

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Flujo y el mitigar del tráfico de unidifusión](#)

[Flujo y el mitigar del tráfico Multicast](#)

[¿Qué causa los descartes de la entrada?](#)

[Ejemplo de Troubleshooting](#)

[Scenerio 1: Descartes de la entrada](#)

[Paso 1: Identifique los puertos con los descartes de la entrada](#)

[Paso 2: Identificación de ASIC](#)

[Paso 3: Identifique el puerto congestionado salida](#)

[Scenerio 2: Descartes de la entrada con HOLB \(jefe de la línea bloqueo\)](#)

[Mitigación HOLB: Límite del permiso VOQ](#)

[Mitigación HOLB: Clasificación de tráfico](#)

[Información pertinente](#)

Introducción

Este documento describe cómo resolver problemas los descartes de la entrada en el Switches de las 5600/6000 Series del nexo de Cisco. Los descartes de la entrada son una indicación de un puerto de egreso oversubscribed. También significa que usted es tráfico de unidifusión de caída probable en ese puerto específico. Las secciones abajo ayudarán a entender cómo el unicast y el tráfico Multicast está mitigado en esta plataforma y cómo los descartes de la entrada podrían ocurrir junto con los pasos de la mitigación.

Prerrequisitos

Requisitos

Cisco recomienda que usted tiene conocimiento básico de estos temas

- Configuración de las 6000 Series del nexo de Cisco

Componentes Utilizados

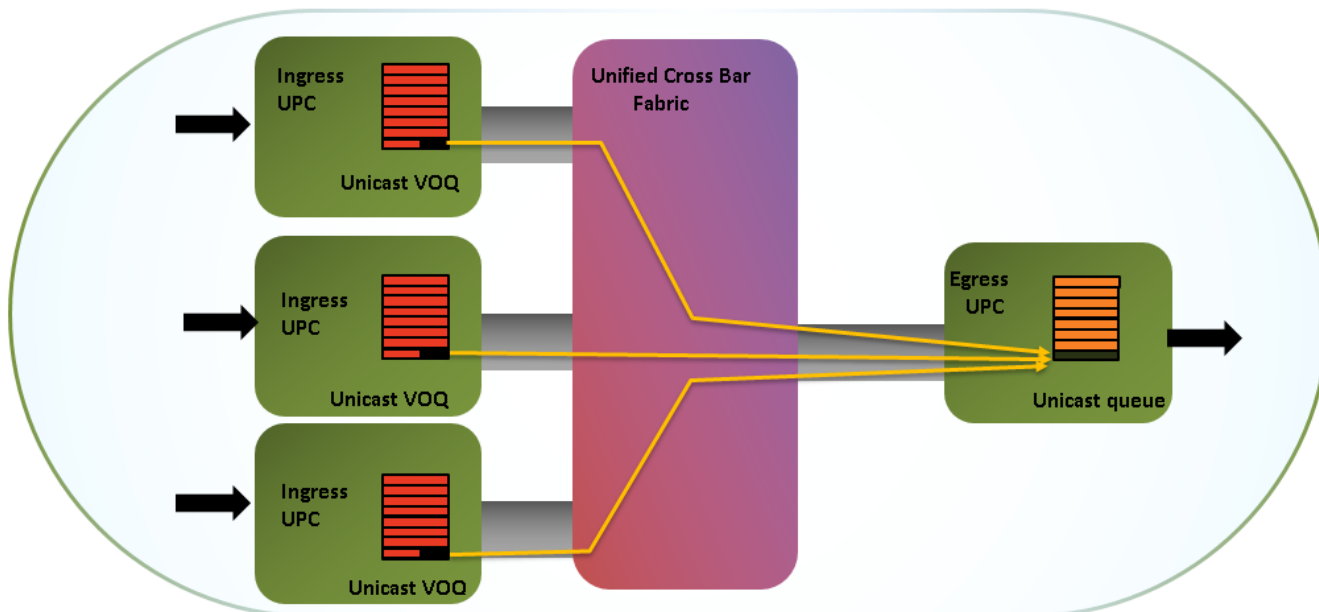
La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Nexo 6001 de Cisco
- 7.1(3)N1(1)

