolo de resolución de direcciones [ARP]). El switch A envía este paquete a la VLAN 1 y el switch B recibe y aprende la dirección MAC de S1. Puesto que el switch no recibe tráfico constantemente, esta entrada de reenvío al final se vencerá y la inundación se reanudará. El mismo proceso se aplica al S2.

Hay distintos enfoques para limitar la inundación causada por el ruteo asimétrico. Si desea más información, consulte estos documentos:

- Ruteo asimétrico con grupos de puentes en switches Catalyst 2948G-L3 y 4908G-L3
- Ruteo Asimétrico y HSRP (Flujo Excesivo de Tráfico Unicast en la Red con Routers que corren HSRP)

El enfoque normalmente consiste en lograr que el tiempo de espera ARP del router y el tiempo de vencimiento de la tabla de reenvío de los switches sean lo más próximos posible. Esto hará que los paquetes ARP sean transmitidos. El reaprendizaje debe producirse antes del vencimiento de la entrada de tabla de reenvío L2.

Un escenario típico en el que se puede observar este tipo de problema es cuando hay switches redundantes de capa 3 (L3) (como un Catalyst 6000 con tarjeta de función de switch multicapa (MSFC)) configurados para equilibrar la carga con protocolo de router de espera en caliente (HSRP). En este caso, un switch estará activo para las VLAN pares y el otro para las VLAN impares.

Causa 2: Cambios de topología del protocolo de árbol de expansión

Otro problema común causado por inundación es la Notificación de cambios de topología (TCN) del Protocolo del árbol de expansión (STP). El TCN está diseñado para corregir las tablas de reenvío una vez que la topología de reenvío ha cambiado. Esto es necesario para evitar una interrupción de conectividad, ya que después de un cambio de la topología algunos destinos previamente accesibles a través de puertos determinados pueden volverse accesibles a través de diferentes puertos. TCN funciona al acortar el tiempo de vencimiento de la tabla de reenvíos, de manera que si no se vuelve a aprender una dirección, caducará y se producirá la inundación.

Las TCN son activadas por un puerto que pasa al o del estado de reenvío. Luego de la TCN, incluso si la dirección MAC de destino en particular ha caducado, la inundación no debería ocurrir durante mucho tiempo en la mayoría de los casos, ya que la dirección se volverá a aprender. El problema puede surgir cuando las TCN se producen repetidas veces en intervalos cortos. Los switches dejarán obsoletas sus tablas de reenvío de manera constante; por lo tanto, la inundación será casi permanente.

Normalmente, una TCN es poco frecuente en una red bien configurada. Cuando el puerto en un switch se activa o desactiva, aparece finalmente un TCN una vez que el estado STP del puerto se cambia hacia o desde reenvío. Cuando el puerto es inestable, se producen TCNs repetitivas e inundación.

Los puertos que tienen habilitada la función STP portfast no provocan TCN cuando entran o salen del estado de reenvío. La configuración de Portfast en todos los puertos de dispositivo final (tales como impresoras, PC y servidores) debe limitar los TC a una cantidad baja. Consulte este documento para obtener más información sobre las TCNs:

- Cómo Comprender los Cambios de Topología de Protocolo de Spanning Tree

Nota: En MSFC IOS, hay una optimización que activará las interfaces VLAN para volver a llenar sus tablas ARP cuando hay una TCN en la VLAN respectiva. Esto limita la inundación en caso de TCN, ya que habrá una difusión de ARP y la dirección MAC del host será aprendida de nuevo mientras el host responda a ARP.

Causa 3: Desbordamiento de tabla de reenvío

Otra posible causa de inundación puede ser desbordamiento de la tabla de reenvío del switch. En este caso, las nuevas direcciones no pueden aprenderse y los paquetes destinados a tales direcciones son inundados hasta que el espacio se torne disponible en la tabla de reenvío. Por lo tanto, se conocerán nuevas direcciones. Esto es posible pero poco común, ya que la mayoría de los switches modernos cuentan con tablas de reenvío lo suficientemente extensas como para acomodar las direcciones MAC para la mayor parte de los diseños.

El agotamiento de la tabla de reenvío también puede derivar de un ataque en la red en que un host comienza a generar tramas con distintas direcciones MAC. Esto inmovilizará todos los recursos de la tabla de reenvío. Cuando las tablas de reenvío se saturan, se producirá la inundación de otro tráfico ya que no puede tener lugar un nuevo aprendizaje. Este tipo de ataque puede detectarse al examinar la tabla de reenvío del switch. La mayoría de las direcciones MAC señalará al mismo puerto o grupo de puertos. Tales ataques pueden prevenirse al limitar el número de direcciones MAC aprendidas en los puertos no confiables a través de la función de seguridad de puerto.

