Causas comunes del IntraVLAN lento y Conectividad del interVLAN en las redes del Campus Switch

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.

prerrequisitos

Requisitos

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 del IntraVLAN y de la Conectividad lentos del interVLAN

Los síntomas de conectividad lenta en un VLA N se pueden causar por los factores múltiples en diversas capas de red. El problema de la velocidad de la red puede ocurrir comúnmente en un nivel inferior, pero los síntomas se pueden observar en un de alto nivel mientras que el problema se enmascara bajo término “VLA N lento”. Para aclarar, este documento define los nuevos términos siguientes: “dominio de colisión lento”, “dominio de broadcast lento” (es decir VLA N lento), y “interVLAN lento que remite”. Éstos se definen en las categorías de la sección tres de causas, abajo.

En el escenario siguiente (ilustrado en el diagrama de la red abajo), hay un Switch de la capa 3 (L3) que realiza el InterVLAN Routing entre el servidor y los VLA N del cliente. En este escenario de falla, un servidor está conectado con un Switch, y el modo de dúplex de puerto es semidúplex configurado en el lado del servidor y el FULL-duplex en el lado del Switch. Este misconfiguration da lugar a una pérdida del paquete y a una lentitud, con la pérdida del paquete creciente cuando relaciones del tráfico más altas ocurren en el link donde el servidor está conectado. Para los clientes que comunican con este servidor, los parecer del problema el interVLAN lento que remite porque no tienen un problema que comunican a los otros dispositivos o a los clientes en el mismo VLA N. El problema ocurre solamente al comunicar al servidor en un diverso VLA N. Así, el problema ocurrió en un solo dominio de colisión, pero se considera como envío lento del interVLAN.

Tres categorías de causas

Las causas de la lentitud se pueden dividir en tres categorías, como sigue:

Conectividad lenta del dominio de colisión

El dominio de colisión se define como dispositivos conectados configurados en una configuración del puerto semi dúplex, conectada el uno al otro o un concentrador. Si un dispositivo está conectado con un puerto del switch y configuran al modo dúplex completo, tal conexión Point-to-Point es sin colisiones. La lentitud en tal segmento todavía puede ocurrir por diversas razones.

Conectividad lenta del dominio de broadcast (VLA N lento)

La Conectividad lenta del dominio de broadcast ocurre cuando el VLAN entero (es decir, todos los dispositivos en el mismo VLA N) experimenta la lentitud.

Conectividad lenta del interVLAN (reenvío lento entre los VLA N)

La Conectividad lenta del interVLAN (reenvío lento entre los VLA N) ocurre cuando no hay lentitud en el VLA N local, solamente tráfico necesita ser remitida a un VLA N alterno, y no se remite a la velocidad esperada.

Causas para la lentitud de la red

Pérdida del paquete

En la mayoría de los casos, una red se considera lenta cuando los protocolos de capa más altas (aplicaciones) requieren la hora extendida de completar una operación que se ejecute típicamente más rápidamente. Esa lentitud es causada por la pérdida de algunos paquetes en la red, que hace los protocolos de mayor nivel como el TCP o las aplicaciones medir el tiempo hacia fuera e iniciar la retransmisión.

Problemas del hardware que reenvía

Con otro tipo de lentitud, causado por el equipo de red, el envío (si la capa 2 [L2] o L3) se realiza lentamente. Esto es debido a una desviación de la operación (diseñada) normal y de la transferencia reducir el reenvío de trayecto. No está funcionando un ejemplo de esto es cuando el Multilayer Switching (MLS) en del Switch los paquetes L3 adelante entre los VLA N en el hardware, pero debido al misconfiguration, MLS correctamente y el envío es hecho por el router en el software (que cae la velocidad de reenvío del interVLAN perceptiblemente).

Resuelva problemas la causa

Resuelva problemas los problemas del dominio de colisión

Tan si su VLA N aparece ser lento, primero aísle los problemas del dominio de colisión. Usted necesita establecer si solamente los usuarios en el mismo dominio de colisión están experimentando los problemas de conectividad, o si está sucediendo en los dominios múltiples. Para hacer esto, haga una Transferencia de datos entre el usuario PC en el mismo dominio de colisión, y compare este funcionamiento con el funcionamiento de otro dominio de colisión, o con su rendimiento esperado.