Flujo y el mitigar del tráfico de unidifusión

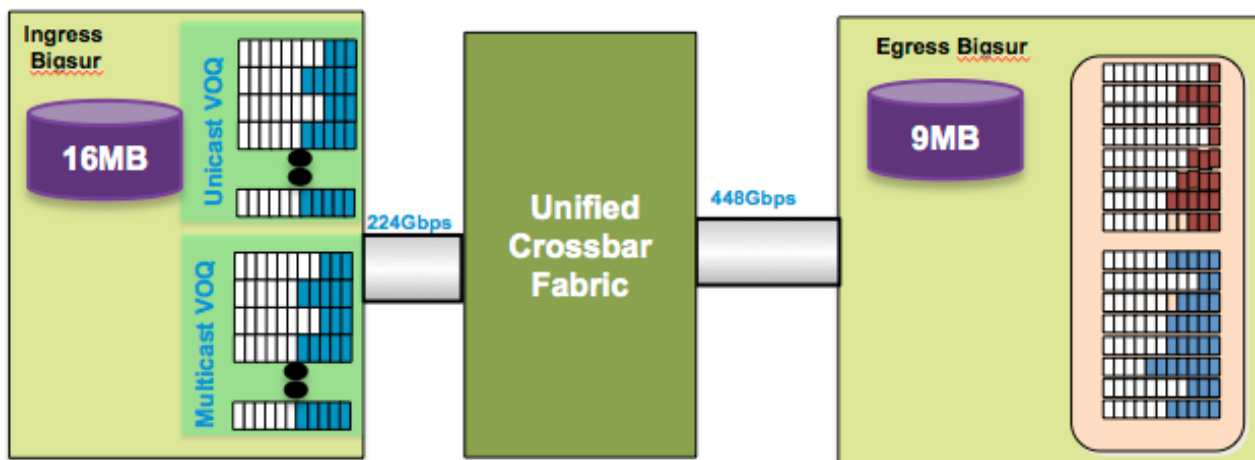
El tráfico de unidifusión primero y después se hace cola en el pool de búfer de egreso memoria

intermedia de ingreso después de que la cola de la salida sea llena.



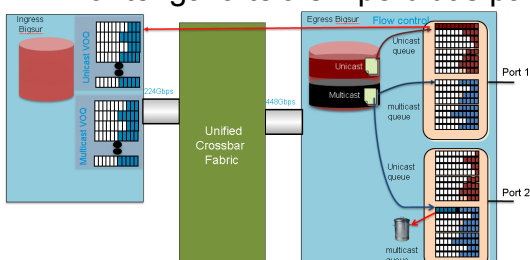
¿Allí es 16MB ingreso? ¿compartido? ¿buffer y salida 9MB? ¿compartido? buffer. Los buffers se comparten entre 12 puertos x10gig O los puertos 3x40gig. El buffer compartido es bueno para la absorción de la explosión.

Aquí está una pintura visual de la asignación de memoria para la referencia (Bigsur es el nombre del regulador del puerto ASIC/Unified)



Flujo y el mitigar del tráfico Multicast

- Los paquetes de multidifusión están mitigados y caídos en la salida
- Caiga el paquete de multidifusión cerca del punto de congestión evitan HOLB
- Mantenga la tela sin pérdidas para el unicast



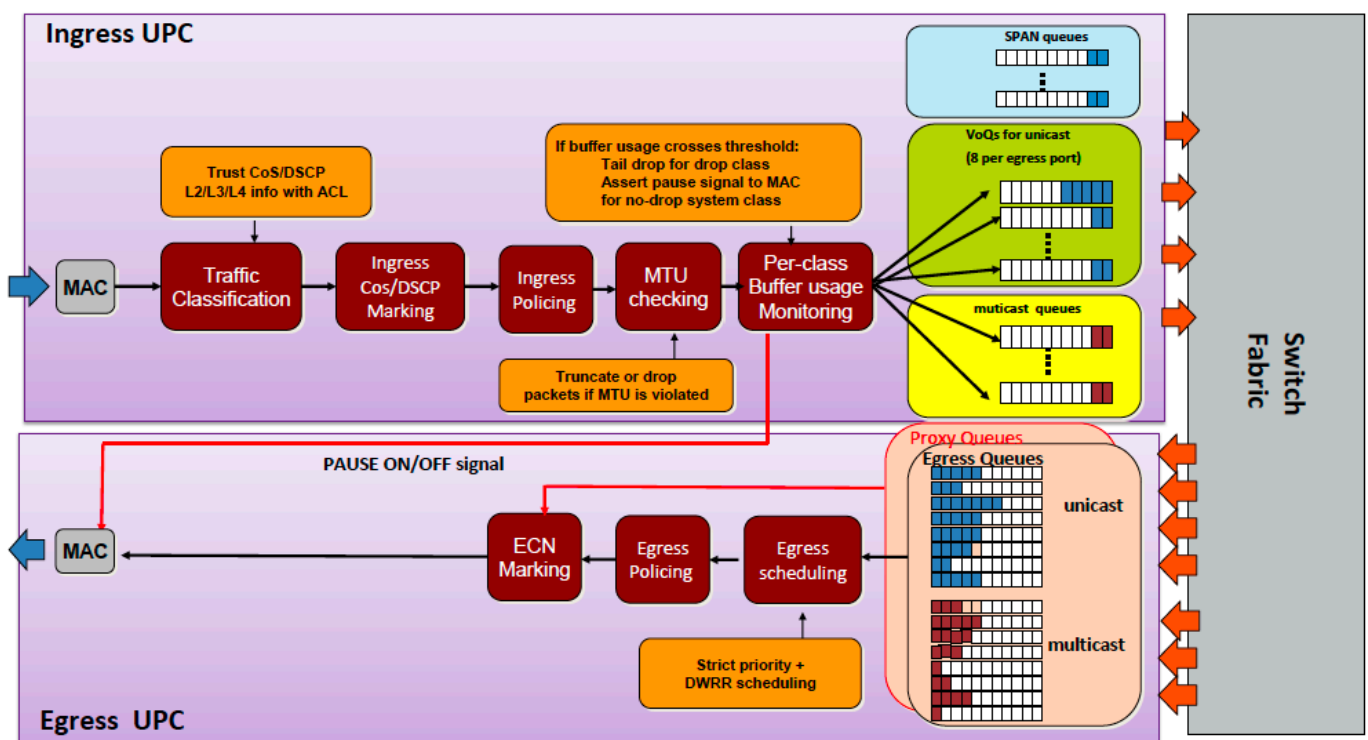
En la mayoría de los casos, los descensos de la salida serán siempre debido al Multicast/al tráfico transmitido/de la unidifusión desconocida.

