Verificación de infracciones de políticas del plano de control en plataformas Nexus

Contenido

Introducción

Este documento describe los detalles sobre Control Plane Policing (CoPP) en los switches Cisco Nexus y su impacto relevante en las violaciones de clase no predeterminadas.

Prerequisites

Cisco recomienda que comprenda la información básica con respecto a la política de plano de control (CoPP), sus directrices y limitaciones, y la configuración general, así como la funcionalidad de la política de calidad de servicio (QoS) (CIR). Para obtener más información sobre esta función, consulte los documentos correspondientes:

- Guía de configuración de seguridad de NX-OS para Cisco Nexus serie 9000, versión 10.2(x)
- CoPP en los switches Nexus de la serie 7000
- Guía de configuración de la calidad de servicio de Cisco Nexus serie 9000 NX-OS, versión 10.2(x)

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

Este documento no se limita a requisitos específicos de software y hardware.

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 tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

El tráfico del plano de control se redirige hacia el módulo supervisor mediante listas de control de acceso (ACL) de redirección programadas para dirigir el tráfico coincidente que pasa a través de dos capas de protección, los limitadores de velocidad de hardware y la CoPP. Cualquier interrupción o ataque al módulo supervisor, si no se controla, puede provocar graves interrupciones en la red; por lo tanto, CoPP está ahí para servir como mecanismo de protección. Si hay inestabilidad en el nivel del plano de control, es importante verificar la CoPP, porque los patrones de tráfico anormales creados a partir de loops o inundaciones, o los dispositivos no autorizados pueden aplicar impuestos y evitar que el supervisor procese tráfico legítimo. Estos ataques, que pueden ser perpetrados de forma inadvertida por dispositivos desconocidos o de forma malintencionada por atacantes, suelen implicar altas tasas de tráfico destinado al módulo supervisor o a la CPU.

La política de plan de control (CoPP) es una función que clasifica y controla todos los paquetes recibidos a través de los puertos en banda (panel frontal) destinados a la dirección del router o que requieren la intervención de un supervisor. Esta función permite aplicar un mapa de política al plano de control. Este mapa de política parece una política de calidad de servicio (QoS) normal y se aplica a todo el tráfico que entra en el switch desde un puerto no de administración. La protección del módulo supervisor mediante la regulación de tráfico permite que el switch mitigue las saturaciones de tráfico que superan la velocidad de entrada comprometida (CIR) para cada clase mediante el descarte de paquetes para evitar que el switch se sobrecargue y, por lo tanto, repercuta en el rendimiento.

Es importante monitorear los contadores CoPP continuamente y justificarlos, que es el propósito de este documento. Las infracciones de CoPP, si no se controlan, pueden impedir que el plano de control procese tráfico genuino en la clase afectada asociada. La configuración CoPP es un proceso fluido y continuo que debe responder a los requisitos de la red y la infraestructura. Existen tres políticas de sistema predeterminadas para CoPP. De forma predeterminada, Cisco recomienda el uso de la política predeterminada strict como punto inicial y se utiliza como base para este documento.

La CoPP solo se aplica al tráfico en banda recibido a través de los puertos del panel frontal. El puerto de administración fuera de banda (mgmt0) no está sujeto a CoPP. El hardware del dispositivo Cisco NX-OS realiza la CoPP por motor de reenvío. Por lo tanto, elija velocidades para que el tráfico agregado no sobrecargue el módulo supervisor. Esto es especialmente importante para los switches modulares/de final de la fila, ya que la

CIR se aplica al tráfico agregado de todos los módulos de tráfico dirigido a la CPU.

Hardware aplicable

El componente tratado en este documento se aplica a todos los switches de Data Center Cisco Nexus.

Interpretación de políticas del plano de control

El objetivo de este documento es abordar las violaciones de clase no predeterminadas más comunes y críticas observadas en los switches Nexus.

Perfil predeterminado de CoPP estándar

Para comprender cómo interpretar la CoPP, la primera verificación debe ser garantizar que se aplica un perfil y comprender si se aplica un perfil predeterminado o un perfil personalizado en el switch.

Nota: como práctica recomendada, todos los switches Nexus deben tener activada la función CoPP. Si esta función no está habilitada, puede causar inestabilidad para todo el tráfico del plano de control, ya que diferentes plataformas pueden restringir el tráfico enlazado al supervisor (SUP). Por ejemplo, si no se habilita CoPP en un Nexus 9000, el tráfico destinado al SUP está limitado a una velocidad de 50 pps, por lo que el switch se vuelve prácticamente inoperativo. CoPP se considera un requisito en las plataformas Nexus 3000 y Nexus 9000.

Si no se habilita CoPP, se puede volver a habilitar o configurar en el switch mediante el uso del **setup** comando o mediante la aplicación de una de las políticas predeterminadas estándar en la opción de configuración: copp profile [dense|lenient|moderate|strict].

Un dispositivo no protegido no clasifica y segrega correctamente el tráfico en clases y, por lo tanto, cualquier comportamiento de denegación de servicio para una función o protocolo específico no se limita a ese ámbito y puede afectar a todo el plano de control.

Nota: las políticas de CoPP se implementan mediante redirecciones de clasificación de Memoria direccionable por contenido ternario (TCAM) y se pueden ver directamente en **show system internal access-list input statistics module X | b CoPP** o **show hardware access-list input entries detail**.

N9K1# show copp status Last Config Operation: None Last Config Operation Timestamp: None Last Config Operation Status: None Policy-map attached t

Clases de políticas del plano de control

CoPP clasifica el tráfico en función de las coincidencias que corresponden a las ACL IP o MAC; por lo tanto, es importante comprender qué tráfico se clasifica en qué clase.

Las clases, que dependen de la plataforma, pueden variar. Por lo tanto, es importante entender cómo verificar las clases.

Por ejemplo, en la parte superior del rack (TOR) de Nexus 9000:

```
N9K1# show policy-map interface control-plane
Control Plane

Service-policy input: copp-system-p-policy-strict
...
class-map copp-system-p-class-critical (match-any)
match access-group name copp-system-p-acl-bgp
match access-group name copp-system-p-acl-rip
match access-group name copp-system-p-acl-vpc
match access-group name copp-system-p-acl-bgp6
match access-group name copp-system-p-acl-ospf
match access-group name copp-system-p-acl-rip6
match access-group name copp-system-p-acl-eigrp
match access-group name copp-system-p-acl-ospf6
match access-group name copp-system-p-acl-eigrp6
match access-group name copp-system-p-acl-auto-rp
match access-group name copp-system-p-acl-mac-l3-isis
set cos 7
police cir 36000 kbps , bc 1280000 bytes
module 1 :
transmitted 177446058 bytes;
5-minute offered rate 3 bytes/sec
conformed 27 peak-rate bytes/sec
at Sat Apr 23 04:25:27 2022

dropped 0 bytes;
5-min violate rate 0 byte/sec
violated 0 peak-rate byte/sec
...
```

En este ejemplo, el mapa de clase copp-system-p-class-critical engloba el tráfico relacionado con los protocolos de routing, como el protocolo de gateway fronterizo (BGP), la ruta de acceso más corta primero (OSPF) y el protocolo de router de gateway interior mejorado (EIGRP), e incluye otros protocolos, como vPC.

La convención de nombres de ACL IP o MAC es mayormente autoexplicativa para el protocolo o función involucrada, con el prefijo copp-system-p-acl-[protocol|feature].

Para ver una clase específica, se puede especificar directamente mientras se ejecuta el comando **show**. Por ejemplo:

```
N9K-4# show policy-map interface control-plane class copp-system-p-class-management
Control Plane

Service-policy input: copp-system-p-policy-strict

class-map copp-system-p-class-management (match-any)
match access-group name copp-system-p-acl-ftp
match access-group name copp-system-p-acl-ntp
```

match access-group name copp-system-p-acl-ssh
match access-group name copp-system-p-acl-http
match access-group name copp-system-p-acl-ntp6
match access-group name copp-system-p-acl-sftp
match access-group name copp-system-p-acl-snmp
match access-group name copp-system-p-acl-ssh6
match access-group name copp-system-p-acl-tftp
match access-group name copp-system-p-acl-https
match access-group name copp-system-p-acl-snmp6
match access-group name copp-system-p-acl-tftp6
match access-group name copp-system-p-acl-radius
match access-group name copp-system-p-acl-tacacs
match access-group name copp-system-p-acl-telnet
match access-group name copp-system-p-acl-radius6
match access-group name copp-system-p-acl-tacacs6
match access-group name copp-system-p-acl-telnet6
set cos 2
police cir 36000 kbps , bc 512000 bytes
module 1 :
transmitted 0 bytes;
5-minute offered rate 0 bytes/sec
conformed 0 peak-rate bytes/sec

dropped 0 bytes;
5-min violate rate 0 byte/sec
violated 0 peak-rate byte/sec

Mientras que los perfiles predeterminados de CoPP normalmente están ocultos como parte de la configuración predeterminada, puede ver la configuración con **show running-conf copp all**:

<#root>

N9K1# show running-config copp all

!Command: show running-config copp all
!Running configuration last done at: Tue Apr 26 16:34:10 2022
!Time: Sun May 1 16:41:55 2022

version 10.2(1) Bios:version 05.45
control-plane
scale-factor 1.00 module 1
class-map type control-plane match-any copp-system-p-class-critical
match access-group name

copp-system-p-acl-bgp

match access-group name copp-system-p-acl-rip
match access-group name copp-system-p-acl-vpc
match access-group name copp-system-p-acl-bgp6
match access-group name copp-system-p-acl-ospf
match access-group name copp-system-p-acl-rip6
match access-group name copp-system-p-acl-eigrp
match access-group name copp-system-p-acl-ospf6

```
match access-group name copp-system-p-acl-eigrp6
match access-group name copp-system-p-acl-auto-rp
match access-group name copp-system-p-acl-mac-l3-isis
(snip)
...
```

El mapa de clase copp-system-p-class-critical, visto antes, hace referencia a múltiples sentencias de coincidencia que llaman a las ACL del sistema, que de forma predeterminada están ocultas, y hacen referencia a la clasificación que se compara. Por ejemplo, para BGP:

<#root>

N9K1# show running-config aclmgr all | b

copp-system-p-acl-bgp

```
ip access-list
```

copp-system-p-acl-bgp

```
10 permit tcp any gt 1023 any eq bgp
20 permit tcp any eq bgp any gt 1023
(snip)
```

Esto significa que cualquier tráfico BGP coincide con esta clase y se clasifica en copp-system-p-class-critical, junto con todos los demás protocolos en la misma clase.