Si los problemas ocurren solamente en ese dominio de colisión, y el funcionamiento de otros dominios de colisión en el mismo VLA N es normal, después mirada en los contadores de puerto en el Switch para determinar qué problemas puede experimentar este segmento. Muy probablemente, la causa es simple, por ejemplo una discordancia dúplex. Otro, causa menos frecuente es un segmento sobrecargado u oversubscribed. Para más información sobre resolver problemas un solo problema del segmento, refiera al documento que configura y que resuelve problemas la negociación automática del dúplex completo y del semidúplex de los Ethernetes 10/100/1000Mb.

Si los usuarios en diversos dominios de colisión (pero en el mismo VLA N) están teniendo los mismos problemas de rendimiento, todavía puede ser causado por una discordancia dúplex en uno o más segmentos Ethernet entre la fuente y el destino. El escenario siguiente sucede a menudo: un Switch se configura manualmente para tener FULL-duplex en todos los puertos en el VLA N (la configuración predeterminada es “auto”), mientras que los usuarios ([NICs] del Network Interface Cards) conectados con los puertos están realizando un procedimiento de negociación automática. Esto da lugar a la discordancia dúplex en todos los puertos y, por lo tanto, al mún funcionamiento en cada puerto (dominio de colisión). Así pues, aunque aparezca como si el VLAN entero (dominio de broadcast) esté teniendo un problema de rendimiento, todavía se categoriza como discordancia dúplex, para el dominio de colisión de cada puerto.

Otro caso que se considerará es un problema de rendimiento de NIC determinado. Si un NIC con un problema de rendimiento está conectado con un segmento compartido, después puede aparecer que un segmento entero está experimentando la lentitud, especialmente si el NIC

pertenece a un servidor que también sirva otros segmentos o VLA N. Tenga este caso presente porque puede engañarle mientras que usted resuelve problemas. Una vez más la mejor manera de estrechar abajo este problema es realizar una Transferencia de datos entre dos host en el mismo segmento (donde el NIC con el problema supuesto está conectado), o si solamente el NIC está en ese puerto, el aislamiento no es fácil, así que intente un diverso NIC en este host, o intente conectar el host sospechoso en un puerto separado, asegurando la configuración adecuada del puerto y del NIC.

Si todavía existe el problema, intente resolver problemas el puerto del switch. Refiera al puerto del switch del troubleshooting del documento e interconecte los problemas.

La mayoría del caso grave es cuando algunos o todos los NIC incompatibles están conectados con un switch Cisco. En este caso, aparece que el Switch está teniendo problemas de rendimiento. Para marcar la compatibilidad de los NIC con los switches Cisco, refiera al Switches del Cisco Catalyst del troubleshooting del documento a los problemas de la compatibilidad NIC.

Usted necesita distinguir entre los primeros dos casos (lentitud y lentitud de VLAN del dominio de colisión del troubleshooting) porque estas dos causas implican diversos dominios. Con la lentitud del dominio de colisión, el problema miente fuera del Switch (o al borde del Switch, en un puerto del switch) o del externo al Switch. Puede ser que el segmento solamente tenga problemas (por ejemplo, un segmento oversubscribed, excediendo la longitud del segmento, los problemas físicos en el segmento, o el concentrador/los problemas del repetidor). En el caso de la lentitud de VLAN, el problema miente muy probablemente dentro del Switch (o de los switches múltiples). Si usted diagnostica el problema incorrectamente, usted puede perder el tiempo que busca el problema en el lugar incorrecto.

Después de que usted haya diagnosticado una caja, marque así pues, los elementos enumerados abajo.

