Causas comunes de conectividad intraVLAN e interVLAN lenta en redes conmutadas de campus

Contenido

Introducción

Este documento aborda la mayoría de los problemas más comunes que pueden contribuir a la lentitud de la red. El documento clasifica los síntomas de lentitud de la red comunes, y esboza los métodos de diagnóstico y resolución de problemas.

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

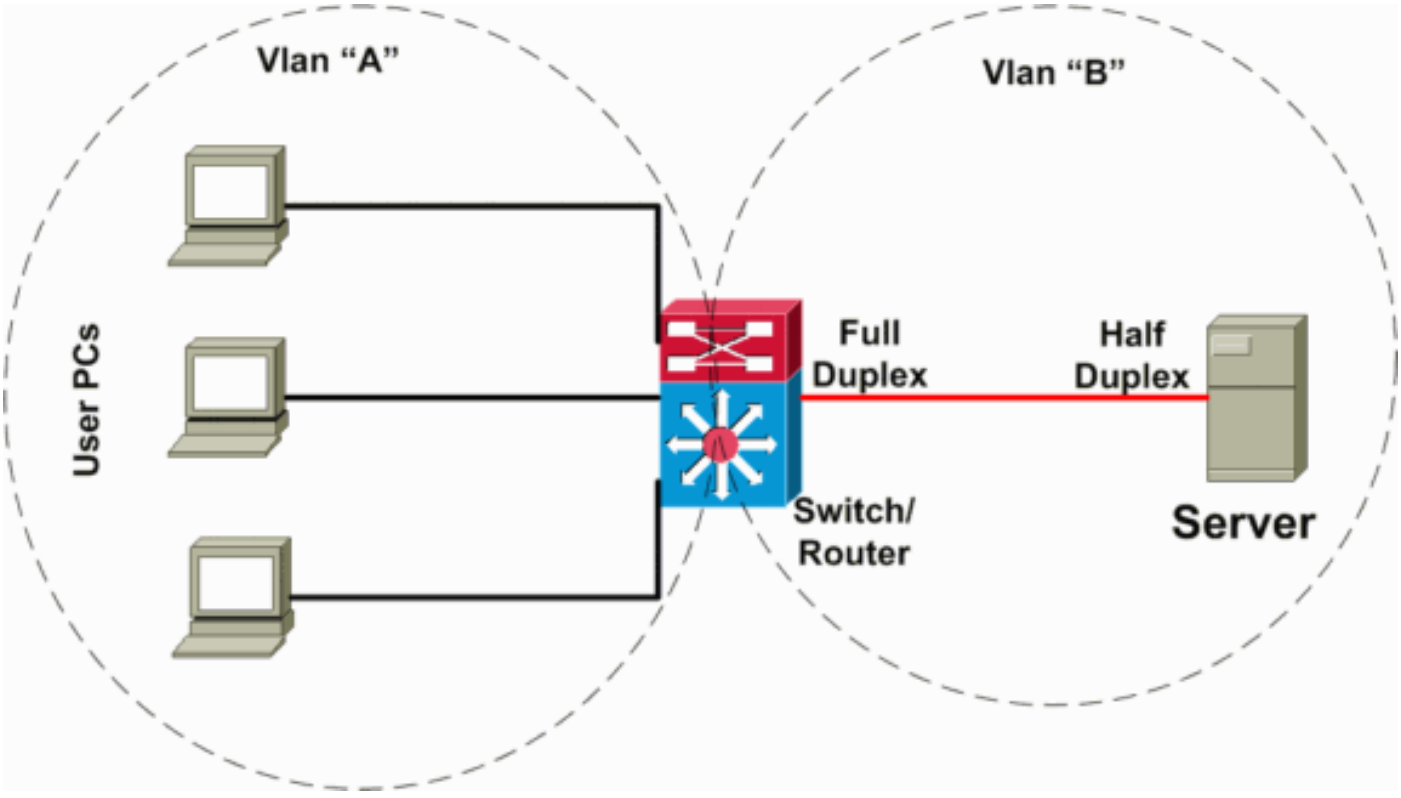
Para obtener más información sobre las convenciones del documento, consulte Convenciones de

Consejos Técnicos de Cisco.

Causas comunes de conectividad lenta dentro y entre las VLAN

Los síntomas de conectividad lenta en las VLAN pueden deberse a varios factores en diferentes capas de la red. Comúnmente, el problema de velocidad de la red puede ocurrir en un nivel inferior, pero los síntomas pueden observarse en un nivel superior a medida que el problema se oculta bajo el término “VLAN lenta”. A modo de aclaración, este documento define los siguientes términos nuevos: "dominio de colisión lenta", "dominio de difusión lenta" (en otras palabras, VLAN lenta) y "reenvío lento entre las VLAN". Estos se definen en la sección Tres categorías de causas a continuación.

