Captura VACL para la análisis del tráfico granular con el Cisco Catalyst 6000/6500 Cisco IOS Software corriente

Contenido

Introducción

Este documento suministra una configuración de ejemplo para el uso de la función Capture Port de Lista de Control de Acceso (ACL) de VLAN (VACL) para el análisis del tráfico de la red de una manera más granular. Este documento también explica la ventaja del uso de Capture Port de VACL frente al uso de SPAN basado en VLAN (VSPAN).

Para configurar la característica del captura-puerto VACL en eso del Cisco Catalyst 6000/6500 funciona con el software OS Catalyst, refiere a la captura VACL para la análisis del tráfico granular con el Cisco Catalyst 6000/6500 software CatOS corriente.

prerrequisitos

Requisitos

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Listas de acceso por IP: refiera a configurar las listas de acceso por IP para más información.
- LAN virtual: refiera al LAN virtuales/VLAN Trunking Protocol (VLANs/VTP) - Introducción para más información.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware. Cisco Catalyst 6506 Series Switch que funciona con la versión 12.2(18)SXF8 del Cisco IOS ® Software.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Productos Relacionados

Esta configuración se puede también utilizar con el Cisco Catalyst 6000/6500 Series Switch que funciona con el Cisco IOS Software Release 12.1(13)E y Posterior.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Antecedentes

SPAN basado VLA N

ATRAVIESE las copias (del Switched Port Analyzer) trafican de uno o más puertos de origen en cualquier VLA N o de uno o más VLA N a un puerto destino para el análisis. El SPAN local soporta los puertos de origen, los VLA N de la fuente, y los puertos destino en el mismo Catalyst 6500 Series Switch.

Un VLA N de la fuente es un VLA N monitoreado para el análisis de tráfico de la red. El SPAN VLAN basado (VSPAN) utiliza un VLA N como la fuente del SPAN. Todos los puertos en los VLA N de la fuente se convierten en puertos de origen. Un puerto de origen es un puerto monitoreado para el análisis de tráfico de la red. Los puertos troncales se pueden configurar como puertos de origen y mezclar con los puertos de origen del nontrunk, pero el SPAN no copia la encapsulación de un puerto troncal de la fuente.

Para las sesiones VSPAN con el ingreso y la salida configurados, dos paquetes se remiten del puerto destino si los paquetes consiguen conmutados en el mismo VLA N (uno que el Tráfico de ingreso del puerto de ingreso y uno como tráfico de salida del puerto de egreso).

El VSPAN monitorea solamente el tráfico que deja o ingresa la capa 2 puertos en el VLA N.

- Si usted configura un VLA N como fuente del ingreso y el tráfico consigue ruteado en el VLA N monitoreado, el tráfico ruteado no se monitorea porque nunca aparece como Tráfico de

ingreso que ingrese un puerto de la capa 2 en el VLA N.
- Si usted configura un VLA N como fuente de la salida y el tráfico consigue el VLA N monitoreado de los ruteado, el tráfico ruteado no se monitorea porque nunca aparece como tráfico de salida que salga de un puerto de la capa 2 en el VLA N.

Para más información sobre los VLA N de la fuente, refiera a las características del VLA N de la fuente.

VLA N ACL

Los VACL pueden proporcionar el control de acceso para todos los paquetes que se interliguen dentro de un VLA N o en los cuales se ruteen o fuera de un VLA N o de una interfaz de WAN para la captura VACL. El estándar o los ACL ampliados del Cisco IOS del distinto a lo regular que se configuran en las interfaces del router solamente y se aplican en los paquetes ruteados solamente, los VACL se aplica a todos los paquetes y se puede aplicar a cualquier VLA N o interfaz de WAN. Los VACL se procesan en hardware. Cisco IOS ACL del uso VACL. Los VACL ignoran cualquier campo del Cisco IOS ACL que no se soporte en hardware.