Nexus 7000 utiliza una estructura de funciones de CoPP muy similar a la de Nexus 9000:

N77-A-Admin# show policy-map interface control-plane
Control Plane
service-policy input copp-system-p-policy-strict

class-map copp-system-p-class-critical (match-any)
match access-group name copp-system-p-acl-bgp
match access-group name copp-system-p-acl-rip
match access-group name copp-system-p-acl-vpc
match access-group name copp-system-p-acl-bgp6
match access-group name copp-system-p-acl-lisp
match access-group name copp-system-p-acl-ospf
match access-group name copp-system-p-acl-rip6
match access-group name copp-system-p-acl-rise
match access-group name copp-system-p-acl-eigrp
match access-group name copp-system-p-acl-lisp6
match access-group name copp-system-p-acl-ospf6
match access-group name copp-system-p-acl-rise6
match access-group name copp-system-p-acl-eigrp6
match access-group name copp-system-p-acl-otv-as
match access-group name copp-system-p-acl-mac-l2pt

```
match access-group name copp-system-p-acl-mpls-ldp
match access-group name copp-system-p-acl-mpls-rsvp
match access-group name copp-system-p-acl-mac-l3-isis
match access-group name copp-system-p-acl-mac-otv-isis
match access-group name copp-system-p-acl-mac-fabricpath-isis
match protocol mpls router-alert
set cos 7
police cir 36000 kbps bc 250 ms
conform action: transmit
violate action: drop
module 1:
conformed 300763871 bytes,
5-min offered rate 132 bytes/sec
peak rate 125 bytes/sec at Sun May 01 09:50:51 2022
violated 0 bytes,
5-min violate rate 0 bytes/sec
peak rate 0 bytes/sec
module 2:
conformed 4516900216 bytes,
5-min offered rate 1981 bytes/sec
peak rate 1421 bytes/sec at Fri Apr 29 15:40:40 2022
violated 0 bytes,
5-min violate rate 0 bytes/sec
peak rate 0 bytes/sec
module 6:
conformed 0 bytes,
5-min offered rate 0 bytes/sec
peak rate 0 bytes/sec
violated 0 bytes,
5-min violate rate 0 bytes/sec
peak rate 0 bytes/sec
```

Es importante tener en cuenta que en un Nexus 7000, como se trata de switches modulares, la clase se divide por módulo; sin embargo, la CIR se aplica a la suma de todos los módulos y la CoPP se aplica a todo el chasis. La verificación CoPP y las salidas solo se pueden ver desde el contexto de dispositivo virtual (VDC) predeterminado o de administración.

Es especialmente importante verificar la CoPP en un Nexus 7000 si se observan problemas en el plano de control, ya que la inestabilidad en un VDC con tráfico excesivamente dirigido a la CPU que causa violaciones de CoPP puede afectar la estabilidad de otros VDC.

En un Nexus 5600, las clases varían. Por lo tanto, para BGP es su propia clase separada:

```
N5K# show policy-map interface control-plane
Control Plane
(snip)
class-map copp-system-class-bgp (match-any)
match protocol bgp
police cir 9600 kbps , bc 4800000 bytes
conformed 1510660 bytes; action: transmit
violated 0 bytes;
(snip)
```

En un Nexus 3100, hay 3 clases de protocolo de routing, por lo que para verificar a qué clase pertenece el BGP, haga referencia cruzada a las 4 ACL CoPP a las que se hace referencia:

EIGRP es gestionado por su propia clase en el Nexus 3100.

<#root>

N3K-C3172# show policy-map interface control-plane
Control Plane

service-policy input: copp-system-policy

class-map copp-s-routingProto2 (match-any)
match access-group name copp-system-acl-routingproto2
police pps 1300
OutPackets 0
DropPackets 0
class-map copp-s-v6routingProto2 (match-any)
match access-group name copp-system-acl-v6routingProto2
police pps 1300
OutPackets 0
DropPackets 0
class-map copp-s-eigrp (match-any)
match access-group name copp-system-acl-eigrp
match access-group name copp-system-acl-eigrp6
police pps 200
OutPackets 0
DropPackets 0
class-map copp-s-routingProto1 (match-any)
match access-group name

copp-system-acl-routingproto1

match access-group name copp-system-acl-v6routingproto1
police pps 1000
OutPackets 0
DropPackets 0

N3K-C3172# show running-config aclmgr

!Command: show running-config aclmgr
!No configuration change since last restart
!Time: Sun May 1 18:14:16 2022

version 9.3(9) Bios:version 5.3.1
ip access-list copp-system-acl-eigrp
10 permit eigrp any 224.0.0.10/32
ipv6 access-list copp-system-acl-eigrp6
10 permit eigrp any ff02::a/128
ip access-list

copp-system-acl-routingproto1

10 permit tcp any gt 1024 any eq bgp

```
20 permit tcp any eq bgp any gt 1024


30 permit udp any 224.0.0.0/24 eq rip
40 permit tcp any gt 1024 any eq 639
50 permit tcp any eq 639 any gt 1024
70 permit ospf any any
80 permit ospf any 224.0.0.5/32
90 permit ospf any 224.0.0.6/32
ip access-list copp-system-acl-routingproto2
10 permit udp any 224.0.0.0/24 eq 1985
20 permit 112 any 224.0.0.0/24
ipv6 access-list copp-system-acl-v6routingProto2
10 permit udp any ff02::66/128 eq 2029
20 permit udp any ff02::fb/128 eq 5353
30 permit 112 any ff02::12/128
ipv6 access-list copp-system-acl-v6routingproto1
10 permit 89 any ff02::5/128
20 permit 89 any ff02::6/128
30 permit udp any ff02::9/128 eq 521
```

En este caso, BGP es igualado por la ACL copp-system-acl-routingproto1, y por lo tanto la clase CoPP BGP cae en is copp-s-routingProto1.

Estadísticas y contadores de políticas del plano de control

CoPP admite estadísticas de QoS para realizar un seguimiento de los contadores agregados de tráfico que confirman o infringen la velocidad de entrada comprometida (CIR) para una clase determinada, para cada módulo.

Cada mapa de clase clasifica el tráfico enlazado a la CPU, en función de la clase a la que corresponde, y adjunta una CIR para todos los paquetes incluidos en esa clasificación. Por ejemplo, la clase que se relaciona con el tráfico BGP se utiliza como referencia:

En una parte superior del rack (TOR) de Nexus 9000 para copp-system-p-class-critical:

<#root>

class-map copp-system-p-class-critical (match-any)
match access-group name

copp-system-p-acl-bgp

```
match access-group name copp-system-p-acl-rip
match access-group name copp-system-p-acl-vpc
match access-group name copp-system-p-acl-bgp6
match access-group name copp-system-p-acl-ospf
match access-group name copp-system-p-acl-rip6
match access-group name copp-system-p-acl-eigrp
match access-group name copp-system-p-acl-ospf6
match access-group name copp-system-p-acl-eigrp6
match access-group name copp-system-p-acl-auto-rp
match access-group name copp-system-p-acl-mac-l3-isis
set cos 7
police cir 36000 kbps , bc 1280000 bytes
```

```
module 1 :
transmitted 177446058 bytes;
5-minute offered rate 3 bytes/sec
conformed 27 peak-rate bytes/sec
at Sat Apr 23 04:25:27 2022

dropped 0 bytes;
5-min violate rate 0 byte/sec
violated 0 peak-rate byte/sec
```

En la sección del mapa de clase, después de las sentencias match, verá las acciones que se relacionan con todo el tráfico dentro de la clase. Todo el tráfico clasificado en copp-system-p-class-critical se establece con una clase de servicio (CoS) de 7, que es el tráfico de mayor prioridad, y esta clase se controla con una CIR de 36000 kbps y una velocidad de ráfaga comprometida de 1280000 bytes.

El tráfico que se ajusta a esta política se reenvía al SUP para su procesamiento y se descartan las infracciones.

<#root>

set cos 7

police cir 36000 kbps , bc 1280000 bytes

La siguiente sección contiene las estadísticas relacionadas con el módulo. Para los switches de la parte superior del rack (TOR), con un único módulo, el módulo 1 hace referencia al switch.

module 1 :
transmitted 177446058 bytes;
5-minute offered rate 3 bytes/sec
conformed 27 peak-rate bytes/sec
at Sat Apr 23 04:25:27 2022

dropped 0 bytes;
5-min violate rate 0 byte/sec
violated 0 peak-rate byte/sec

Las estadísticas que se ven en el resultado son históricas, por lo que esto proporciona una instantánea de las estadísticas actuales en el momento en que se ejecuta el comando.

Hay dos secciones para interpretar aquí: las secciones transmitidas y eliminadas:
El punto de datos transmitido rastrea todos los paquetes transmitidos que cumplen con la política. Esta sección es importante ya que proporciona información sobre el tipo de tráfico que procesa el supervisor.

El valor de la tarifa ofrecida de 5 minutos proporciona una perspectiva de la tarifa actual.
La velocidad pico conformada y la fecha, proporciona un ajuste de la velocidad pico más alta por segundo que aún se conforma dentro de la política y el tiempo que ocurrió.
Si se observa un nuevo pico, reemplaza este valor y esta fecha.