En la siguiente situación (ilustrada en el diagrama de red debajo), hay un switch de capa 3 (L3) que realiza el routing entre las VLAN del servidor y el cliente. En esta situación de falla, un servidor está conectado a un switch y el modo de dúplex del puerto se configura como semidúplex en el lado del servidor y como dúplex completo en el lado del switch. Esta configuración incorrecta da como resultado una pérdida de paquetes y lentitud, con una mayor pérdida de paquetes cuando se producen mayores velocidades de tráfico en el enlace donde está conectado el servidor. Para los clientes que se comunican con este servidor, el problema parece ser el reenvío lento entre VLAN porque no tienen inconvenientes para comunicarse con otros dispositivos o clientes en la misma VLAN. El problema se produce solo cuando se comunican con el servidor en una VLAN diferente. Por lo tanto, el problema ocurre en un único dominio de colisión, pero se considera un reenvío lento entre VLAN.



Tres categorías de causas

Las causas de lentitud se pueden dividir en tres categorías:

Conectividad de dominio de colisión lenta

El dominio de colisión se define como los dispositivos conectados configurados en una configuración de puerto semidúplex, conectados entre sí o a un concentrador. Si un dispositivo está conectado a un puerto de switch y se configura el modo dúplex completo, dicha conexión punto a punto no tiene colisiones. La lentitud en ese segmento aún puede ocurrir por diferentes motivos.

Conectividad de dominio de difusión lenta (VLAN lenta)

La conectividad de dominio de difusión lenta se produce cuando toda la VLAN experimenta lentitud (es decir, todos los dispositivos en la misma VLAN).

Conectividad lenta entre las VLAN (reenvío lento entre las VLAN)

La conectividad lenta entre las VLAN (reenvío lento entre las VLAN) se produce cuando no hay lentitud en la VLAN local, pero el tráfico debe reenviarse a una VLAN alternativa y no se reenvía a la velocidad esperada.

Causas de lentitud de la red

Pérdida del paquete

En la mayoría de los casos, una red se considera lenta cuando los protocolos de capa superior (aplicaciones) requieren tiempo extendido para completar una operación que generalmente se ejecuta más rápido. Esa lentitud se debe a la pérdida de algunos paquetes en la red, lo que hace que los protocolos de nivel superior, como TCP o aplicaciones, expiren e inicien la retransmisión.

Problemas de reenvío del hardware

Con otro tipo de lentitud, causada por el equipo de red, el reenvío (ya sea de capa 2 [L2] o L3) se realiza lentamente. Esto se debe a una desviación del funcionamiento y switching normal (diseñados) al reenvío lento de la ruta. Un ejemplo es cuando el switching multicapa (MLS) en el switch reenvía paquetes de L3 entre VLAN en el hardware pero, debido a una configuración errónea, el MLS no funciona correctamente y el router realiza el reenvío en el software (lo que reduce la velocidad de reenvío entre VLAN significativamente).

Solución de problemas de las causas

Solución de problemas del dominio de colisión

Si la VLAN parece estar lenta, primero aísle los problemas del dominio de colisión. Debe establecer si solo los usuarios en el mismo dominio de colisión experimentan problemas de conectividad o si sucede en varios dominios. Para esto, realice una transferencia de datos entre las PC del usuario en el mismo dominio de colisión y compare este rendimiento con el rendimiento de otro dominio de colisión o con el rendimiento esperado.

Si solo se producen problemas en ese dominio de colisión y el rendimiento de los otros dominios de colisión en la misma VLAN es normal, observe los contadores de puertos en el switch para determinar qué problemas puede experimentar este segmento. Lo más probable es que la causa sea simple, como una incompatibilidad de dúplex. Otra causa menos frecuente es la sobrecarga o

sobresuscripción de un segmento. Para obtener más información sobre cómo solucionar los problemas de un solo segmento, consulte el documento Configuración y solución de problemas de autonegociación de dúplex completo/semidúplex de Ethernet 10/100/1000 MB.