Usted puede configurar los VACL para el IP, el IPX, y el tráfico de la Capa MAC. VACL aplicados al tráfico IP del soporte de las interfaces de WAN solamente para la captura VACL.

Cuando usted configura un VACL y lo aplica a un VLA N, todos los paquetes que ingresan el VLA N se marcan contra este VACL. Si usted aplica un VACL al VLA N y un ACL a una interfaz ruteada en el VLA N, un paquete que entra en el VLA N primero se marca contra el VACL y, si está permitido, en seguida se marca contra la entrada ACL antes de que sea manejado por la interfaz ruteada. Cuando el paquete se rutea a otro VLA N, primero se marca contra el ACL de salida que se aplica a la interfaz ruteada, y, si está permitido, el VACL configurado para el VLAN de destino es aplicado. Si un VACL se configura para un tipo de paquete y un paquete de ese tipo no hace juego el VACL, la acción predeterminada es niega. Éstas son las guías de consulta para la opción de la captura en el VACL.

- El puerto de la captura no puede ser un puerto ATM.
- El puerto de la captura necesita estar en el estado de reenvío del atravesar-árbol para el VLA N.
- El Switch no tiene ninguna restricción en el número de puertos de la captura.
- El puerto de la captura captura solamente los paquetes permitidos por el ACL configurado.
- Los puertos de la captura transmiten solamente el tráfico que pertenece al puerto VLAN de la captura. Configure el puerto de la captura como trunk que lleve los VLA N requeridos para capturar el tráfico que va a muchos VLA N.

Precaución: La combinación incorrecta de ACL puede interrumpir el flujo de tráfico. Ejercite la precaución adicional mientras que usted configura los ACL en su dispositivo.

Nota: El VACL no se soporta con el IPv6 en un Catalyst 6000 Series Switch. Es decir el VLA N ACL reorienta y el IPv6 no es compatible así que el ACL no se puede utilizar para hacer juego el tráfico del IPv6.

Ventajas del uso VACL sobre el uso VSPAN

Hay varias limitaciones del uso VSPAN para la análisis del tráfico:

- Todos acodan el tráfico 2 que los flujos en un VLA N se capturan. Esto aumenta la cantidad

de datos que se analizarán.
- Las cantidades de sesión de SPAN que pueden ser configuradas en los Catalyst 6500 Series Switch son limitadas. Refiera a los límites del SPAN local y de la sesión de RSPAN para más información.
- Un puerto de destino recibe copias del tráfico enviado y recibido para todos los puertos de origen monitoreados. Si un puerto de destino tiene exceso de suscriptores, puede congestionarse. Esta congestión puede afectar al reenvío de tráfico en uno o más de los puertos de origen.

La característica del puerto de la captura VACL puede ayudar a superar algunas de estas limitaciones. Los VACL no se diseñan sobre todo para monitorear el tráfico, pero, con una amplia gama de capacidad para clasificar el tráfico, la característica del puerto de la captura fue introducida de modo que el análisis de tráfico de la red pueda llegar a ser mucho más simple. Éstas son las ventajas del uso del puerto de la captura VACL sobre el VSPAN:

- Análisis del tráfico granularLos VACL pueden hacer juego basado en la dirección IP de origen, IP Address de destino, acodan los 4 Tipo de protocolo, los puertos de la fuente y de la capa de destino 4, y la otra información. Esta capacidad hace los VACL muy útiles para la identificación y la filtración granulares del tráfico.
- Número de sesionesLos VACL se aplican en hardware; el número de entradas de control de acceso (ACE) que puedan ser creadas depende del TCAM disponible en el Switches.
- Oversubscription del puerto destinoLa identificación granular del tráfico reduce el número de bastidores que se remitirán al puerto destino y de tal modo minimiza la probabilidad de su oversubscription.
- RendimientoLos VACL se aplican en hardware; no hay multa de rendimiento para la aplicación de los VACL a un VLA N en los Cisco Catalyst 6500 Series Switch