La parte más importante de las estadísticas es el punto de datoseliminado. Al igual que las estadísticas transmitidas, la sección eliminada realiza un seguimiento de los bytes acumulados eliminados debido a las violaciones a la tasa de policía. También proporciona la tasa de violación de los últimos 5 minutos, el pico violado y, si hay un pico, la marca de tiempo de esa violación pico. Y de nuevo, si se observa un nuevo pico, entonces reemplaza este valor y fecha. En otras plataformas, los resultados varían, pero la lógica es muy similar.

Nexus 7000 utiliza una estructura idéntica y la verificación es la misma, aunque algunas clases varían ligeramente en las ACL a las que se hace referencia:

<#root>

class-map

copp-system-p-class-critical

```
 (match-any)
match access-group name
```

copp-system-p-acl-bgp

```
match access-group name copp-system-p-acl-rip
match access-group name copp-system-p-acl-vpc
match access-group name copp-system-p-acl-bgp6
match access-group name copp-system-p-acl-lisp
match access-group name copp-system-p-acl-ospf
match access-group name copp-system-p-acl-rip6
match access-group name copp-system-p-acl-rise
match access-group name copp-system-p-acl-eigrp
match access-group name copp-system-p-acl-lisp6
match access-group name copp-system-p-acl-ospf6
match access-group name copp-system-p-acl-rise6
match access-group name copp-system-p-acl-eigrp6
match access-group name copp-system-p-acl-otv-as
match access-group name copp-system-p-acl-mac-l2pt
match access-group name copp-system-p-acl-mpls-ldp
match access-group name copp-system-p-acl-mpls-rsvp
match access-group name copp-system-p-acl-mac-l3-isis
match access-group name copp-system-p-acl-mac-otv-isis
match access-group name copp-system-p-acl-mac-fabricpath-isis
match protocol mpls router-alert
```

set cos 7

police cir 36000 kbps bc 250 ms

conform action: transmit

```
violate action: drop
module 1:
conformed 300763871 bytes,
5-min offered rate 132 bytes/sec
peak rate 125 bytes/sec at Sun May 01 09:50:51 2022
violated 0 bytes,
5-min violate rate 0 bytes/sec
peak rate 0 bytes/sec
module 2:
```

```
conformed 4516900216 bytes,
5-min offered rate 1981 bytes/sec
peak rate 1421 bytes/sec at Fri Apr 29 15:40:40 2022
violated 0 bytes,
5-min violate rate 0 bytes/sec
peak rate 0 bytes/sec
module 6:
conformed 0 bytes,
5-min offered rate 0 bytes/sec
peak rate 0 bytes/sec
violated 0 bytes,
5-min violate rate 0 bytes/sec
peak rate 0 bytes/sec
```

En un Nexus 5600:

<#root>

class-map copp-system-class-bgp

(match-any)

match protocol bgp

```
police cir 9600 kbps , bc 4800000 bytes
conformed 1510660 bytes; action: transmit
violated 0 bytes;
```

Aunque no proporciona información sobre la velocidad o los picos, sigue proporcionando los bytes agregados conformados y violados.

En un Nexus 3100, la salida del plano de control muestra OutPackets y DropPackets.

class-map copp-s-routingProto1 (match-any)
match access-group name copp-system-acl-routingproto1
match access-group name copp-system-acl-v6routingproto1
police pps 1000
OutPackets 8732060
DropPackets 0

OutPackets hace referencia a paquetes conformados, mientras que DropPackets hace referencia a violaciones a CIR. En este escenario, no verá descartes en la clase asociada.

En un Nexus 3500, la salida muestra los paquetes coincidentes de hardware y software:

class-map copp-s-routingProto1 (match-any)

match access-group name copp-system-acl-routingproto1
police pps 900
HW Matched Packets 471425
SW Matched Packets 471425

Los paquetes coincidentes de HW hacen referencia a los paquetes que la ACL hace coincidir en HW. Los paquetes coincidentes de SW son los que cumplen con la política. Cualquier diferencia entre los paquetes coincidentes de hardware y software implica una violación.

En este caso, no se observan caídas en los paquetes de clase del protocolo de ruteo 1 (que incluye BGP), ya que los valores coinciden.

Comprobar si hay infracciones de descarte activas

Dado que las estadísticas de regulación del plano de control son históricas, es importante determinar si las violaciones activas están aumentando. La manera estándar de realizar esta tarea es comparar dos salidas completas y verificar cualquier diferencia.

Esta tarea se puede realizar manualmente, o los switches Nexus proporcionan la herramienta de diferencia que puede ayudar a comparar las salidas.

Aunque se puede comparar el resultado completo, no es necesario porque el enfoque está solo en las estadísticas descartadas. Por lo tanto, el resultado de CoPP se puede filtrar para centrarse solo en las infracciones.

El comando es el siguiente: show policy-map interface control-plane | egrep class|module|violated|dropped | diff -y

---

Nota: El comando debe ejecutarse dos veces para que el diff pueda comparar la salida actual con la anterior.

```
N9K-3# show policy-map interface control-plane | egrep class|module|violated|dropped | diff -y
    class-map copp-system-p-class-l3uc-data (match-any)             class-map copp-system-p-class-l3uc-data (match-any)
      module 1 :                                                      module 1 :
        dropped 0 bytes;                                                dropped 0 bytes;
        violated 0 peak-rate byte/sec                                   violated 0 peak-rate byte/sec
    class-map copp-system-p-class-critical (match-any)              class-map copp-system-p-class-critical (match-any)
      module 1 :                                                      module 1 :
        dropped 0 bytes;                                                dropped 0 bytes;
        violated 0 peak-rate byte/sec                                   violated 0 peak-rate byte/sec
    class-map copp-system-p-class-important (match-any)             class-map copp-system-p-class-important (match-any)
      module 1 :                                                      module 1 :
        dropped 0 bytes;                                                dropped 0 bytes;
        violated 0 peak-rate byte/sec                                   violated 0 peak-rate byte/sec
    class-map copp-system-p-class-openflow (match-any)              class-map copp-system-p-class-openflow (match-any)
      module 1 :                                                      module 1 :
        dropped 0 bytes;                                                dropped 0 bytes;
        violated 0 peak-rate byte/sec                                   violated 0 peak-rate byte/sec
    class-map copp-system-p-class-multicast-router (match-any       class-map copp-system-p-class-multicast-router (match-any
      module 1 :                                                      module 1 :
        dropped 0 bytes;                                                dropped 0 bytes;
        violated 0 peak-rate byte/sec                                   violated 0 peak-rate byte/sec
    class-map copp-system-p-class-multicast-host (match-any)        class-map copp-system-p-class-multicast-host (match-any)
      module 1 :                                                      module 1 :
        dropped 0 bytes;                                                dropped 0 bytes;
        violated 0 peak-rate byte/sec                                   violated 0 peak-rate byte/sec
    class-map copp-system-p-class-l3mc-data (match-any)             class-map copp-system-p-class-l3mc-data (match-any)
      module 1 :                                                      module 1 :
        dropped 0 bytes;                                                dropped 0 bytes;
        violated 0 peak-rate byte/sec                                   violated 0 peak-rate byte/sec
    class-map copp-system-p-class-normal (match-any)                class-map copp-system-p-class-normal (match-any)
      module 1 :                                                      module 1 :
        dropped 0 bytes;                                                dropped 0 bytes;
        violated 0 peak-rate byte/sec                                   violated 0 peak-rate byte/sec
    class-map copp-system-p-class-ndp (match-any)                   class-map copp-system-p-class-ndp (match-any)
      module 1 :                                                      module 1 :
        dropped 0 bytes;                                                dropped 0 bytes;
        violated 0 peak-rate byte/sec                                   violated 0 peak-rate byte/sec
    class-map copp-system-p-class-normal-dhcp (match-any)           class-map copp-system-p-class-normal-dhcp (match-any)
      module 1 :                                                      module 1 :
        dropped 0 bytes;                                                dropped 0 bytes;
        violated 0 peak-rate byte/sec                                   violated 0 peak-rate byte/sec
    class-map copp-system-p-class-normal-dhcp-relay-response        class-map copp-system-p-class-normal-dhcp-relay-response
      module 1 :                                                      module 1 :
        dropped 0 bytes;                                                dropped 0 bytes;
        violated 0 peak-rate byte/sec                                   violated 0 peak-rate byte/sec
    class-map copp-system-p-class-normal-igmp (match-any)           class-map copp-system-p-class-normal-igmp (match-any)
      module 1 :                                                      module 1 :
        dropped 0 bytes;                                                dropped 0 bytes;
```

El comando anterior permite ver el delta entre dos clases y encontrar aumentos de infracciones.

Nota: Como las estadísticas de CoPP son históricas, otra recomendación es borrar las estadísticas después de ejecutar el comando, para verificar si hay aumentos activos. Para borrar las estadísticas de CoPP, ejecute el comando: **clear copp statistics**.

Tipos de caídas de CoPP

CoPP es una estructura de regulación de tráfico simple, ya que se descarta cualquier tráfico enlazado a la CPU que viole la CIR. Sin embargo, las implicaciones varían significativamente dependiendo del tipo de caídas.

Aunque la lógica es la misma, no es lo mismo descartar el tráfico destinado a copp-system-p-class-critical.

class-map copp-system-p-class-critical (match-any)
match access-group name copp-system-p-acl-bgp
match access-group name copp-system-p-acl-rip
match access-group name copp-system-p-acl-vpc
match access-group name copp-system-p-acl-bgp6
match access-group name copp-system-p-acl-ospf
match access-group name copp-system-p-acl-rip6
match access-group name copp-system-p-acl-eigrp
match access-group name copp-system-p-acl-ospf6
match access-group name copp-system-p-acl-eigrp6
match access-group name copp-system-p-acl-auto-rp
match access-group name copp-system-p-acl-mac-l3-isis
set cos 7
police cir 36000 kbps , bc 1280000 bytes

Comparado con tráfico descartado destinado a class-map copp-system-p-class-monitoring.

class-map copp-system-p-class-monitoring (match-any)
match access-group name copp-system-p-acl-icmp
match access-group name copp-system-p-acl-icmp6
match access-group name copp-system-p-acl-traceroute
set cos 1
police cir 360 kbps , bc 128000 bytes

El primero trata principalmente de los protocolos de ruteo, el segundo trata del Protocolo de mensajes de control de Internet (ICMP) que tiene una de las prioridades más bajas y CIR. La diferencia en CIR es cien veces mayor. Por lo tanto, es importante comprender las clases, los impactos, las comprobaciones/verificaciones comunes y las recomendaciones.