Si los usuarios en diferentes dominios de colisión (pero en la misma VLAN) tienen los mismos problemas de rendimiento, aún puede deberse a una incompatibilidad de dúplex en uno o más segmentos Ethernet entre el origen y el destino. A menudo sucede lo siguiente: un switch se configura manualmente para tener un dúplex completo en todos los puertos de la VLAN (la configuración predeterminada es "automática"), mientras que los usuarios (tarjetas de interfaz de red [NIC]) conectados a los puertos realizan un procedimiento de negociación automática. Esto genera una incompatibilidad de dúplex en todos los puertos y, por lo tanto, un mal rendimiento en cada puerto (dominio de colisión). Entonces, aunque parece que toda la VLAN (dominio de difusión) tiene un problema de rendimiento, aún se clasifica como incompatibilidad de dúplex para el dominio de colisión de cada puerto.

Otro caso a tener en cuenta es un problema de rendimiento de NIC en particular. Si una NIC con un problema de rendimiento está conectada a un segmento compartido, puede parecer que un segmento completo experimenta lentitud, especialmente si la NIC pertenece a un servidor que también sirve a otros segmentos o VLAN. Tenga en cuenta este caso, ya que puede confundirlo mientras intenta resolver el problema. Una vez más, la mejor manera de limitar este problema es realizar una transferencia de datos entre dos hosts en el mismo segmento (donde está conectada la NIC con el supuesto problema) o, si solo la NIC está en ese puerto y el aislamiento no es fácil, probar una NIC diferente en este host o intentar conectar el host sospechoso a un puerto separado, garantizando la configuración correcta del puerto y la NIC.

Si el problema persiste, intente solucionar el problema del puerto del switch. Consulte el documento Solución de problemas de la interfaz y el puerto del switch.

El caso más grave es cuando algunas o todas las NIC incompatibles están conectadas a un switch de Cisco. En este caso, parece que el switch tiene problemas de rendimiento. Para verificar la compatibilidad de las NIC con los switches de Cisco, consulte el documento Resolución de problemas de compatibilidad entre las NIC y los switches Catalyst de Cisco.

Debe distinguir entre los dos primeros casos (resolución de problemas de lentitud del dominio de colisión y lentitud de la VLAN) porque estas dos causas implican dominios diferentes. En la lentitud del dominio de colisión, el problema radica fuera del switch (en el extremo del switch en un puerto del switch) o es ajeno al switch. Es posible que solo el segmento tenga problemas (por ejemplo, un segmento sobresuscrito que excede la longitud del segmento, tiene problemas físicos o problemas de concentrador/repetidor). En el caso de la lentitud de la VLAN, el problema probablemente se encuentre dentro del switch (o en varios switches). Si diagnostica el problema incorrectamente, puede perder tiempo buscando el problema en el lugar incorrecto.

Después de haber diagnosticado un caso, revise los elementos que se indican a continuación.

En el caso de un segmento compartido:

- Determine si el segmento está sobrecargado o sobresuscrito.
- Determine si el segmento está en buen estado (incluso si la longitud del cable es correcta, si la atenuación está dentro de la norma y si hay daños físicos en el medio).
- Determine si el puerto de red y todas las NIC conectadas a un segmento tienen configuraciones compatibles.
- Determine si la NIC funciona bien (y ejecuta el controlador más reciente).

- Determine si el puerto de red sigue mostrando errores crecientes.
- Determine si el puerto de red está sobrecargado (especialmente si es un puerto de servidor).

En el caso de un segmento compartido punto a punto o un segmento sin colisión (dúplex completo):

- Determine el puerto y la configuración compatible con la NIC.
- Determine el estado del segmento.
- Determine el estado de la NIC.
- Busque errores de puertos de red o sobresuscripción.

Solución de problemas de conectividad lenta dentro de las VLAN (dominio de difusión)

Después de verificar que no haya ninguna diferencia de dúplex o problemas de dominio de colisión, como se explicó en la sección anterior, ahora puede solucionar problemas de lentitud dentro de las VLAN. El siguiente paso para aislar la ubicación de la lentitud es realizar una transferencia de datos entre hosts en la misma VLAN (pero en puertos diferentes; es decir, en diferentes dominios de colisión) y comparar el rendimiento con las mismas pruebas en VLAN alternativas.