En el caso de un segmento compartido:

- determine si el segmento es sobrecargado u oversubscribed
- determine si el segmento es sano (incluyendo si la longitud del cable está correcta, si la atenuación está dentro de la norma, y si hay daños físicos del media)
- determine si el puerto de red y todos los NIC conectados con un segmento tienen configuraciones compatibles
- determine si el NIC se está realizando bien (y está funcionando con el último driver)
- determine si el puerto de red continúa mostrando los errores cada vez mayores
- determine si se sobrecarga el puerto de red (especialmente si es un puerto de servidor)

En el caso de un segmento compartido del Punto a punto, o del segmento sin colisiones (del FULL-duplex):

- determine el puerto y la configuración NIC-compatible
- determine la salud del segmento
- determine la salud del NIC
- busque los errores o el oversubscription del puerto de red

Resuelva problemas el IntraVLAN lento (el dominio de broadcast)

Después de verificar no hay discordancia dúplex o los problemas del dominio de colisión como se explica en la sección antedicha, usted puede ahora resolver problemas la lentitud del IntraVLAN.

El siguiente paso en el aislamiento de la ubicación de la lentitud es realizar una Transferencia de datos entre los host en el mismo VLA N (pero en diversos puertos; es decir, en diversos dominios de colisión), y compare el funcionamiento con las mismas pruebas en los VLA N alternos.

Lo que sigue puede causar los VLA N lentos:

- loop del tráfico
- VLA N sobrecargado u oversubscribed
- congestión en el Switch trayecto dentro de la banda
- utilización del procesador del administrador de switches CPU elevada
- errores de ingreso en a corte-por el Switch
- [1] software o error de configuración del hardware
- bug de software [1]
- problemas de hardware [1]

las causas [1]These tres de la Conectividad lenta del intraVLAN están fuera del alcance de este documento, y pueden requerir el troubleshooting de un ingeniero de soporte técnico de Cisco. Después de eliminar las primeras cinco posibles causas enumeradas arriba, usted puede necesitar abrir una solicitud de servicio con el Soporte técnico de Cisco.

Loop del tráfico

Un loop del tráfico es la mayoría de la causa común de un VLA N lento. Junto con un loop, usted debe ver otros síntomas que indiquen que usted está experimentando un loop. Para resolver problemas los loopes del Spanning Tree Protocol (STP), refiera a los problemas y a las consideraciones de diseño relacionadas del Spanning Tree Protocol del documento. Aunque el Switches potente (como el Cisco Catalyst 6500/6000) con las placas madre gigabit-capaces pueda dirigir algún (STP) coloque sin el compromiso del funcionamiento de la Administración CPU, los paquetes colocados pueda hacer memorias intermedias de entrada desbordar en los NIC y recibir/transmita los buffers (del rx/tx) en el Switches, causando el rendimiento lento al conectar con los otros dispositivos.

Otro ejemplo del loop es un EtherChannel asimétrico configurado, tal y como se muestra en del escenario siguiente:

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

El Switch1 tiene un canal configurado (canal forzado), y el Switch2 no tiene ninguna Configuración de canal para los puertos correspondientes. Si el tráfico saturado (mcast/bcast/unidifusión desconocida) fluye del Switch1 hacia el Switch2, el Switch2 lo coloca nuevamente dentro del canal. No es un loop completo, puesto que el tráfico no se coloca continuamente, pero se refleja solamente una vez. Es una mitad del loop total. Tener dos tales misconfigurations puede crear un loop completo, tal y como se muestra en del ejemplo abajo.

El peligro del tener tal misconfiguration es que las direcciones MAC están aprendidas en los puertos incorrectos mientras que el tráfico se conmuta incorrectamente, que causa la pérdida del paquete. Considere, por ejemplo, a un router con el Hot Standby Router Protocol (HSRP) activo que esté conectado con el Switch1 (tal y como se muestra en del diagrama antedicho). Después de que el router transmita los paquetes, su MAC es circuito hecho atrás por el Switch2 y aprendido del canal por el Switch1, hasta que un paquete de unidifusión se envíe del router otra vez.

VLA N sobrecargado u Oversubscribed

Aviso si hay embotellamientos (segmentos oversubscribed) dondequiera en sus VLA N y los localiza. La primera muestra que su VLA N está sobrecargado es si los buffers del rx o del tx en un puerto son oversubscribed. Si usted ve los outdiscards o los indiscards en algunos puertos, marque para ver si se sobrecargan esos puertos. (Un aumento en los indiscards no sólo indica un buffer completo del rx.) En el Catalyst OS (CatOS), los comandos útiles de publicar son */port Mod del* **mac de la demostración** o **de mostrar superior [n]**. En el software de Cisco IOS® (nativo), usted puede publicar el **comando show interfaces slot-/port- counters errors** de ver los descartes. Haber sobrecargado o escenario de VLAN excedido de suscriptores y el escenario del loop del tráfico se acompañan a menudo, pero pueden también existir por separado.