Clases CoPP

Supervisión de clase: copp-system-p-class-monitoring

Esta clase incluye ICMP para IPv4 e IPv6, y traceroute del tráfico dirigido al switch en cuestión.

class-map copp-system-p-class-monitoring (match-any)
match access-group name copp-system-p-acl-icmp
match access-group name copp-system-p-acl-icmp6
match access-group name copp-system-p-acl-traceroute
set cos 1
police cir 360 kbps , bc 128000 bytes

Impacto

Un error común cuando se resuelve un problema de pérdida o latencia de paquetes es hacer ping al switch a través de sus puertos en banda, que están limitados por la velocidad por CoPP. Como CoPP controla fuertemente el ICMP, incluso con un tráfico bajo o congestión, la pérdida de paquetes puede ser vista por un ping a las interfaces dentro de banda directamente si violan la CIR.

Por ejemplo, mediante un ping a interfaces conectadas directamente en puertos enrutados, con una carga útil de paquetes de 500, las caídas se pueden ver periódicamente.

<#root>

N9K-3# ping 192.168.1.1 count 1000 packet-size 500
...
--- 192.168.1.1 ping statistics ---
1000 packets transmitted, 995 packets received,

0.50% packet loss

```
round-trip min/avg/max = 0.597/0.693/2.056 ms
```

En el Nexus, donde se destinaron los paquetes ICMP, puede ver que CoPP los descartó cuando se detectó la violación y se protegió la CPU:

<#root>

N9K-4# show policy-map interface control-plane class copp-system-p-class-monitoring
Control Plane

Service-policy input: copp-system-p-policy-strict

class-map copp-system-p-class-monitoring (match-any)
match access-group name copp-system-p-acl-icmp
match access-group name copp-system-p-acl-icmp6
match access-group name copp-system-p-acl-traceroute
set cos 1
police cir 360 kbps , bc 128000 bytes
module 1 :
transmitted 750902 bytes;
5-minute offered rate 13606 bytes/sec
conformed 13606 peak-rate bytes/sec
at Sun May 01 22:49:24 2022

dropped 2950 bytes;

5-min violate rate 53 byte/sec

violated 53 peak-rate byte/sec at Sun May 01 22:49:24 2022

Para solucionar problemas de latencia o pérdida de paquetes, se recomienda utilizar hosts accesibles a través del switch por el plano de datos, no destinados al propio switch, que sería tráfico del plano de control. El tráfico del plano de datos se reenvía/enruta en el nivel de hardware sin intervención del SUP y, por lo tanto, no se controla mediante CoPP, y normalmente no experimenta caídas.

Recomendaciones

- Envíe un ping a través del switch a través del plano de datos, no al switch, para verificar resultados falsos positivos para la pérdida de paquetes.
- Limite el Network Monitoring System (NMS) o las herramientas que utilizan de forma agresiva el ICMP en el switch para evitar una ráfaga a través de la velocidad de entrada comprometida para la clase. Recuerde que la CoPP se aplica a todo el tráfico agregado que cae en la clase.

Gestión de clases - copp-system-p-class-management

Como se puede ver aquí, esta clase abarca diferentes protocolos de gestión que se pueden utilizar para la comunicación (SSH, Telnet),

transferencias (SCP, FTP, HTTP, SFTP, TFTP), reloj (NTP), AAA (Radius/TACACS) y supervisión (SNMP), para las comunicaciones IPv4 e IPv6.

```
class-map copp-system-p-class-management (match-any)
match access-group name copp-system-p-acl-ftp
match access-group name copp-system-p-acl-ntp
match access-group name copp-system-p-acl-ssh
match access-group name copp-system-p-acl-http
match access-group name copp-system-p-acl-ntp6
match access-group name copp-system-p-acl-sftp
match access-group name copp-system-p-acl-snmp
match access-group name copp-system-p-acl-ssh6
match access-group name copp-system-p-acl-tftp
match access-group name copp-system-p-acl-https
match access-group name copp-system-p-acl-snmp6
match access-group name copp-system-p-acl-tftp6
match access-group name copp-system-p-acl-radius
match access-group name copp-system-p-acl-tacacs
match access-group name copp-system-p-acl-telnet
match access-group name copp-system-p-acl-radius6
match access-group name copp-system-p-acl-tacacs6
match access-group name copp-system-p-acl-telnet6
set cos 2
police cir 36000 kbps , bc 512000 bytes
```

Impacto

Los comportamientos o caídas más comunes asociados con esta clase incluyen:

- Lentitud CLI percibida al conectarse mediante SSH/Telnet. Si hay caídas activas en la clase, las sesiones de comunicación pueden ser lentas y sufrir caídas.
- Transfiera archivos con los protocolos FTP, SCP, SFTP y TFTP en el switch. El comportamiento más común observado es un intento de transferir imágenes de arranque del sistema/kickstart mediante puertos de administración en banda. Esto puede conducir a tiempos de transferencia más altos y sesiones de transmisión cerradas/terminadas determinadas por el ancho de banda agregado para la clase.
- Problemas de sincronización de NTP, esta clase también es importante porque mitiga los agentes o ataques NTP desconocidos.
- Los servicios AAA Radius y TACACS también pertenecen a esta clase. Si se percibe un impacto en esta clase, puede afectar a los servicios de autorización y autenticación en el switch para las cuentas de usuario, lo que también puede contribuir a la demora en los comandos CLI.
- SNMP también se controla en esta clase. El comportamiento más común observado debido a caídas debido a la clase SNMP es en servidores NMS, que realizan paseos, recolecciones masivas o escaneos de red. Cuando se produce inestabilidad periódica, por lo general se correlaciona con la programación de recolección de NMS.

Recomendaciones

- Si se percibe lentitud de CLI, junto con caídas en esta clase, utilice el acceso a la consola o el acceso fuera de banda de administración (mgmt0).

- Si las imágenes del sistema deben cargarse en el switch, utilice el puerto de administración fuera de banda (mgmt0) o los puertos USB para la transferencia más rápida.

- Si se pierden paquetes NTP, verifique show ntp peer-status y verifique la columna de alcance, ninguna caída se traduce a 377.

- Si se observan problemas con los servicios AAA, utilice usuarios solo locales para resolver problemas, hasta que se mitigue el comportamiento.

- La mitigación de los problemas de SNMP incluye un comportamiento menos agresivo, la recopilación dirigida o la minimización de los escáneres de red. Examine los tiempos periódicos desde los analizadores hasta los eventos que se ven a nivel de la CPU.

Datos unidifusión de clase L3: copp-system-p-class-l3uc-data

Esta clase se ocupa específicamente de los paquetes de búsqueda. Este tipo de paquete también lo gestiona el limitador de velocidad de hardware (HWRL).

Si la solicitud de protocolo de resolución de direcciones (ARP) para el siguiente salto no se resuelve cuando los paquetes IP entrantes se reenvían en una tarjeta de línea, la tarjeta de línea reenvía los paquetes al módulo supervisor.

El supervisor resuelve la dirección MAC para el siguiente salto y programa el hardware.

```
class-map copp-system-p-class-l3uc-data (match-any)
match exception glean
set cos 1
```

Esto ocurre normalmente cuando se utilizan rutas estáticas y el salto siguiente es inalcanzable o no se resuelve.

Cuando se envía una solicitud ARP, el software agrega una adyacencia de caída /32 en el hardware para evitar que los paquetes a la misma dirección IP de siguiente salto sean reenviados al supervisor. Cuando se resuelve el ARP, la entrada de hardware se actualiza con la dirección MAC correcta. Si la entrada ARP no se resuelve antes de un período de tiempo de espera, la entrada se elimina del hardware.

Nota: CoPP y HWRL funcionan conjuntamente para garantizar la protección de la CPU. Aunque parece que realizan funciones similares, HWRL es el primero. La implementación se basa en el lugar donde se implementa la función específica en los motores de reenvío del ASIC. Este enfoque en serie permite la granularidad y las protecciones multicapa que clasifican todos los paquetes enlazados a la CPU.

El HWRL se realiza por instancia/motor de reenvío en el módulo y se puede ver con el comando **show hardware rate-limiter**. El HWRL queda fuera del alcance de este documento técnico.

show hardware rate-limiter

Units for Config: kilo bits per second
Allowed, Dropped & Total: aggregated bytes since last clear counters

Module: 1
R-L Class Config Allowed Dropped Total
+---------------+----------+--------------------+--------------------+--------------------+

L3 glean 100 0 0 0

L3 mcast loc-grp 3000 0 0 0
access-list-log 100 0 0 0
bfd 10000 0 0 0
fex 12000 0 0 0
span 50 0 0 0
sflow 40000 0 0 0
vxlan-oam 1000 0 0 0
100M-ethports 10000 0 0 0
span-egress disabled 0 0 0
dot1x 3000 0 0 0
mpls-oam 300 0 0 0
netflow 120000 0 0 0
ucs-mgmt 12000 0 0 0

Impacto

- El tráfico del plano de datos se envía al supervisor como una infracción, ya que no se puede procesar en el hardware y, por lo tanto, crea presión en la CPU.

Recomendaciones

- La resolución común para esta materia para minimizar las gotas de espiga es asegurar que el salto siguiente es alcanzable, y para habilitar la aceleración de espiga mediante el comando de configuración: **hardware ip glean throttle**.

En Nexus 7000 8.4(2), también introdujo el soporte de filtro de floración para adyacencias de espiga para módulos M3 y F4. Consulte: Guía de Configuración de Unicast Routing de Cisco Nexus serie 7000 NX-OS

Revise cualquier configuración de ruta estática que utilice direcciones de siguiente salto inalcanzables, o utilice protocolos de ruteo dinámico que eliminarían dichas rutas de la RIB dinámicamente.