Lo siguiente puede causar VLAN lentas:

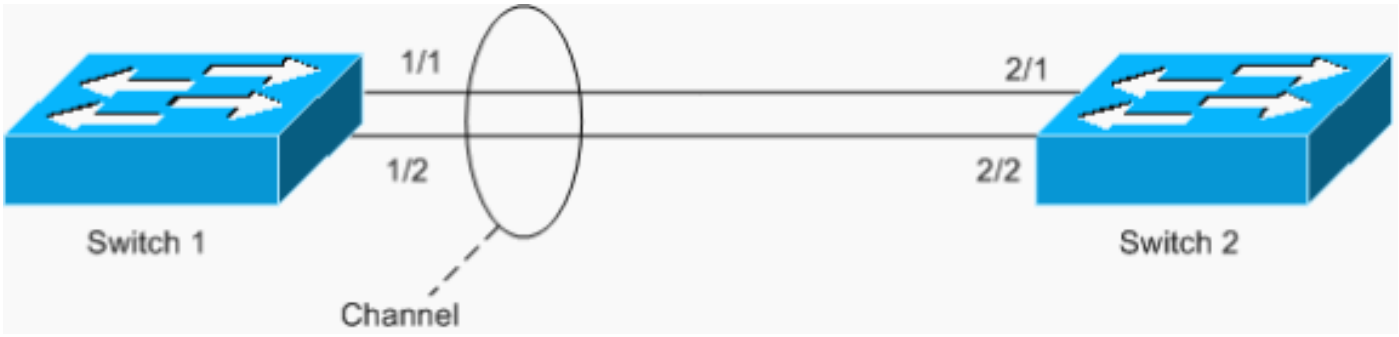
- Bucle de tráfico
- VLAN sobrecargada o sobresuscrita
- Congestión en la ruta en banda del switch
- Uso elevado de la CPU del procesador de administración del switch
- Errores de entrada en un switch de corte
- [1] error de configuración de software o hardware
- [1] bugs de software
- [1] problemas de hardware

1 Estas tres causas de conectividad lenta dentro de las VLAN exceden el alcance de este documento y pueden requerir que un ingeniero de soporte técnico de Cisco resuelva el problema. Después de descartar las primeras cinco causas posibles enumeradas anteriormente, es posible que deba abrir una solicitud de servicio con el soporte técnico de Cisco.

Bucle de tráfico

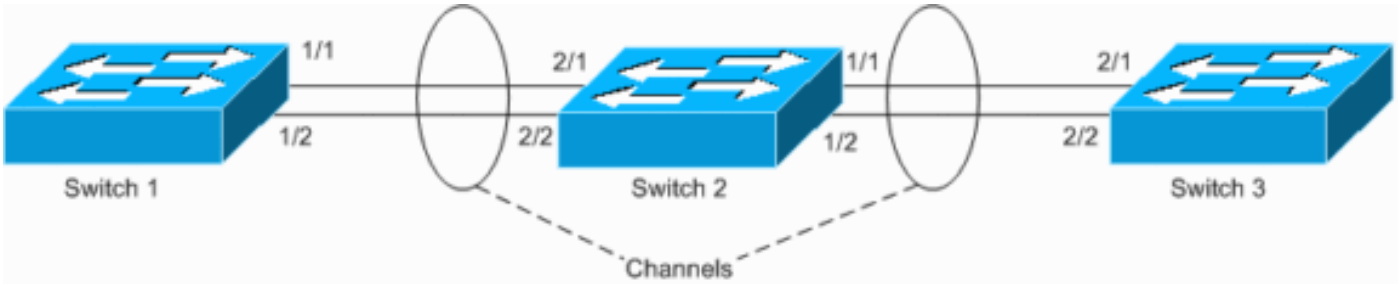
Un bucle de tráfico es la causa más común de una VLAN lenta. Junto con un bucle, debería ver otros síntomas que indican que está experimentando el bucle. Para solucionar problemas de bucles del protocolo de árbol de expansión (STP), consulte el documento Problemas del protocolo de árbol de expansión y consideraciones de diseño relacionadas. Si bien los switches potentes (como Cisco Catalyst 6500/6000) con placas de circuito con capacidad para gigabits pueden manejar algunos bucles (STP) sin comprometer el rendimiento de la CPU de administración, los paquetes en bucle pueden hacer que los búferes de entrada se desborden en las NIC y los búferes de recepción/transmisión (Rx/Tx) en los switches, lo que provoca un rendimiento lento cuando se conectan con otros dispositivos.

Otro ejemplo de bucle es un EtherChannel configurado asimétricamente, como se muestra en la siguiente situación:



En este ejemplo, los puertos 1/1 y 1/2 están en el canal, pero los puertos 2/1 y 2/2 no.

El switch 1 tiene un canal configurado (canal forzado) y el switch 2 no tiene ninguna configuración de canal para los puertos correspondientes. Si el tráfico saturado (mcast/bcast/unidifusión desconocida) fluye desde el switch 1 hacia el switch 2, el switch 2 lo devuelve al canal. No es un bucle completo, ya que el tráfico no se repite continuamente, sino que solo se refleja una vez. Es la mitad del bucle total. Tener dos de estas configuraciones incorrectas puede crear un bucle completo, como se muestra en el siguiente ejemplo.