Lo más frecuentemente, la sobrecarga sucede en los puertos de la estructura básica cuando el ancho de banda agregado del tráfico se subestima. La mejor manera de trabajar alrededor de este problema es configurar un EtherChannel entre los dispositivos para los cuales los puertos bottlenecked. Si el segmento de red es ya un canal, agregue más puertos en un grupo de canal para aumentar la capacidad del canal.

También sea consciente del problema de la polarización del Cisco Express Forwarding (CEF). Este problema sucede en las redes en las cuales el tráfico es carga balanceada de Routers, pero debido a la uniformidad de algoritmos del Cisco Express Forwarding, se polariza todo el tráfico y, en el salto siguiente, no es carga balanceada. Este problema no ocurre a menudo, sin embargo, porque requiere cierta topología con los links de la carga balanceada L3. Para más información con respecto el Cisco Express Forwarding y al Equilibrio de carga, vea el Unicast IP Routing del Troubleshooting el implicar del CEF en los Catalyst 6500/6000 Series Switch con un Supervisor Engine 2 y un software del sistema corriente de CatOS.

Otra causa para el VLA N sobrecargado es un problema del Asymmetric Routing. Los este tipos de configuración también pueden causar excesivamente - una mucha cantidad de tráfico que inunda sus VLA N. Para más información, refiera a la *causa 1:* Sección del *Asymmetric Routing de las* saturaciones de unidifusión en red de campus conmutada del documento.

A veces un embotellamiento puede ser un dispositivo de red sí mismo. Si usted intenta, por ejemplo, bombear el tráfico 4-gigabit aunque el Switch con un backplane 3-gigabit, usted termina para arriba con una pérdida dramática del tráfico. La comprensión de la arquitectura del switch de red está fuera del ámbito de este documento; sin embargo, cuando en vista de la capacidad de un switch de red, atención de la paga a los aspectos siguientes:

- capacidad de backplane
- jefe de line que bloquea los problemas
- bloqueo y arquitectura no bloqueando del /port del Switch

Congestión en el Switch trayecto dentro de la banda

La congestión en el Switch trayecto dentro de la banda puede dar lugar a un Spanning-Tree Loop o a otros tipos de inestabilidad en la red. El puerto inband en cualquier switch Cisco es un puerto virtual que proporciona la interfaz para el tráfico de administración (tráfico tal como protocolo cisco discovery y Protocolo de agrupamiento de puertos PAgP) al procesador de administración. El puerto inband se considera virtual porque, en algunas arquitecturas, el usuario no puede verlo, y las funciones inband se combinan con el funcionamiento normal de puerto. Por ejemplo, la interfaz SC0 en el Catalyst 4000, Switches de las Catalyst 5000 y Catalyst 6500/6000 Series (CatOS que se ejecuta) es un subconjunto del puerto inband. La interfaz SC0 proporciona

solamente una pila IP para el procesador de administración dentro del VLAN configurado, mientras que el puerto inband proporciona el acceso al procesador de administración para las Unidades (BPDU) en los VLAN configurados uces de los y para muchos otros protocolos de la Administración (tales como protocolo cisco discovery, Internet Group Management Protocol [IGMP], Cisco Group Management Protocol, y protocolo dynamic trunking [DTP]).

Si el puerto inband consigue sobrecargado (debido a una aplicación o a un tráfico de usuarios mal configurado), puede dar lugar a la inestabilidad de cualquier protocolo para las cuales la estabilidad del estado del protocolo se base en los mensajes regulares o del “hellos” recibido. Este estado puede dar lugar a los Loop temporales, interconecta el cambio, y otros problemas, causando este tipo de lentitud.