Clase crítica - class-map copp-system-p-class-critical

Esta clase hace referencia a los protocolos de plano de control más importantes desde una perspectiva L3, que incluyen protocolos de routing para IPv4 e IPv6, (RIP, OSPF, EIGRP, BGP), RP automático, canal de puerto virtual (vPC), y l2pt e IS-IS.

class-map copp-system-p-class-critical (match-any)
match access-group name copp-system-p-acl-bgp
match access-group name copp-system-p-acl-rip
match access-group name copp-system-p-acl-vpc
match access-group name copp-system-p-acl-bgp6
match access-group name copp-system-p-acl-ospf
match access-group name copp-system-p-acl-rip6
match access-group name copp-system-p-acl-eigrp
match access-group name copp-system-p-acl-ospf6
match access-group name copp-system-p-acl-eigrp6
match access-group name copp-system-p-acl-auto-rp
match access-group name copp-system-p-acl-mac-l2pt
match access-group name copp-system-p-acl-mac-l3-isis
set cos 7
police cir 36000 kbps , bc 1280000 bytes

Impacto

Caídas en inestabilidad de copp-system-p-class-critical transferencia a protocolos de ruteo, que pueden incluir adyacencias caídas o fallas de convergencia, o propagación de actualización/NLRI.
Las caídas de políticas más comunes en esta clase pueden estar relacionadas con dispositivos no autorizados en la red que actúan de forma anormal (debido a una configuración incorrecta o a un error) o con la escalabilidad.

Recomendaciones

- Si no se detectan anomalías, como un dispositivo no autorizado o inestabilidad de capa 2 que provoca una reconvergencia continua de los protocolos de capa superior, se puede requerir una configuración personalizada de CoPP o una clase más indulgente para adaptar la escala.

- Consulte la guía de configuración de CoPP para obtener información sobre cómo configurar un perfil CoPP personalizado a partir de un perfil predeterminado que existe actualmente.
Copia de la directiva de prácticas recomendadas de CoPP

Clase importante - copp-system-p-class-important

Esta clase está relacionada con los protocolos de redundancia de primer salto (FHRP), que incluyen HSRP, VRRP y también LLDP

class-map copp-system-p-class-important (match-any)
match access-group name copp-system-p-acl-hsrp
match access-group name copp-system-p-acl-vrrp
match access-group name copp-system-p-acl-hsrp6
match access-group name copp-system-p-acl-vrrp6
match access-group name copp-system-p-acl-mac-lldp
set cos 6
police cir 2500 kbps , bc 1280000 bytes

Impacto

El comportamiento más común que se observa aquí y que conduce a caídas son los problemas con la inestabilidad de la capa 2, que lleva a dispositivos que pasan a escenarios de estado activo (cerebro dividido), temporizadores agresivos, configuraciones erróneas o escalabilidad.

Recomendaciones:

- Asegúrese para FHRP de que los grupos estén correctamente configurados y de que los roles sean activo/en espera o primario/secundario y se negocien correctamente, y de que no haya flaps en el estado.
- Verifique si hay problemas de convergencia en L2 o problemas con la propagación multicast para el dominio L2.

Class L2 Unpoliced - copp-system-p-class-l2-unpoliced

La clase sin regulación de tráfico L2 hace referencia a todos los protocolos críticos de la Capa 2 que son la base para todos los protocolos de la capa superior y, por lo tanto, se consideran casi sin regulación de tráfico con la CIR y prioridad más altas.

Efectivamente, esta clase gestiona el protocolo de árbol de extensión (STP), el protocolo de control de agregación de enlaces (LACP) y el servicio Cisco Fabric sobre Ethernet (CFSoE)

```
class-map copp-system-p-class-l2-unpoliced (match-any)
match access-group name copp-system-p-acl-mac-stp
match access-group name copp-system-p-acl-mac-lacp
match access-group name copp-system-p-acl-mac-cfsoe
match access-group name copp-system-p-acl-mac-sdp-srp
match access-group name copp-system-p-acl-mac-l2-tunnel
match access-group name copp-system-p-acl-mac-cdp-udld-vtp
set cos 7
police cir 50 mbps , bc 8192000 bytes
```

Esta clase tiene una CIR de policía de 50 Mbps, la más alta de todas las clases, junto con la mayor absorción de velocidad de ráfaga.

Impacto

Las caídas en esta clase pueden conducir a la inestabilidad global, ya que todos los protocolos de capa superior y las comunicaciones en los planos de datos, control y gestión dependen de una estabilidad de capa 2 subyacente.

Los problemas con las violaciones de STP pueden causar problemas de convergencia de TCN y STP, que incluyen disputas de STP, vaciados de MAC, movimientos y comportamientos con discapacidad de aprendizaje, que causan problemas de disponibilidad y pueden causar loops de tráfico que desestabilizan la red.

Esta clase también hace referencia a LACP y, por lo tanto, gestiona todos los paquetes EtherType asociados con 0x8809, que incluyen todas las LACPDU utilizadas para mantener el estado de los enlaces de canal de puerto. La inestabilidad en esta clase puede hacer que los canales de puerto agoten el tiempo de espera si se descartan las LACPDU.

Cisco Fabric Service over Ethernet (CSFoE) pertenece a esta clase y se utiliza para comunicar estados de control de aplicaciones críticos entre switches Nexus, por lo que es imprescindible para la estabilidad.

Lo mismo se aplica a otros protocolos dentro de esta clase, que incluye CDP, UDLD y VTP.

Recomendaciones

- El comportamiento más común se relaciona con la inestabilidad de Ethernet L2. Asegúrese de que el STP esté diseñado correctamente de manera determinista con las mejoras de funciones relevantes en juego para minimizar el impacto de la reconvergencia o de los dispositivos no autorizados en la red. Asegúrese de que el tipo de puerto STP adecuado esté configurado para todos los dispositivos de host final que no participen en la extensión L2 estén configurados como puertos troncales de borde/borde para minimizar los TCN.

- Utilice las mejoras de STP, como BPDUguard, Loopguard, BPDUfilter y RootGuard cuando sea apropiado para limitar el alcance de una falla, o problemas con la configuración incorrecta o dispositivos no autorizados en la red.

- Consulte: Guía de Configuración de Switching de Capa 2 de Cisco Nexus 9000 NX-OS, Release 10.2(x)

- Compruebe si hay comportamientos de movimiento de MAC que puedan provocar la desactivación del aprendizaje y los vaciados de MAC. Consulte:Solución de problemas y métodos preventivos de movimiento de Mac Nexus 9000

Router de multidifusión de clase: class-map copp-system-p-class-multicast-router

Esta clase hace referencia a los paquetes de multidifusión independiente del protocolo (PIM) del plano de control utilizados para el establecimiento y control de árboles compartidos de multidifusión enrutados a través de todos los dispositivos habilitados para PIM en la ruta del plano de datos e incluye el router de primer salto (FHR), el router de último salto (LHR), los routers de salto intermedio (IHR) y los puntos de encuentro (RP). Los paquetes clasificados dentro de esta clase incluyen el registro PIM para orígenes, las uniones PIM para receptores tanto para IPv4 como para IPv6, en general cualquier tráfico destinado a PIM (224.0.0.13) y el protocolo de transmisión de fuente multidifusión (MSDP). Tenga en cuenta que hay varias clases adicionales, que se ocupan de partes muy específicas de la funcionalidad de multidifusión o RP que son controladas por diferentes clases.

```
class-map copp-system-p-class-multicast-router (match-any)
match access-group name copp-system-p-acl-pim
match access-group name copp-system-p-acl-msdp
match access-group name copp-system-p-acl-pim6
match access-group name copp-system-p-acl-pim-reg
match access-group name copp-system-p-acl-pim6-reg
match access-group name copp-system-p-acl-pim-mdt-join
match exception mvpn
set cos 6
police cir 2600 kbps , bc 128000 bytes
```

Impacto

El impacto principal en las caídas que se relacionan con esta clase se asocia con problemas que se comunican a los orígenes de multidifusión mediante el registro PIM hacia los RP o uniones PIM no procesadas correctamente, lo que desestabilizaría los árboles de trayectoria compartida o más corta hacia los orígenes del flujo de multidifusión o hacia los RP. El comportamiento puede incluir una lista de interfaz saliente (OIL) que no se rellena correctamente debido a uniones ausentes, o bien (S, G) o (*, G) que no se ve de forma coherente en el entorno. También pueden

surgir problemas entre los dominios de ruteo multicast que dependen de MSDP para la interconexión.

Recomendaciones

- El comportamiento más común para los problemas relacionados con el control PIM se refiere a problemas de escala o comportamientos sospechosos. Uno de los comportamientos más comunes se observa debido a la implementación en UPnP, que también puede causar problemas de agotamiento de la memoria. Esto se puede solucionar mediante filtros y la reducción del alcance de los dispositivos no fiables. Para obtener detalles sobre cómo mitigar y filtrar los paquetes de control de multidifusión que dependen de la función de red del dispositivo, consulte: Configuración del filtrado de multidifusión en Nexus 7K/N9K - Cisco

Class Multicast Host - copp-system-p-class-multicast-host

Esta clase hace referencia a Multicast Listener Discovery (MLD), específicamente a los tipos de paquete MLD query, report, reduction y MLDv2. MLD es un protocolo IPv6 que un host utiliza para solicitar datos de multidifusión para un grupo determinado. Con la información obtenida a través de MLD, el software mantiene una lista de membresías de grupo o canal multicast por interfaz. Los dispositivos que reciben paquetes MLD envían los datos de multidifusión que reciben para los grupos o canales solicitados fuera del segmento de red de los receptores conocidos. MLDv1 se deriva de IGMPv2 y MLDv2 se deriva de IGMPv3. IGMP utiliza los tipos de mensajes del Protocolo IP 2, mientras que MLD utiliza los tipos de mensajes del Protocolo IP 58, que es un subconjunto de los mensajes ICMPv6.

```
class-map copp-system-p-class-multicast-host (match-any)
match access-group name copp-system-p-acl-mld
set cos 1
police cir 1000 kbps , bc 128000 bytes
```

Impacto

Las caídas en esta clase se traducen en problemas en las comunicaciones multicast IPv6 locales de link, que pueden hacer que se descarten los informes del receptor de los receptores o las respuestas a las consultas generales, lo que impide la detección de grupos multicast que los hosts desean recibir. Esto puede afectar el mecanismo de indagación y no reenviar correctamente el tráfico a través de las interfaces esperadas que solicitaron el tráfico.