Configurar

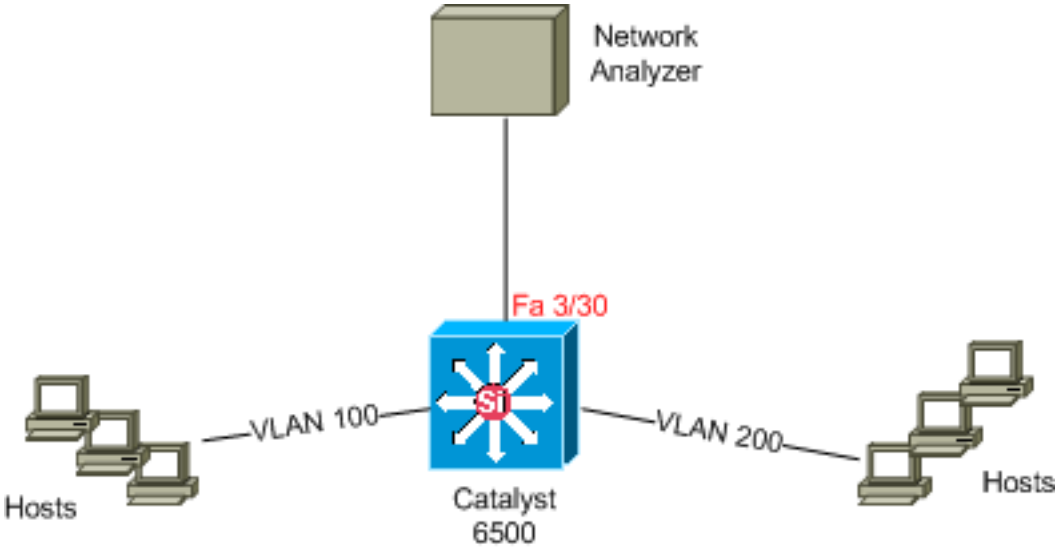
En esta sección encontrará la información para configurar las funciones descritas en este documento.

- El configurar con el SPAN basado VLA N
- El configurar con el VACL

Nota: Use la herramienta Command Lookup Tool (clientes registrados solamente) para encontrar más información sobre los comandos usados en este documento.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Configuración con el SPAN VLAN basado

Este ejemplo de configuración enumera los pasos requeridos para capturar todo el tráfico de la capa 2 que los flujos en el VLAN 100 y el VLA N 200 y les envíen al dispositivo del analizador de red.

1. Especifique el tráfico interesante. En nuestro ejemplo, es el tráfico que fluye en el VLAN 100 y el VLA N 200.`Cat6K-IOS#conf t Cat6K-IOS(config)#`**`monitor session`** *`50`* **`source vlan`** *`100 , 200`* **`?`** `, Specify another range of VLANs - Specify a range of VLANs both Monitor received and transmitted traffic rx Monitor received traffic only tx Monitor transmitted traffic only <cr>` *`!--- Default is to monitor`* ***`both`*** *`received and transmitted traffic`* `Cat6K-IOS(config)#`**`monitor session`** *`50`* **`source vlan`** *`100 , 200`* `Cat6K-IOS(config)#`
2. Especifique el puerto destino para el tráfico capturado.`Cat6K-IOS(config)#`**`monitor session`** *`50`* **`destination`** *`interface Fa3/30`* `Cat6K-IOS(config)#`

Con esto, todo el tráfico de la capa 2 que pertenece al VLAN 100 y al VLA N 200 se copia y se envía para virar Fa3/30 hacia el lado de babor. Si el puerto destino es parte del mismo VLA N cuyo se monitorea tráfico, el tráfico que sale del puerto destino no se captura.