Es difícil causar la congestión del puerto inband en el Switch, aunque los ataques malévolo formados de la negación de servicio (DOS) pueden tener éxito. No hay tarifa-límite de la manera ni reduce el tráfico en el puerto inband. Una solución requiere la intervención del administrador y la investigación del Switch. Los puertos Inband tienen generalmente una alta tolerancia para la congestión. Hace el malfuncionamiento inband del puerto o consigue raramente pegado en la dirección del rx o del tx. Esto significaría la caída del sistema severa del hardware y afectaría al Switch del conjunto. Esta condición es difícil de reconocer y es diagnosticada generalmente por los ingenieros de soporte técnico de Cisco. Los síntomas son que un Switch llega a ser “sordo” y para repentinamente el considerar del tráfico de control tal como actualizaciones del vecino del protocolo cisco discovery. Esto indica un rx problema dentro de la banda. (Si, sin embargo, ven a apenas un vecino del protocolo cisco discovery, usted puede sentirse confiado que inband está trabajando.) Correspondientemente, si todos los switches conectados pierden el protocolo cisco discovery de un un solo switch (así como del resto de los protocolos de la Administración), indica los problemas del tx de la interfaz inband de ese Switch.

Utilización del procesador del administrador de switches CPU elevada

Si trayecto dentro de la banda se sobrecarga, puede hacer un Switch experimentar CPU elevada las condiciones; y, como el CPU procesa todo ese tráfico innecesario, la situación empeora. Si CPU elevada la utilización es causada por sobrecargado trayecto dentro de la banda o un problema alterno, puede afectar a los protocolos de la Administración según lo descrito en la congestión en la sección del Switch trayecto dentro de la banda, arriba.

Considere generalmente la Administración CPU ser una punta vulnerable de cualquier Switch. Un switch configurado reduce correctamente el riesgo de problemas causados por CPU elevada la utilización.

La arquitectura del Supervisor Engine I e II de los Catalyst 4000 Series Switch se diseña tales que la Administración CPU está implicada en la transferencia por encima. Tenga presente el siguiente:

- El CPU programa un Switch Fabric siempre que una nueva trayectoria (trayectoria-se basan el Supervisor Engine I e II) ingrese el Switch. Si se sobrecarga un puerto inband, hace cualquier nueva trayectoria ser caído. Esto da lugar al paquete perdido (descarte silencioso) y a la lentitud en los protocolos de capa más altas cuando el tráfico se conmuta entre los puertos. (Refiera a la congestión de la sección en el Switch trayecto dentro de la banda, arriba.)
- Puesto que el CPU realiza parcialmente la transferencia en el Supervisor Engine I e II, CPU elevada las condiciones pueden afectar a las capacidades de Switching del Catalyst 4000. CPU elevada la utilización en el Supervisor Engine I e II se pueden causar por la

transferencia por encima sí mismo.

Los motores II+, III y IV del supervisor de las 4500/4000 Series del Catalyst son bastante tráfico-tolerantes, pero el MAC Address Learning en el Supervisor Engine basado en software del Cisco IOS todavía se hace totalmente en el software (por la Administración CPU); hay una ocasión que CPU elevada la utilización puede afectar a este proceso y causar la lentitud. Como con el Supervisor Engine I e II, el MAC Address Learning masivo o el volver a aprender puede causar CPU elevada la utilización en los motores II+, III y IV del supervisor.

El CPU está implicado en el aprendizaje de MAC en el Switches de las Catalyst 3500XL y 2900XL Series también, tan un proceso que los resultados en el rendimiento de la CPU de las influencias del direccionamiento que vuelve a aprender rápido.

También, el proceso del MAC Address Learning (incluso si se implementa totalmente en hardware) es un proceso relativamente lento, comparado a un proceso de la transferencia. Si hay continuamente una alta velocidad de la dirección MAC que vuelve a aprender, después la causa debe ser encontrada y ser eliminada. Un Spanning-Tree Loop en la red puede causar este tipo de volver a aprender de la dirección MAC. El volver a aprender del MAC address (o el cambio del MAC address) se puede también causar por el Switches de tercera persona que implementa los VLA N del acceso basado, así que él significa que los direccionamientos MAC no están consiguiendo asociados a una etiqueta del VLA N. Esta clase de Switch, cuando está conectada con los switches Cisco en ciertas configuraciones, puede dar lugar a la fuga de MAC entre los VLA N. A su vez, esto puede llevar a una alta velocidad de la dirección MAC que vuelve a aprender y puede degradar el funcionamiento.