Recomendaciones

- Dado que el tráfico MLD es significativo a nivel local de enlace para IPv6, si se observan caídas en esta clase, las causas de comportamiento más comunes están relacionadas con la escalabilidad, la inestabilidad de L2 o los dispositivos no autorizados.

Datos multidifusión de capa 3 de clase - copp-system-p-class-l3mc-data y datos multidifusión IPv6 de capa 3 de clase - copp-system-p-class-l3mcv6-data

Estas clases hacen referencia al tráfico que coincide con una redirección de excepción de multidifusión hacia el SUP. En este caso, hay dos condiciones controladas por estas clases. La primera es la falla de Reverse-Path Forwarding (RPF) y la segunda es la falla de destino. La pérdida de destino se refiere a los paquetes de multidifusión en los que la búsqueda en el hardware para la tabla de reenvío de multidifusión de capa 3 falla y, por lo tanto, el paquete de datos se envía a la CPU. Estos paquetes se utilizan a veces para activar/instalar el plano de control de multidifusión y agregar las entradas de las tablas de reenvío de hardware, según el tráfico del plano de datos. Los paquetes multicast del plano de

datos que violan el RPF también coincidirían con esta excepción y se clasificarían como una violación.

```
class-map copp-system-p-class-l3mc-data (match-any)
match exception multicast rpf-failure
match exception multicast dest-miss
set cos 1
police cir 2400 kbps , bc 32000 bytes

class-map copp-system-p-class-l3mcv6-data (match-any)
match exception multicast ipv6-rpf-failure
match exception multicast ipv6-dest-miss
set cos 1
police cir 2400 kbps , bc 32000 bytes
```

Impacto

Los fallos de RPF y los errores de destino implican un problema de diseño o configuración relacionado con la forma en que el tráfico fluye a través del router multicast. Las pérdidas de destino son comunes en la creación de estados, las caídas pueden conducir a la programación y creación de (*, G), (S, G) fallas.

Recomendaciones

- Realice cambios en el diseño básico de RIB de unidifusión o agregue una ruta multicast estática para dirigir el tráfico a través de una interfaz en particular, en el caso de fallas de RPF.
- Consulte El Router No Reenvía Paquetes Multicast al Host Debido a una Falla RPF

Clase IGMP - copp-system-p-class-igmp

Esta clase hace referencia a todos los mensajes IGMP, para todas las versiones que se utilizan para solicitar datos de multidifusión para un grupo determinado, y que utiliza la funcionalidad de indagación IGMP para mantener los grupos y la lista de interfaz saliente (OIL) relevante que reenvía el tráfico a través de los receptores interesados en la Capa 2. Los mensajes IGMP son significativos a nivel local porque no atraviesan un límite de Capa 3, ya que su tiempo de vida (TTL) debe ser 1, como se documenta en RFC2236 (Internet Group Management Protocol, Version 2). Los paquetes IGMP manejados por esta clase incluyen todas las consultas de membresía (generales o de origen/grupo específico), junto con la membresía y los informes de abandono de los receptores.

```
class-map copp-system-p-class-normal-igmp (match-any)
match access-group name copp-system-p-acl-igmp
set cos 3
police cir 3000 kbps , bc 64000 bytes
```

Impacto

Las caídas en esta clase se traducirían en problemas en todos los niveles de una comunicación multicast entre el origen y el receptor, según el

tipo de mensaje IGMP descartado debido a la violación. Si se pierden los informes de pertenencia de los receptores, el router no detecta los dispositivos interesados en el tráfico y, por lo tanto, no incluye la interfaz/VLAN en su lista de interfaz saliente relevante. Si este dispositivo es también el solicitante o el router designado, no activa los mensajes de unión PIM relevantes hacia el RP si el origen está más allá del dominio de Capa 2 local, por lo tanto, nunca establece el plano de datos a través del árbol multicast hasta el receptor o RP. Si se pierde el informe de ausencia, el receptor puede continuar recibiendo tráfico no deseado. Esto también puede afectar todas las consultas IGMP relevantes activadas por el solicitante y la comunicación entre los routers multicast en un dominio.

Recomendaciones

- Los comportamientos más comunes asociados con las caídas de IGMP están relacionados con la inestabilidad de L2, problemas con los temporizadores o la escala.

Clase Normal - copp-system-p-class-normalcopp-system-p-class-normal

Esta clase hace referencia al tráfico que coincide con el tráfico ARP estándar y también incluye el tráfico asociado con 802.1X, utilizado para el control de acceso a la red basado en puertos. Esta es una de las clases más comunes que encuentra violaciones como solicitudes ARP, Gratuitous ARP, paquetes ARP inverso se transmiten y se propagan a través de todo el dominio de Capa 2. Es importante recordar que los paquetes ARP no son paquetes IP, estos paquetes no contienen un encabezado L3, y por lo tanto la decisión se toma solamente en el alcance de los encabezados L2. Si un router está configurado con una interfaz IP asociada a esa subred, como una Interfaz virtual de switch (SVI), el router dirige los paquetes ARP al SUP para su procesamiento, ya que están destinados a la dirección de difusión de hardware. Cualquier tormenta de difusión, loop de Capa 2 (debido a STP o flaps), o un dispositivo rugoso en la red puede conducir a una tormenta ARP que hace que las violaciones aumenten significativamente.

```
class-map copp-system-p-class-normal (match-any)
match access-group name copp-system-p-acl-mac-dot1x
match protocol arp
set cos 1
police cir 1400 kbps , bc 32000 bytes
```

Impacto

El impacto de las infracciones en esta clase depende en gran medida de la duración de los eventos y de la función del switch en el entorno. Las caídas en esta clase implican que los paquetes ARP actualmente son descartados y, por lo tanto, no procesados por el motor SUP, lo que puede conducir a dos comportamientos principales causados por resoluciones ARP incompletas.

Desde la perspectiva del host final, los dispositivos de la red no pueden resolver o completar la resolución de direcciones con el switch. Si este dispositivo actúa como el gateway predeterminado para el segmento, puede ocasionar que los dispositivos no puedan resolver su gateway y, por lo tanto, no puedan rutear fuera de su segmento Ethernet de capa 2 (VLAN). Los dispositivos todavía pueden comunicarse en el segmento local si pueden completar la resolución ARP para otros hosts extremos en el segmento local.

Desde la perspectiva del switch, si la tormenta y las violaciones son frecuentes, también puede hacer que el switch no pueda completar el proceso para la solicitud ARP que generó. Estas solicitudes se generan normalmente para resoluciones de subredes de siguiente salto o conectadas directamente. Aunque las respuestas ARP son de naturaleza unicast, ya que se dirigen a la MAC propiedad del switch, se clasifican en esta misma clase, ya que siguen siendo paquetes ARP. Esto se traduce en problemas de disponibilidad porque el switch no puede procesar correctamente el tráfico si no se resuelve el siguiente salto, y puede generar problemas con la reescritura del encabezado de Capa 2, si el

administrador de adyacencia no tiene una entrada para el host.

El impacto también depende del alcance del problema fundamental que desencadenó la violación ARP. Por ejemplo, en una tormenta de difusión, los hosts y el switch continúan a ARP para intentar resolver la adyacencia, lo que puede conducir a tráfico de difusión adicional en la red, y como los paquetes ARP son de Capa 2, no hay tiempo de vida (TTL) de Capa 3 para interrumpir un loop L2 y, por lo tanto, continúan en loop, y crecen exponencialmente a través de la red hasta que se rompe el loop.

Recomendaciones

- Resuelva cualquier inestabilidad L2 fundamental que pueda causar tormentas ARP en el entorno, como STP, flaps o dispositivos no autorizados. Rompa esos bucles según sea necesario, con cualquier método que desee para abrir la ruta de enlace.

- El control de tormentas también se puede utilizar para mitigar una tormenta ARP. Si el control de tormentas no está habilitado, verifique las estadísticas de contador en las interfaces para verificar el porcentaje de tráfico de difusión visto en las interfaces en relación con el tráfico total que pasa a través de la interfaz.

- Si no hay tormenta, pero aún se observan caídas constantes en el entorno, verifique el tráfico SUP para identificar cualquier dispositivo no autorizado, que envía constantemente paquetes ARP en la red, que pueda afectar el tráfico legítimo.

- Los aumentos que se pueden ver dependen del número de hosts en la red y del rol del switch en el entorno, el ARP está diseñado para reintentar, resolver y actualizar las entradas y, por lo tanto, se espera que vea el tráfico ARP en todo momento. Si solo se observan caídas esporádicas, pueden ser transitorias debido a la carga de la red y no se percibe ningún impacto. Sin embargo, es importante supervisar y conocer la red para identificar y diferenciar adecuadamente una situación esperada de otra anormal.

Class NDP - copp-system-p-acl-ndp

Esta clase hace referencia al tráfico asociado con la detección/anuncio de vecino IPv6 y los paquetes de solicitud y anuncio de router que utilizan mensajes ICMP para determinar las direcciones de la capa de link local de los vecinos, y se utiliza para la accesibilidad y el seguimiento de los dispositivos vecinos.

```
class-map copp-system-p-class-ndp (match-any)
match access-group name copp-system-p-acl-ndp
set cos 6
police cir 1400 kbps , bc 32000 bytes
```

Impacto

Las infracciones en esta clase pueden impedir la comunicación IPv6 entre los dispositivos vecinos, ya que estos paquetes se utilizan para facilitar la detección dinámica o la información local/de capa de link entre los hosts y los routers en el link local. Una interrupción de esta comunicación también puede causar problemas con la disponibilidad más allá o a través del link local asociado. Si hay problemas de comunicación entre vecinos IPv6, asegúrese de que no haya caídas en esta clase.