Las Guías de Configuración para los switches de Catalyst que ejecutan Cisco IOS® o software CatOS tienen una sección llamada Configuración de Seguridad de Puerto o Configuración del Control de Tráfico Basado en el Puerto. Consulte la Documentación Técnica para su switch en las

páginas de productos de Cisco Switches para obtener más información.

Nota: Si se produce una inundación de unidifusión en un puerto del switch que está configurado para la seguridad del puerto con la condición de "Restringir" para detener la inundación, se desencadena una violación de la seguridad.

```
Router(config-if)#switchport port-security violation restrict
```

Nota: Cuando se produce una violación de seguridad, los puertos afectados configurados para el modo de "restricción" deben descartar los paquetes con direcciones de origen desconocidas hasta que elimine un número suficiente de direcciones MAC seguras para caer por debajo del valor máximo. Esto hace que aumente el contador SecurityViolation.

Nota: En lugar de este comportamiento, si el puerto del switch pasa al estado "Shutdown", debe configurar `Router(config-if)#switchport block unicast` para que el puerto del switch en particular esté inhabilitado para la inundación de unidifusión.

Cómo detectar una inundación excesiva

La mayoría de los switches no implementan un comando especial para detectar la saturación. Catalyst 6500/6000 Supervisor Engine 2 y switches de series posteriores que ejecutan Cisco IOS System software (nativo) versión 12.1(14)E y posterior o Cisco CatOS system software versión 7.5 o posterior implementan la **función de protección contra inundaciones** unicast. En resumen, esta función permite que el switch monitoree la cantidad de inundación unicast por VLAN y tome medidas especificadas si la inundación excede la cantidad especificada. Las acciones pueden ser syslog, limitar o apagar la VLAN; la acción syslog es la más útil para la detección de la inundación. Cuando la inundación excede la velocidad configurada y la acción configurada es syslog, podrá verse un mensaje similar al siguiente:

```
%UNICAST_FLOOD-4-DETECTED: Host 0000.0000.2100 on vlan 1 is flooding
to an unknown unicast destination at a rate greater than/equal to 1 Kfps
```

La dirección MAC indicada es la dirección MAC de origen desde la cual los paquetes se inundan en este switch. A menudo, es necesario conocer las direcciones MAC de destino por las cuales el switch está inundando (porque el switch realiza el reenvío al observar la dirección MAC de destino). Las versiones (nativas) 12.1(20)E de Cisco IOS catalyst 6500/6000 supervisor engine 2 y posterior implementarán la capacidad para visualizar las direcciones MAC para las cuales se produce la inundación:

```
cat6000#sh mac-address-table unicast-flood
Unicast Flood Protection status: enabled

Configuration:
 vlan      Kfps         action       timeout
------+----------+-----------------+----------
   55          1             alert      none

Mac filters:
 No.   vlan   souce mac addr.           installed on           time left (mm:ss)
-----+------+-----------------+------------------------------+------------------

Flood details:
```

```
 Vlan   souce mac addr.              destination mac addr.
------+---------------+-------------------------------------------------
   55   0000.2222.0000    0000.1111.0029, 0000.1111.0040, 0000.1111.0063
                          0000.1111.0018, 0000.1111.0090, 0000.1111.0046
                          0000.1111.006d
```

Por lo tanto, deben realizarse más investigaciones para determinar si la dirección MAC 0000.2222.0000 envía tráfico a las direcciones MAC mencionadas en la sección de dirección MAC de destino. Si el tráfico es legítimo, luego deberían establecer los motivos por los cuales el switch no conoce las direcciones MAC de destino.

Puede detectar si hay una inundación por medio de la captura de un rastro de paquetes que se visualizó en una estación de trabajo durante el momento en que se produjo la disminución de velocidad o la interrupción. Generalmente, los paquetes de unidifusión que no involucran a la estación de trabajo no deberían ser vistos continuamente en el puerto. Si esto ocurre, es muy probable que esté ocurriendo una saturación. Es posible que los seguimientos de paquetes se vean diferentes cuando hay varias causas para la inundación.

Con el ruteo asimétrico, es posible que haya paquetes destinados a direcciones MAC específicas que no detendrán la inundación incluso después de que el destino responda. Con TCN, la inundación incluirá muchas direcciones distintas pero debería detenerse finalmente y, luego, reiniciar.

Con el desbordamiento de la tabla de reenvío L2, es probable que observe la misma clase de inundación que con el ruteo asimétrico. La diferencia radica en que probablemente haya una gran cantidad de paquetes extraños o de paquetes normales con cantidades anormales, con una dirección MAC de origen diferente.

Información Relacionada

- Soporte de Productos de Switches
- Soporte de Tecnología de LAN Switching
- Soporte Técnico - Cisco Systems