Errores de ingreso en a Corte-por el Switch

Corte-por la propagación de paquetes del error de ingreso se relaciona para reducir la Conectividad del dominio de colisión, pero porque los paquetes de errores se transfieren a otro segmento, el problema aparece conmutar entre los segmentos. Corte-por el Switches (tal como los routeres switch de campus de las Catalyst 8500 Series (CSR) y el Catalyst 2948G-L3 o el módulo de switching L3 para las Catalyst 4000 Series) comience el Packet/Frame Switching tan pronto como el Switch tenga bastante información de leer la encabezado L2/L3 del paquete para remitir el paquete a su puerto destino o puertos. Así pues, mientras que el paquete se está conmutando entre el ingreso y los puertos de egreso, el principio del paquete se remite ya el puerto de egreso de los, mientras que el resto del paquete todavía está siendo recibido por el puerto de ingreso. ¿Qué sucede si el segmento del ingreso no es sano y genera un error de la verificación por redundancia cíclica (CRC) o un runt? El Switch reconoce esto solamente cuando recibe el extremo del bastidor y, para entonces, la mayor parte de la trama es puerto de egreso transferido de los. Puesto que no tiene ningún sentido de transferir el resto del bastidor erróneo, se cae el resto, el puerto de egreso incrementa el error del “underrun”, y el puerto de ingreso incrementa al contador de errores correspondiente. Si los puertos de ingreso múltiples son malsanos y su servidor reside en el puerto de egreso, aparece que el segmento del servidor está teniendo el problema, aunque no es.

Para corte-por el Switches L3, mire para los underrruns y, cuando usted los ve, marque todos los puertos de ingreso para los errores.

Software o error de configuración del hardware

El misconfiguration puede hacer un VLA N ser lento. Estos efectos negativos pueden resultar de un VLA N que es oversubscribed o sobrecargado, pero lo más a menudo posible, resultan de un diseño inadecuado o de las configuraciones pasadas por alto. Por ejemplo, un segmento (VLA N)

se puede abrumar fácilmente por el tráfico Multicast (por ejemplo, vídeo o secuencia de audio) si el tráfico Multicast que obliga las técnicas no se configura correctamente en ese VLA N. Tal tráfico Multicast puede afectar a la Transferencia de datos, causando la pérdida del paquete en un VLA N entero para todos los usuarios (e inundando los segmentos de los usuarios que no se prepusieron recibir las secuencias de multidifusión).

Bug de software y problemas de hardware

Los bug de software y los problemas de hardware son difíciles de identificar porque causan la desviación, que es dura de resolver problemas. Si usted cree que el problema es causado por un bug de software o un problema de hardware, entre en contacto a los ingenieros de soporte técnico de Cisco para tenerlos investigar el problema.

Resuelva problemas la Conectividad lenta del interVLAN

Antes de resolver problemas la Conectividad lenta del interVLAN (entre los VLA N), investigue y elimine los problemas discutidos en los problemas del dominio de colisión del Troubleshooting y resuelva problemas las secciones lentas del IntraVLAN (dominio de broadcast) de este documento.

La mayor parte del tiempo, la Conectividad lenta del interVLAN es causada por la configuración errónea del usuario. Por ejemplo, si usted configuró incorrectamente MLS o el Multicast Multilayer Switching (MMLS), después el reenvío de paquete es hecho por CPU del router, que es una trayectoria lenta. Para evitar el misconfiguration y resolverlo problemas eficientemente cuando sea necesario, usted debe entender el mecanismo usado por su dispositivo de reenvío L3. En la mayoría de los casos, el mecanismo de reenvío L3 se basa en una compilación de la encaminamiento y de las tablas del Address Resolution Protocol (ARP) y la información extraída programada del reenvío de paquete en el hardware (accesos directos). Cualquier error en curso de accesos directos programados lleva al reenvío de paquete del software (una trayectoria lenta), a misforwarding (expedición a un puerto incorrecto), o al agujero negro de tráfico.