El riesgo de tener una configuración tan mala es que las direcciones MAC se detectan en los puertos incorrectos, ya que el tráfico se conmuta erróneamente, lo que provoca la pérdida de paquetes. Considere, por ejemplo, un router con un protocolo de router de reserva activa (HSRP) vigente conectado al switch 1 (como se muestra en el diagrama anterior). Después de que el router difunde los paquetes, el switch 2 vuelve a colocar su MAC en bucle y el switch 1 lo desconecta del canal hasta que el router envía nuevamente un paquete de unidifusión.

VLAN sobrecargada o sobresuscrita

Observe si hay cuellos de botella (segmentos sobresuscritos) en alguna de las VLAN y ubíquelos. La primera señal de que su VLAN está sobrecargada es cuando los búferes de recepción o transmisión en un puerto están sobresuscritos. Si ve descartes de paquetes salientes o entrantes en algunos puertos, verifique si esos puertos están sobrecargados. (Un aumento en el descarte de paquetes entrantes no solo puede indicar un búfer de recepción completo). En Catalyst OS (CatOS), los comandos útiles para emitir son **show mac *mod/port*** o show top [N]**.** En el software Cisco IOS® (nativo), puede emitir el comando **show interfaces slot#/port# counters errors command para ver los descartes.** La situación de VLAN sobrecargada o sobresuscrita y la situación del bucle de tráfico a menudo se dan juntas, pero también pueden existir por separado.

Con mayor frecuencia, se produce una sobrecarga en los puertos troncales cuando se subestima el ancho de banda agregado del tráfico. La mejor manera de evitar este problema es configurar un EtherChannel entre los dispositivos donde los puertos tienen cuellos de botella. Si el segmento de red ya es un canal, agregue más puertos a un grupo de canales para aumentar la capacidad del canal.

También tenga en cuenta el problema de polarización de Cisco Express Forwarding (CEF). Este

problema ocurre en las redes donde los routers equilibran la carga de tráfico pero, debido a la uniformidad del algoritmo de Cisco Express Forwarding, todo el tráfico se polariza y, en el siguiente salto, no se equilibra la carga. Sin embargo, este problema no ocurre con frecuencia, ya que requiere una cierta topología con enlaces de L3 con equilibrio de carga. Para obtener más información sobre Cisco Express Forwarding y el equilibrio de carga, consulte Solución de problemas de routing de unidifusión IP que involucran CEF en los switches Catalyst de la serie 6500/6000 con Supervisor Engine 2 que ejecuta el software de sistema CatOS.

Otra causa de sobrecarga de la VLAN es un problema de routing asimétrico. Este tipo de configuración también puede causar una cantidad excesivamente alta de tráfico que satura las VLAN. Para obtener más información, consulte la sección *Causa 1: routing asimétrico del documento* Saturación de unidifusión en redes de campus conmutadas.

A veces, un cuello de botella puede ser un dispositivo de red en sí mismo. Si intenta, por ejemplo, bombear tráfico de 4 gigabits a través del switch con una placa de circuito de 3 gigabits, terminará con una pérdida drástica de tráfico. La comprensión de la arquitectura del switch de red está fuera del alcance de este documento; sin embargo, al considerar la capacidad de un switch de red, preste atención a los siguientes aspectos:

- Capacidad de la placa de circuito
- Problemas de bloqueo de encabezados
- Arquitectura de puerto/switch con y sin bloqueo

Congestión en la ruta en banda del switch

La congestión en la ruta en banda del switch puede generar un bucle de árbol de expansión u otros tipos de inestabilidad en la red. El puerto en banda de cualquier switch de Cisco es un puerto virtual que proporciona una interfaz para el tráfico de administración (como Cisco Discovery Protocol y Port Aggregation Protocol [PAgP]) al procesador de administración. El puerto en banda se considera virtual porque, en algunas arquitecturas, el usuario no puede verlo y las funciones en banda se combinan con el funcionamiento normal del puerto. Por ejemplo, la interfaz SC0 en los switches Catalyst 4000, Catalyst 5000 y Catalyst 6500/6000 (que ejecutan CatOS) es un subconjunto del puerto en banda. La interfaz SC0 proporciona solo una pila IP para el procesador de administración dentro de la VLAN configurada, mientras que el puerto en banda proporciona acceso al procesador de administración para las unidades de datos de protocolo de puente (BPDU) en cualquiera de las VLAN configuradas y para muchos otros protocolos de administración (como Cisco Discovery Protocol, Internet Group Management Protocol [IGMP], Cisco Group Management Protocol y Dynamic Trunking Protocol [DTP]).