¿Qué causa los descartes de la entrada?

Un puerto de egreso congestionado causará los búferes de egreso se llenará primero y entonces esto causará la presión posterior en el ingreso. Esto está solamente para el tráfico de unidifusión. Una vez que memorias intermedias de ingreso son llenas entonces podríamos potencialmente caer el tráfico en el ingreso que los resultados en la entrada desechan.

Esta explicación está en un nivel muy alto y fácil digerir pero hay un poco más a él especialmente cuando usted está mirando diversa clase de tráfico, a las colas de administración del tráfico etc. Hay un concepto de VOQ (cola de salida virtual) que se utilice con frecuencia en la plataforma del nexo. El VOQ es una asignación de memorias intermedias de ingreso para cada Clase de Servicio (CoS) del IEEE 802.1P por el puerto de egreso. Tan hay 8 VOQ por el puerto de egreso. La congestión en un puerto de egreso en un CoS eventually sangrará en congestionar el VOQ correspondiente en el puerto de ingreso. Una vez que el límite entonces se alcanza trafique conseguirá caído. Sin embargo no afecta al tráfico destinado para el otro CoSs u otras interfaces de egreso, así evitando al jefe de line (HOL) que bloquea, que haría de otra manera la congestión separarse.

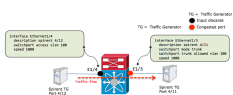
Aquí está una representación visual del flujo de tráfico del ingreso al puerto de egreso y de los diversos bloques en el juego



Ejemplo de Troubleshooting

Scenerio 1: Descartes de la entrada

Configuración de laboratorio:



Línea tráfico de la tarifa egressing e1/3 y el oversubscription posible

En una configuración simulada como arriba, usted conoce la causa del oversubscription pero en una producción ponga donde está bursty el perfil del tráfico él puede ser desafiador manchar hacia fuera los puertos de egreso congestionados sin embargo los comandos antedichos.

Los pasos enumerados ayudarán con la identificación de los puertos de egreso congestionados

Paso 1: Identifique los puertos con los descartes de la entrada

Entre los descartes vistos en el puerto e1/4

Paso 2: Identificación de ASIC

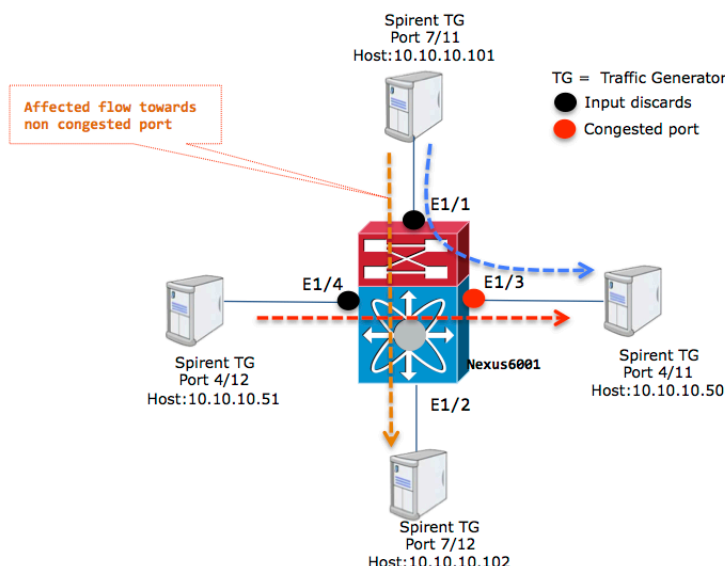
- ¿? Asocie la interfaz a la forma de número interna de ASIC (UPC) la salida abajo.
- ¿? Descubra el ingreso ASIC ID del puerto de ingreso ID en el cual notamos los descensos