Generalmente un error acceso directo-programado o la creación de accesos directos incompletos (que pueden también llevar al software el reenvío de paquete, misforwarding, o el agujero negro de tráfico) es el resultado de un bug de software. Si usted sospecha esto para ser caso, tenga los ingenieros de soporte técnico de Cisco investigarlo. Otras razones del envío lento del interVLAN incluyen los Malos funcionamientos de hardware, no obstante estas causas están fuera del ámbito de este documento. Los Malos funcionamientos de hardware previenen simplemente creación exitosa de acceso directo en hardware y, por lo tanto, el tráfico puede tomar una trayectoria lenta (del software) o puede ser negro agujereado. Los Malos funcionamientos de hardware se deben manejar por los ingenieros de soporte técnico de Cisco, también.

Si usted es que el equipo está configurado correctamente, solamente Hardware Switching seguro no está ocurriendo, después un bug de software o un Mal funcionamiento de hardware puede ser la causa. Sin embargo, sea consciente de las capacidades del dispositivo antes de formar esta conclusión.

Los siguientes son las dos situaciones más frecuentes de cuando el hardware que reenvía puede cesar o no ocurrir en absoluto:

- Se agota la memoria que salva los accesos directos. Una vez que la memoria es llena, el software cesa generalmente más lejos creación de acceso directo. (Por ejemplo, MLS, si basado en el reenvío expreso del Netflow o de Cisco, llega a estar inactivo una vez que no

hay sitio para los nuevos accesos directos, y él conmuta al [slow path] del software.)
- El equipo no se diseña para realizar el Hardware Switching, sino que no es obvio. Por ejemplo, los motores III del supervisor de las Catalyst 4000 Series y posterior son solamente tráfico IP hardware-delantero diseñado; el resto de los tipos de tráfico son software procesado por el CPU. Otro ejemplo es la configuración de un Access Control List (ACL) que requiere la intervención del CPU (por ejemplo, con la opción del “registro”). El tráfico que se aplica a esta regla es procesado por el CPU en el software.

Los errores de ingreso en a corte-por el Switch pueden también contribuir a la lentitud del InterVLAN Routing. Corte-por el Switches utilice los mismos principios de arquitectura para remitir el tráfico L3 y L2, así que los métodos de Troubleshooting proporcionados en la sección resuelven problemas el IntraVLAN lento (dominio de broadcast), arriba, se pueden aplicar al tráfico L2, también.

Otro tipo de misconfiguration que afecta al InterVLAN Routing es misconfiguration en los dispositivos del usuario final (tales como el PC y las impresoras). Una situación común es un PC mal configurado; por ejemplo, se configura mal un default gateway, la tabla ARP PC es inválida, o el cliente IGMP funcionó incorrectamente. Un caso común es cuando hay routeres múltiples o dispositivos encaminamiento-capaces, y configuran mal algo o a todo el usuario final PC para utilizar el default gateway incorrecto. Éste puede ser el caso más molesto, pues todos los dispositivos de red son configurados y trabajando correctamente, sin embargo, los dispositivos del usuario final no los utilizan debido a este misconfiguration.

Si un dispositivo en la red es un router normal que no tiene ningún tipo de aceleración por hardware (y no participa en el Netflow MLS), después el índice de reenvío de tráfico depende totalmente de la velocidad del CPU y cómo está ocupado es. CPU elevada la utilización afecta definitivamente a la velocidad de reenvío. En el Switches L3, sin embargo, CPU elevada las condiciones no afectan necesariamente a la velocidad de reenvío; CPU elevada la utilización afecta a la capacidad del CPU de crear (programa) un acceso directo por hardware. Si el acceso directo está instalado ya en el hardware, después incluso si el CPU se utiliza altamente, el tráfico (para el acceso directo programado) se conmuta en hardware hasta que el acceso directo se envejezca hacia fuera (si hay un temporizador de vencimiento) o quitado por el CPU. Sin embargo, si configuran a un router para cualquier tipo de aceleración del software (tal como transferencia rápida o Cisco Express Forwarding Switching), después el reenvío de paquete se puede afectar por los accesos directos del software; si un acceso directo está quebrado, o el mecanismo sí mismo está fallando, después en vez de la velocidad de reenvío que es acelerada, el tráfico se lleva en batea al CPU, reduciendo la tarifa del 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