Si el puerto en banda se sobrecarga (debido a una aplicación o tráfico de usuario mal configurados), puede producirse una inestabilidad en cualquier protocolo para el que la estabilidad del estado del protocolo se basa en mensajes regulares o "saludos" recibidos. Este estado puede ocasionar bucles temporales, intermitencia en las interfaces y otros problemas, lo que provoca este tipo de lentitud.

Es difícil provocar la congestión del puerto en banda en el switch, aunque los ataques de denegación de servicio (DoS) conformados con fines malintencionados pueden tener éxito. No hay forma de limitar o reducir el tráfico en el puerto en banda. Su solución requiere la intervención e investigación del administrador del switch. Los puertos en banda generalmente tienen una alta tolerancia a la congestión. En raras ocasiones, el puerto en banda no funciona correctamente o se atasca en la dirección de recepción o transmisión. Esto significaría una interrupción grave del hardware y afectaría a todo el switch. Esta condición es difícil de reconocer y generalmente la

diagnostican los ingenieros de soporte técnico de Cisco. Los síntomas son que un switch de repente se vuelve “sordo” y deja de escuchar el tráfico de control, como las actualizaciones de vecinos de Cisco Discovery Protocol. Esto indica un problema de recepción en banda. (Sin embargo, si solo se ve un vecino de Cisco Discovery Protocol, puede estar seguro de que la recepción en banda funciona). En consecuencia, si todos los switches conectados pierden Cisco Discovery Protocol en un solo switch (así como todos los demás protocolos de administración), esto indica un problema de transmisión de la interfaz en banda de ese switch.

Uso elevado de la CPU del procesador de administración del switch

Si se sobrecarga una ruta en banda, puede hacer que un switch experimente condiciones de CPU elevadas; a medida que la CPU procesa todo ese tráfico innecesario, la situación empeora. Si el uso elevado de la CPU se debe a una ruta en banda sobrecargada o un problema alternativo, puede afectar los protocolos de administración, como se describe en la sección Congestión en la ruta en banda del switch más arriba.

En general, considere que la CPU de administración es un punto vulnerable en cualquier switch. Un switch configurado correctamente reduce el riesgo de problemas causados por el uso elevado de la CPU.

La arquitectura de Supervisor Engine I y II de los switches Catalyst de la serie 4000 está diseñada para que la CPU de administración participe en la sobrecarga del switch. Tenga en cuenta lo siguiente:

- La CPU programa una estructura de switch cada vez que una nueva ruta (Supervisor Engine I y II se basan en rutas) ingresa al switch. Si se sobrecarga un puerto en banda, se descarta cualquier ruta nueva. Esto genera pérdida de paquetes (descarte silencioso) y lentitud en los protocolos de capa superior cuando el tráfico se conmuta entre los puertos. (Consulte la sección Congestión en la ruta en banda del switch anterior).
- Dado que la CPU realiza parcialmente el switching en Supervisor Engine I y II, las condiciones de uso elevado de la CPU pueden afectar las capacidades de switching de Catalyst 4000. El uso elevado de la CPU en Supervisor Engine I y II puede deberse a la sobrecarga del switch.

Supervisor Engine II+, III y IV de Catalyst de la serie 4500/4000 son bastante tolerantes al tráfico, pero el aprendizaje de direcciones MAC en Supervisor Engine basado en el software Cisco IOS todavía se realiza por completo en el software (a través de la CPU de administración); existe la posibilidad de que el uso elevado de la CPU pueda afectar este proceso y causar lentitud. Al igual que con Supervisor Engine I y II, el aprendizaje masivo o el reaprendizaje de direcciones MAC pueden causar un uso elevado de la CPU en Supervisor Engine II+, III y IV.

La CPU también participa en el aprendizaje de MAC en los switches Catalyst de las series 3500XL y 2900XL, por lo que el proceso que genera un nuevo aprendizaje rápido de direcciones afecta el rendimiento de la CPU.

Además, el proceso de aprendizaje de direcciones MAC (aunque esté completamente implementado en el hardware) es un proceso relativamente lento en comparación con el proceso de switching. Si hay una tasa continuamente alta de reaprendizaje de direcciones MAC, se debe encontrar y eliminar la causa. Un bucle de árbol de expansión en la red puede provocar este tipo de reaprendizaje de direcciones MAC. El reaprendizaje de direcciones MAC (o la intermitencia de direcciones MAC) también puede deberse a switches de terceros que implementan VLAN basadas en puertos, lo que significa que las direcciones MAC no se asocian a una etiqueta de

VLAN. Este tipo de switch, cuando se conecta a los switches de Cisco en ciertas configuraciones, puede provocar una fuga de MAC entre las VLAN. A su vez, esto puede llevar a una alta tasa de reaprendizaje de direcciones MAC y degradar el rendimiento.