Paso 3: Identifique el puerto congestionado salida

- ¿? Identificación del puerto de egreso congestionado con los contadores VOQ
- ¿? ¿Utilice el número de ASIC adentro? ¿contradice el voq ASIC-numérico? para descubrir que el puerto de egreso está contribuyendo a los descensos

Scenerio 2: Descartes de la entrada con HOLB (jefe de la línea bloqueo)

Configuración de laboratorio:



El flujo de tráfico de entrada en el puerto de ingreso que estén enviando el tráfico al puerto de

es el jefe clásico de la línea que bloquea el problema (HOLB).

La foto de los generadores de tráfico de Spirent muestra los flujos que son caídos. Los números del puerto son números del puerto de Spirent.

Traffic Aggregate View: Results 1

Streams > Detailed Stream Results | Change Result View | 1 of 1 | Select Tx Ports: All Ports | Select Rx Ports: All Ports

Change Counter Mode: Basic Mode | Resample

Drops towards non congested ports

Name/ID	Tx Port Name	Rx Port Names	Tx Count (Frames)	Rx Count (Frames)	Dropped Count (Frames)	Dropped Frame Percent	In-order Count (Frames)	Reordered Count (Frames)
StreamBloc...	Port //4/11	Port //4/12	0	0	0	0.000	0	0
StreamBloc...	Port //4/12	N/A	0	0	0	0.000	0	0
StreamBloc...	Port //4/12	Port //4/11	1,307,568	1,100,070	223,516	16.887	1,100,070	0
StreamBloc...	Port //7/11	Port //7/12	461,229	275,398	172,495	38.512	275,398	0
StreamBloc...	Port //7/11	Port //4/11	1,844,950	1,100,058	664,699	37.665	1,100,058	0

Mitigación HOLB: Límite del permiso VOQ

Para evitar este escenario, los VOQ (solamente para el tráfico de unidifusión) se pueden configurar con un umbral del conjunto.

Después de la configuración, los flujos hacia los puertos no congestionados no serán afectados.

Opinión del generador de tráfico de Spirent después de los config del límite VOQ

Streams > Detailed Stream Results | Change Result View | 1 of 1 | Select Tx Ports: All Ports | Select Rx Ports: All Ports

Change Counter Mode: Basic Mode | Resample

There are no dropped packets

Name/ID	Tx Port Name	Rx Port Names	Tx Count (Frames)	Rx Count (Frames)	Dropped Count (Frames)	Dropped Frame Percent	In-order Count (Frames)	Reordered Count (Frames)
StreamBloc...	Port //4/11	Port //4/12	0	0	0	0.000	0	0
StreamBloc...	Port //4/12	N/A	0	0	0	0.000	0	0
StreamBloc...	Port //4/12	Port //4/11	1,348,359	1,133,953	230,398	16.887	1,133,953	0
StreamBloc...	Port //7/11	Port //7/12	474,821	461,488	0	0.000	461,488	0
StreamBloc...	Port //7/11	Port //4/11	1,899,318	1,133,940	685,182	37.665	1,133,940	0

¿Aunque esta configuración muestra una ventaja clara en la prevención de los descensos debido a HOLB porqué está ésta no los config predeterminados?

Típicamente el tráfico en un entorno de producción podía ser bursty en la naturaleza.

Inhabilitando el umbral VOQ permitimos que memorias intermedias de ingreso absorban una explosión del micrófono del tráfico sin conseguir caídos. A menos que la situación autorice la necesidad de habilitar el límite VOQ, se recomienda para utilizar el valor por defecto que es dejarlo inhabilitado.

Mitigación HOLB: Clasificación de tráfico

Hay otro método para atenuar HOLB usando la configuración de QoS. Puesto que los discards del ingreso están afectando solamente a un VOQ specific que a su vez sea una clase specific QOS, usted puede asociar el tráfico afectado al puerto no congestionado a un diverso grupo QOS. De la salida abajo, los descartes del ingreso están afectando a la clase del grupo 0 QOS.

La configuración abajo asociará el QoS-grupo 2. del tráfico interesante.

1. Defina el ACL para el tráfico que no debe ser caído. El objetivo es clasificar este tráfico en un diverso grupo QoS así que no consigue afectado.

2. Clasificación de QoS

3. Config de QoS de la red

4. Aplique las diversas directivas. La red QoS es sistema de par en par mientras que la política de clasificación se puede aplicar a una sola interfaz.

5. Los descensos no se consideran para la clase del group2 de QoS

Información pertinente

[Ejemplo de la configuración de QoS de los 6000 Series Switch del nexa](#)