Verifique su configuración de SPAN con el **comando show monitor**.

```
Cat6K-IOS#show monitor detail Session 50 ---------- Type : Local Session Source Ports : RX Only
: None TX Only : None Both : None Source VLANs : RX Only : None TX Only : None Both : 100,200
Source RSPAN VLAN : None Destination Ports : Fa3/30 Filter VLANs : None Dest RSPAN VLAN : None
```

Configuración con el VACL

En este ejemplo de configuración, hay requisitos múltiples del administrador de la red:

- El tráfico HTTP de un rango de los host (10.20.20.128/25) en el VLA N 200 a un servidor específico (10.10.10.101) en el VLAN 100 necesita ser capturado.
- El tráfico del User Datagram Protocol (UDP) del Multicast en la dirección de transmisión destinada para el grupo de dirección 239.0.0.100 necesita ser capturado del VLAN 100.

1. Defina el tráfico interesante que se caputured y enviado al análisis.`Cat6K-IOS(config)#`**`ip access-list extended`** *`HTTP_UDP_TRAFFIC`* `Cat6K-IOS(config-ext-nacl)#`**`permit tcp`** *`10.20.20.128 0.0.0.127`* **`host`** *`10.10.10.101`* **`eq www`** `Cat6K-IOS(config-ext-nacl)#`**`permit udp any host`** *`239.0.0.100`* `Cat6K-IOS(config-ext-nacl)#exit`
2. Defina un umberlla ACL para asociar el resto del tráfico.`Cat6K-IOS(config)#`**`ip access-list`**

extended *ALL_TRAFFIC* Cat6K-IOS(config-ext-nacl)#**permit ip any any** Cat6K-IOS(config-ext-nacl)#**exit**

3. Defina la correspondencia del acceso de VLAN.Cat6K-IOS(config)#**vlan access-map** *HTTP_UDP_MAP 10* Cat6K-IOS(config-access-map)#**match ip address** *HTTP_UDP_TRAFFIC* Cat6K-IOS(config-access-map)#**action forward capture** Cat6K-IOS(config)#**vlan access-map** *HTTP_UDP_MAP 20* Cat6K-IOS(config-access-map)#**match ip address** *ALL_TRAFFIC* Cat6K-IOS(config-access-map)#**action forward** Cat6K-IOS(config-access-map)#exit
4. Aplique la correspondencia del acceso de VLAN a los VLA N apropiados.Cat6K-IOS(config)#**vlan filter** *HTTP_UDP_MAP* **vlan-list** *100 !--- Here 100 is the ID of VLAN on which the VACL is applied.*
5. Configure el puerto de la captura.Cat6K-IOS(config)#**int fa3/30** Cat6K-IOS(config-if)#**switchport capture allowed vlan** *?* WORD VLAN IDs of the allowed VLANs when this po add add VLANs to the current list all all VLANs except all VLANs except the following remove remove VLANs from the current list Cat6K-IOS(config-if)#**switchport capture allowed vlan** *100* Cat6K-IOS(config-if)#**switchport capture** Cat6K-IOS(config-if)#exit

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

- **muestre el acceso-mapa vlan** — Visualiza el contenido de las correspondencias del acceso de VLAN.Cat6K-IOS#**show vlan access-map** *HTTP_UDP_MAP* Vlan access-map "HTTP_UDP_MAP" 10 match: ip address HTTP_UDP_TRAFFIC action: forward capture Vlan access-map "HTTP_UDP_MAP" 20 match: ip address ALL_TRAFFIC action: forward
- **muestre el filtro vlan** — Visualiza la información sobre los filtros del VLA N.Cat6K-IOS#**show vlan filter** VLAN Map HTTP_UDP_MAP: Configured on VLANs: 100 Active on VLANs: 100

Troubleshooting

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Información Relacionada

- Captura VACL para la análisis del tráfico granular con el Cisco Catalyst 6000/6500 software CatOS corriente
- Soporte de los Cisco Catalyst 6500 Series Switch
- Soporte de Producto de LAN
- Soporte de Tecnología de LAN Switching
- Soporte Técnico y Documentación - Cisco Systems