Errores de entrada en un switch de corte

La propagación de paquetes con errores de entrada en un switch de corte está relacionada con la conectividad del dominio de colisión lenta pero, debido a que los paquetes con errores se transfieren a otro segmento, el problema parece ser la conmutación entre los segmentos. Los switches de corte (como los routers de switch de campus (CSR) Catalyst de la serie 8500 y el módulo de switching L3 o Catalyst 2948G-L3 para Catalyst de la serie 4000) comienzan el switching de paquetes/tramas tan pronto como el switch tiene suficiente información para leer la L2/L3 del paquete a fin de reenviar el paquete a su puerto o a puertos de destino. Por lo tanto, aunque el paquete se conmuta entre los puertos de entrada y salida, el origen del paquete ya se reenvía desde el puerto de salida, mientras que el resto del paquete aún se recibe en el puerto de entrada. ¿Qué sucede si el segmento de entrada no está en buen estado y genera un error de comprobación de redundancia cíclica (CRC) o tiempo de ejecución? El switch reconoce esto solo cuando recibe el final de la trama y, para ese momento, la mayor parte de la trama se ha transferido fuera del puerto de salida. Dado que no tiene sentido transferir el resto de la trama errónea, se descarta lo que queda, el puerto de salida incrementa el error de "agotamiento" y el puerto de entrada incrementa el contador de errores correspondiente. Si varios puertos de entrada no están en buen estado y el servidor reside en el puerto de salida, el segmento del servidor parece tener el problema, aunque no sea así.

En el caso de los switches de corte de L3, observe si hay agotamientos y, cuando lo vea, verifique que no haya errores en todos los puertos de entrada.

Error de configuración de software o hardware

Una configuración incorrecta puede hacer que una VLAN sea lenta. Estos efectos negativos pueden deberse a que una VLAN se sobresuscribe o sobrecarga pero, a menudo, se debe a un mal diseño o configuraciones pasadas por alto. Por ejemplo, un segmento (VLAN) puede verse fácilmente saturado por el tráfico de multidifusión (por ejemplo, transmisión de video o audio) si las técnicas de restricción de tráfico de multidifusión no están configuradas correctamente en esa VLAN. Dicho tráfico de multidifusión puede afectar la transferencia de datos, lo que provoca la pérdida de paquetes en una VLAN completa para todos los usuarios (y satura los segmentos de usuarios que no tenían la intención de recibir los flujos de multidifusión).

Errores de software y problemas de hardware

Los errores de software y los problemas de hardware son difíciles de identificar porque causan desviaciones; algo complicado de resolver. Si cree que el problema está ocasionado por un error de software o un problema de hardware, comuníquese con los ingenieros de soporte técnico de Cisco para que investiguen el problema.

Solución de problemas de conectividad lenta entre las VLAN

Antes de solucionar problemas de conectividad lenta entre las VLAN (interVLAN), investigue y descarte los problemas que se analizan en las secciones Solución de problemas de dominio de colisión y Solución de problemas de conectividad lenta dentro de las VLAN (dominio de difusión) de este documento.

La mayoría de las veces, la conectividad lenta entre las VLAN se debe a la configuración incorrecta del usuario. Por ejemplo, si configuró incorrectamente el MLS o switching multicapa multidifusión (MMLS), la CPU del router realiza el reenvío de paquetes, lo que genera una ruta lenta. Para evitar una configuración incorrecta y solucionar los problemas de manera eficaz cuando sea necesario, debe comprender el mecanismo de reenvío de L3 utilizado por su dispositivo. En la mayoría de los casos, el mecanismo de reenvío de L3 se basa en una compilación de tablas de routing y protocolos de resolución de direcciones (ARP) y en la programación de información de reenvío de paquetes extraída en el hardware (accesos directos). Cualquier falla en el proceso de programación de accesos directos lleva al reenvío de paquetes de software (ruta lenta), al reenvío incorrecto (reenvío a un puerto incorrecto) o al bloqueo del tráfico.