Recomendaciones

- Examine cualquier comportamiento ICMP anormal de los dispositivos vecinos, particularmente aquellos que se relacionan con la detección de vecinos y/o la detección de routers.

- Asegúrese de que todos los valores esperados de temporizador e intervalo para los mensajes periódicos sean consistentes en todo el entorno y se cumplan. Por ejemplo, para mensajes de anuncio de router (mensajes RA).

Clase Normal DHCP - copp-system-p-class-normal-dhcp

Esta clase hace referencia al tráfico asociado al protocolo de arranque (cliente/servidor BOOTP), conocido comúnmente como paquetes de protocolo de control dinámico de host (DHCP) en el mismo segmento Ethernet local para IPv4 e IPv6. Esto se relaciona específicamente sólo con la comunicación de tráfico que se origina desde cualquier cliente de inicialización o que está destinada a cualquier servidor BOOTP, a través de todo el intercambio de paquetes de detección, oferta, solicitud y reconocimiento (DORA), y también incluye la transacción cliente/servidor DHCPv6 a través de los puertos UDP 546/547.

```
class-map copp-system-p-class-normal-dhcp (match-any)
match access-group name copp-system-p-acl-dhcp
match access-group name copp-system-p-acl-dhcp6
set cos 1
police cir 1300 kbps , bc 32000 bytes
```

Impacto

Las infracciones en esta clase pueden provocar que los hosts finales no puedan adquirir correctamente una IP del servidor DHCP y, por tanto, vuelvan a su intervalo de direcciones IP privadas automáticas (APIPA), 169.254.0.0/16. Estas violaciones pueden ocurrir en entornos donde los dispositivos intentan iniciarse simultáneamente y, por lo tanto, van más allá de la CIR asociada con la clase.

Recomendaciones

- Verifique con capturas, en los hosts y el lado del servidor DHCP se ve toda la transacción DORA. Si el switch es parte de esta comunicación, también es importante verificar los paquetes procesados o enviados a la CPU, y verificar las estadísticas sobre el switch: **show ip dhcp global statistics** y las redirecciones: **show system internal access-list sup-redirect-stats module 1 | grep -i dhcp**.

Respuesta de retransmisión DHCP normal de clase - copp-system-p-class-normal-dhcp-relay-response

Esta clase hace referencia al tráfico asociado a la funcionalidad de retransmisión DHCP tanto para IPv4 como para IPv6, dirigido a los servidores DHCP configurados bajo la retransmisión. Esto se relaciona específicamente sólo con la comunicación de tráfico que se origina desde cualquier servidor BOOTP o está destinada a cualquier cliente BOOTP a través de todo el intercambio de paquetes DORA, y también incluye la transacción cliente/servidor DHCPv6 a través de los puertos UDP 546/547.

```
class-map copp-system-p-class-normal-dhcp-relay-response (match-any)
match access-group name copp-system-p-acl-dhcp-relay-response
match access-group name copp-system-p-acl-dhcp6-relay-response
set cos 1
police cir 1500 kbps , bc 64000 bytes
```

Impacto

Las violaciones de esta clase tienen el mismo impacto que las violaciones de la clase copp-system-p-class-normal-dhcp, porque ambas son partes de la misma transacción. Esta clase se centra principalmente en las comunicaciones de respuesta de los servidores del agente de retransmisión. El Nexus no actúa como servidor DHCP, está diseñado únicamente para actuar como agente de retransmisión.

Recomendaciones

- Aquí se aplican las mismas recomendaciones que para la clase normal de DHCP. Dado que la función del Nexus consiste únicamente en actuar como agente relay, en el SUP se espera ver toda la transacción entre el host y el switch actuando como relay, y el switch y los servidores configuran.

- Asegúrese de que no haya dispositivos sospechosos, como servidores DHCP inesperados en la red que respondan al ámbito, o dispositivos atascados en un bucle que inunden la red con paquetes de detección DHCP. Se pueden realizar comprobaciones adicionales mediante los comandos: show ip dhcp relay y **show ip dhcp relay statistics**.

Flujo NAT de clase - copp-system-p-class-nat-flow

Esta clase se refiere al tráfico de flujo de NAT del switch de software. Cuando se crea una nueva traducción dinámica, el flujo se reenvía por software hasta que la traducción se programa en hardware y, a continuación, CoPP la controla para limitar el tráfico dirigido al supervisor mientras la entrada está instalada en el hardware.

class-map copp-system-p-class-nat-flow (match-any)
match exception nat-flow
set cos 7
police cir 800 kbps , bc 64000 bytes

Impacto

Las caídas de esta clase suelen producirse cuando se instala en el hardware una alta tasa de nuevos flujos y traducciones dinámicas. El impacto está relacionado con los paquetes conmutados por software que se descartan y no se entregan al host final, lo que puede provocar pérdidas y retransmisiones. Una vez instalada la entrada en el hardware, no se envía más tráfico al supervisor.

Recomendaciones

- Verifique las pautas y limitaciones de NAT dinámica en la plataforma relevante. Existen limitaciones conocidas que se documentan en las plataformas, como el 3548, en el que la traducción puede tardar unos segundos. Consulte: Restricciones de NAT Dinámica

Excepción de clase - copp-system-p-class-exception

Esta clase hace referencia a los paquetes de excepción asociados a la opción IP y a los paquetes IP ICMP inalcanzables. Si una dirección de destino no está presente en la base de información de reenvío (FIB) y da lugar a una pérdida, el SUP envía un paquete ICMP inalcanzable al remitente. Los paquetes con opciones IP habilitadas también pertenecen a esta clase., Consulte el documento de IANA para obtener detalles sobre las opciones IP: Números de opción IP

class-map copp-system-p-class-exception (match-any)
match exception ip option
match exception ip icmp unreachable
match exception ipv6 option
match exception ipv6 icmp unreachable
set cos 1
police cir 150 kbps , bc 32000 bytes

Impacto

Esta clase está fuertemente regulada, y las caídas en esta clase no son indicativas de una falla sino más bien de un mecanismo de protección para limitar el alcance de los paquetes de opciones IP y de ICMP inalcanzables.

Recomendaciones

- Verifique si hay algún flujo de tráfico visto o dirigido a la CPU para destinos que no están en la FIB.

Redirección de clase: copp-system-p-class-redirect

Esta clase hace referencia al tráfico asociado al protocolo de tiempo de precisión (PTP), utilizado para la sincronización horaria. Esto incluye el tráfico multicast para el rango reservado 224.0.1.129/32, el tráfico unicast en el puerto UDP 319/320 y el Ethetype 0X88F7.

class-map copp-system-p-class-redirect (match-any)
match access-group name copp-system-p-acl-ptp
match access-group name copp-system-p-acl-ptp-l2
match access-group name copp-system-p-acl-ptp-uc
set cos 1
police cir 280 kbps , bc 32000 bytes

Impacto

Las caídas en esta clase pueden ocasionar problemas en los dispositivos que no se han sincronizado correctamente o que no han establecido la jerarquía adecuada.

Recomendaciones

- Garantizar la estabilidad de los relojes y que estén configurados correctamente. Asegúrese de que el dispositivo PTP esté configurado para el modo PTP de multidifusión o unidifusión, pero no para ambos al mismo tiempo. Esto también se documenta bajo las pautas y la limitación, y puede empujar el tráfico más allá de la velocidad de entrada comprometida.

- Revise el diseño y la configuración del reloj de límite y de todos los dispositivos PTP del entorno. Asegúrese de que se siguen todas las directrices y limitaciones por plataforma, ya que varían.

Clase OpenFlow - copp-system-p-class-openflow

Esta clase hace referencia al tráfico asociado con las operaciones del agente OpenFlow y la conexión TCP correspondiente entre el controlador y el agente.

```
class-map copp-system-p-class-openflow (match-any)
match access-group name copp-system-p-acl-openflow
set cos 5
police cir 1000 kbps , bc 32000 bytes
```

Impacto

Las caídas en esta clase pueden conducir a problemas en los agentes que no reciben y procesan correctamente las instrucciones del controlador para administrar el plano de reenvío de la red

Recomendaciones

- Asegúrese de que no se vea tráfico duplicado en la red o en cualquier dispositivo que dificulte la comunicación entre el controlador y los agentes.
- Verifique que la red L2 no tenga inestabilidad (STP o loops).

Solucionar problemas de CoPP descartados

Los primeros pasos para solucionar las infracciones de CoPP son determinar:

- Impacto y alcance de la cuestión.
- Comprender el flujo de tráfico a través del entorno y el papel del switch en la comunicación afectada.
- Determine si hay infracciones en la clase asociada sospechosa e itere según sea necesario.

Por ejemplo, se ha detectado el comportamiento enumerado:

- Los dispositivos no pueden comunicarse con otros dispositivos que no estén en su red, pero pueden comunicarse localmente.
- El impacto se ha aislado en la comunicación enrutada fuera de la VLAN, y el switch actúa como el gateway predeterminado.
- Una comprobación de los hosts indica que no pueden hacer ping al gateway. Después de una verificación de su tabla ARP, la entrada para el gateway permanece como Incompleta.
- El resto de hosts que tienen la resolución de gateway no tienen problemas de comunicación. Una comprobación de CoPP en el switch que actúa como gateway indica que hay infracciones en copp-system-p-class-normal.

<#root>

class-map copp-system-p-class-normal (match-any)
match access-group name copp-system-p-acl-mac-dot1x
match protocol arp
set cos 1
police cir 1400 kbps , bc 32000 bytes
module 1 :
transmitted 3292445628 bytes;

dropped 522023852 bytes;

- Además, múltiples comprobaciones de comando muestran que las caídas están en aumento.