Por lo general, una falla en la programación de accesos directos o la creación de accesos directos incompletos (lo que también puede provocar el reenvío de paquetes de software, el envío incorrecto o agujeros negros de tráfico) es el resultado de un error de software. Si sospecha que esto es así, solicite a los ingenieros de soporte técnico de Cisco que lo investiguen. Otros motivos para el reenvío lento entre VLAN incluyen el mal funcionamiento del hardware; sin embargo, estas causas están fuera del alcance de este documento. El mal funcionamiento del hardware simplemente evita la creación exitosa de accesos directos en el hardware y, por lo tanto, el tráfico puede tomar una ruta lenta (software) o estar oculto. Los errores de hardware también deben ser manejados por los ingenieros de soporte técnico de Cisco.

Si está seguro de que el equipo está configurado correctamente, pero no se realiza el switching en el hardware, la causa puede ser un error de software o un mal funcionamiento del hardware. Sin embargo, tenga en cuenta las capacidades del dispositivo antes de llegar a esta conclusión.

Las siguientes son las dos situaciones más frecuentes en las que el reenvío de hardware puede detenerse o no tener lugar:

- Se agota la memoria que almacena los accesos directos. Una vez que la memoria está llena, el software generalmente deja de crear accesos directos. Por ejemplo, el MLS, ya sea NetFlow o Cisco Express Forwarding, se torna inactivo cuando no hay espacio para nuevos accesos directos y conmuta al software (ruta lenta).
- El equipo no está diseñado para realizar la conmutación de hardware, pero esto no es algo obvio. Por ejemplo, Supervisor Engine III y posterior de Catalyst de la serie 4000 están diseñados para reenviar solo tráfico IP de hardware; todos los otros tipos de tráfico son software procesado por la CPU. Otro ejemplo es la configuración de una lista de control de acceso (ACL) que requiere la intervención de la CPU (como la opción de "registro"). El tráfico que se aplica a esta regla se procesa mediante la CPU en el software.

Los errores de entrada en un switch de corte también pueden contribuir a la lentitud del routing entre VLAN. Los switches de corte utilizan los mismos principios arquitectónicos para reenviar tráfico de L3 y L2, por lo que los métodos de solución de problemas que se proporcionan en la sección Solución de problemas de conectividad lenta dentro de las VLAN (dominio de difusión) anterior también pueden aplicarse al tráfico de L2.

Otro tipo de configuración incorrecta que afecta al routing entre VLAN es la configuración incorrecta de los dispositivos del usuario final (como la PC y las impresoras). Una situación común es una PC mal configurada; por ejemplo, un gateway predeterminado está mal configurado, la tabla ARP de la PC no es válida o el cliente IGMP no funciona correctamente. Un caso común es cuando hay varios routers o dispositivos con capacidad de routing y algunas o todas las PC del usuario final están mal configuradas para utilizar el gateway predeterminado incorrecto. Este puede ser el caso más problemático, ya que todos los dispositivos de red están

configurados y funcionan correctamente; sin embargo, los dispositivos de usuario final no los utilizan debido a esta configuración incorrecta.

Si un dispositivo en la red es un router común que no tiene ningún tipo de aceleración de hardware (y no participa en NetFlow con MLS), la velocidad de reenvío de tráfico depende completamente de la velocidad de la CPU y de qué tan ocupada está. El uso elevado de la CPU definitivamente afecta la velocidad de reenvío. En los switches de L3, sin embargo, las condiciones de uso elevado de la CPU no afectan necesariamente la velocidad de reenvío; el uso elevado de la CPU afecta la capacidad de la CPU para crear (programar) un acceso directo de hardware. Si el acceso directo ya está instalado en el hardware, incluso si se usa mucho la CPU, el tráfico (para el acceso directo programado) se conmuta en el hardware hasta que el acceso directo caduca (si hay un temporizador de caducidad) o lo elimina la CPU. Sin embargo, si un router está configurado para cualquier tipo de aceleración de software (como switching rápido o switching de Cisco Express Forwarding), el reenvío de paquetes puede verse afectado por accesos directos de software; si se rompe un acceso directo o si el mecanismo en sí falla, entonces, en lugar de acelerar la velocidad de reenvío, se envía tráfico a la CPU, lo que reduce la velocidad de reenvío de datos.

Información Relacionada

- Resolución de Problemas de IP MultiLayer Switching
- Troubleshooting de Unicast IP Routing con CEF en Catalyst 6500/6000 Series Switches con Supervisor Engine 2 y ejecutando CatOS System Software.
- Configuración de ruteo inter-VLAN con switches Catalyst de la serie 3550
- Soporte de Productos de Switches
- Soporte de Tecnología de LAN Switching
- Soporte Técnico y Documentación - Cisco Systems