- Estas violaciones pueden hacer que se descarte el tráfico ARP legítimo, lo que conduce a un comportamiento de negación de servicios.

Es importante destacar que CoPP aísla el impacto en el tráfico asociado con la clase específica, que en este ejemplo son ARP y copp-system-p-class-normal. CoPP no descarta el tráfico relacionado con otras clases, como OSPF y BGP, ya que pertenecen a una clase completamente diferente. Si no se marca, los problemas ARP pueden derivar en cascada a otros problemas, lo que puede afectar a los protocolos que dependen de él para empezar. Por ejemplo, si una memoria caché ARP agota el tiempo de espera y no se actualiza debido a violaciones excesivas, una sesión TCP como BGP puede terminar.

- Se aconseja realizar verificaciones del plano de control, como Ethanalyzer, CPU-mac in-band stats, y el proceso de CPU para aislar aún más la materia.

Etanizador

Dado que el tráfico regulado por CoPP está asociado solamente con el tráfico dirigido a la CPU, una de las herramientas más importantes es Ethanalyzer. Esta herramienta es una implementación de Nexus de TShark y permite que el tráfico enviado y recibido por el supervisor sea capturado y decodificado. También puede utilizar filtros basados en diferentes criterios, como protocolos o información de encabezado, lo que se convierte en una herramienta inestimable para determinar el tráfico enviado y recibido por la CPU.

La recomendación es examinar primero el tráfico ARP visto por el supervisor cuando la herramienta Ethanalyzer se ejecuta directamente en la sesión de terminal o se envía a un archivo para su análisis. Se pueden definir filtros y límites para enfocar la captura en un patrón o comportamiento específico. Para ello, agregue filtros de visualización flexibles.

Un error común es que Ethanalyzer captura todo el tráfico que atraviesa el switch. El tráfico del plano de datos, entre los hosts, es conmutado o ruteado por los ASIC de hardware entre los puertos de datos no requiere la participación de la CPU y, por lo tanto, no es visto normalmente por la captura de Ethanalyzer. Para capturar el tráfico del plano de datos, se recomienda utilizar otras herramientas, como ELAM o SPAN. Por ejemplo, para filtrar ARP, utilice el comando:

ethanalyzer local interface inband display-filter arp limit-captured-frames 0 autostop duration 60 > arpcpu

Campos configurables importantes:

- interface inband - se refiere al tráfico dirigido al SUP

- display-filter arp - hace referencia al filtro Tshark aplicado; se aceptan la mayoría de los filtros Wireshark.

- limit-captured-frames 0 - se refiere al límite, 0 equivale a ilimitado, hasta que lo detiene otro parámetro o lo detiene manualmente Ctrl+C

- autostop duration 60 - se refiere a la detención de Ethanalyzer después de 60 segundos, por lo que crea una instantánea de 60 segundos de tráfico ARP visto en la CPU

El resultado de Ethanalyzer se redirige a un archivo en la memoria de inicialización con > arpcpu, para ser procesado manualmente. Después de 60 segundos, la captura se completa, y Ethanalyzer termina dinámicamente, y el archivo arpcpu está en la memoria flash de inicialización del switch, que luego se puede procesar para extraer a los usuarios más activos. Por ejemplo:

show file bootflash:arpcpu | sort -k 3,5 | uniq -f 2 -c | sort -r -n | head lines 50

669 2022-05-10 10:29:50.901295 28:ac:9e:ad:5e:47 -> ff:ff:ff:ff:ff:ff ARP Who has 10.1.1.1? Tell 10.1.1.2
668 2022-05-10 10:29:50.901295 28:ac:9e:ad:5e:43 -> ff:ff:ff:ff:ff:ff ARP Who has 10.2.1.1? Tell 10.2.1.2
668 2022-05-10 10:29:50.901295 28:ac:9e:ad:5e:41 -> ff:ff:ff:ff:ff:ff ARP Who has 10.3.1.1? Tell 10.3.1.2

Este filtro se ordena en función de: las columnas de origen y destino, las coincidencias únicas encontradas (pero omite la columna de fecha), cuenta las instancias y agrega el número visto y, por último, ordena de arriba a abajo, en función del recuento, y muestra los primeros 50 resultados.

En este ejemplo de laboratorio, en 60 segundos, se recibieron más de 600 paquetes ARP de tres dispositivos, que se han identificado como los dispositivos sospechosos de delinquir. La primera columna del filtro detalla el número de instancias de este evento que se vieron en el archivo de captura en la duración especificada.

Es importante comprender que la herramienta Ethanalyzer actúa sobre el driver en banda, que es esencialmente la comunicación en el ASIC. En teoría, el paquete debe pasar a través del núcleo y el administrador de paquetes debe ser entregado al propio proceso asociado. CoPP y HWRL actúan antes de que se vea el tráfico en Ethanalyzer. Incluso si las infracciones aumentan de forma activa, parte del tráfico sigue circulando y se ajusta a la velocidad de la policía, lo que ayuda a proporcionar información sobre los flujos de tráfico dirigidos a la CPU. Es una distinción importante, ya que el tráfico visto en el Ethanalyzer NO es el tráfico que violó la CIR y que se descartó.

El Ethanalyzer también se puede utilizar de forma abierta, sin ningún filtro de visualización o filtro de captura especificado para capturar todo el tráfico SUP relevante. Esto se puede utilizar como medida de aislamiento como parte del enfoque para solucionar los problemas.

Para obtener más información y el uso del Ethanalyzer, consulte la Nota técnica:

Guía de solución de problemas de Ethanalyzer en Nexus 7000

Uso de Ethanalyzer en la plataforma Nexus para el análisis del tráfico del plano de control y del plano de datos

---

Nota: Nexus 7000, antes de la versión de código 8.X, solo puede realizar capturas de Ethanalyzer a través del VDC de administración, que engloba el tráfico dirigido a SUP de todos los VDC. El Ethanalyzer específico de VDC está presente en los códigos 8.X.

CPU-MAC In-band Stats

Las estadísticas en banda asociadas con el tráfico enlazado a la CPU mantienen estadísticas relevantes del tráfico de CPU TX/RX en banda. Estas estadísticas se pueden verificar con el comando: show hardware internal cpu-mac inband stats, que proporciona información sobre las estadísticas de velocidad actual y de velocidad pico.

show hardware internal cpu-mac inband stats`
================ Packet Statistics ======================
Packets received: 363598837
Bytes received: 74156192058
Packets sent: 389466025
Bytes sent: 42501379591
Rx packet rate (current/peak): 35095 / 47577 pps
Peak rx rate time: 2022-05-10 12:56:18
Tx packet rate (current/peak): 949 / 2106 pps
Peak tx rate time: 2022-05-10 12:57:00

Como práctica recomendada, se recomienda crear una línea de base y realizar un seguimiento de la misma, ya que debido a la función del switch y la infraestructura, el resultado de la **show hardware internal cpu-mac inband stats** varía significativamente. En este entorno de laboratorio, los valores habituales y los picos históricos no suelen ser superiores a unos cientos de pps, por lo que esto es anormal. El comando también **show hardware internal cpu-mac inband events** es útil como referencia histórica, porque contiene datos relacionados con el uso máximo y la hora en que se detectó.

CPU del proceso

Los switches Nexus son sistemas basados en Linux, y el sistema operativo Nexus (NXOS) aprovecha el planificador preventivo de la CPU, la multitarea y el subprocesamiento múltiple de su arquitectura de núcleos respectiva para proporcionar un acceso justo a todos los procesos, por lo que los picos no siempre son indicativos de un problema. Sin embargo, si se observan violaciones de tráfico continuas, es probable que el proceso asociado también se utilice mucho y aparezca como un recurso principal en las salidas de la CPU. Tome varias instantáneas de los procesos de la CPU para verificar el uso elevado de un proceso determinado mediante: **show processes cpu sort | exclude 0.0 or show processes cpu sort | grep <process>**.

La CPU del proceso, las estadísticas en banda y las verificaciones de Ethanalyzer proporcionan información sobre los procesos y el tráfico procesados actualmente por el supervisor y ayudan a aislar la inestabilidad en curso en el tráfico del plano de control que puede derivar en problemas del plano de datos. Es importante comprender que la CoPP es un mecanismo de protección. Es reaccionaria porque solo actúa sobre el tráfico dirigido al SUP. Está diseñado para salvaguardar la integridad del supervisor mediante el descarte de las tasas de tráfico, que superan los rangos esperados. No todas las caídas indican un problema o requieren intervención, ya que su importancia está relacionada con la clase CoPP específica y el impacto verificado, según la infraestructura y el diseño de la red. Las caídas debidas a eventos de ráfaga esporádicos no se traducen en impacto, ya que los protocolos tienen mecanismos integrados, como keepalive y reintentos que pueden lidiar con eventos transitorios. Mantener el enfoque en eventos sostenidos o eventos anormales más allá de los valores de referencia establecidos. Recuerde que CoPP debe cumplir con los protocolos y las funciones específicas del entorno y debe ser supervisado e iterado continuamente para ajustarlo, en función de las necesidades de escalabilidad a medida que evolucionan. Si se producen caídas, determine si la CoPP interrumpió el tráfico de forma involuntaria o en respuesta a un mal funcionamiento o un ataque. En cualquier caso, analizar la situación y evaluar la necesidad de intervenir mediante el análisis del impacto y la medida correctora sobre el medio ambiente, que puede estar fuera del alcance del propio switch.

Additional Information

Las plataformas/códigos recientes, pueden tener la capacidad de realizar un SPAN a CPU, por el reflejo de un puerto y el punt del tráfico del plano de datos a la CPU. Esto está normalmente fuertemente limitado por el límite de velocidad de hardware y la CoPP. Se recomienda un uso cuidadoso del SPAN a la CPU, y está fuera del alcance de este documento.

Consulte la nota técnica que aparece para obtener más información sobre esta función:

Procedimiento SPAN-to-CPU para ASIC NX-OS de la escala de nube de Nexus 9000

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).