

# Guía de Configuración de WCCP en Plataformas Catalyst 6500 con Uso Alto de CPU

## Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Descripción general funcional de WCCP](#)

[WCCP y Catalyst 6500](#)

[Método de asignación de WCCP](#)

[Detalles del método de asignación basado en hash](#)

[Detalle del método de asignación basado en máscara](#)

[Método de redirección WCCP](#)

[Método de reenvío L3 \(GRE\)](#)

[Entrada - Redirección L3 \(GRE\) + Asignación de hash](#)

[Entrada - Redirección L3 \(GRE\) + Asignación de máscara](#)

[Salida - Redirección L3 \(GRE\) + Asignación de hash](#)

[Salida - Redirección L3 \(GRE\) + Asignación de máscara](#)

[Método de reenvío L2](#)

[Entrada - L2 + Asignación de hash](#)

[Entrada - L2 + Asignación de máscara](#)

[Salida - L2 + Asignación de hash](#)

[Salida - L2 + Asignación de máscara](#)

[Método de devolución WCCP](#)

[La entidad WCCP puede atender la solicitud](#)

[La entidad WCCP no puede atender la solicitud](#)

[Devolución de GRE](#)

[Mejora de la devolución L2](#)

[Resumen de las opciones WCCP](#)

[Recomendaciones de diseño de WCCP](#)

[Summary](#)

[Recomendaciones adicionales](#)

[Soluciones](#)

[ACNS](#)

[Comandos Show y Debug de WCCP IOS](#)

[Comandos de NetFlow](#)

[Defectos WCCP](#)

# Introducción

Este documento describe cómo utilizar Web Cache Communication Protocol (WCCP) en la plataforma Cisco Catalyst 6500 Series.

WCCP se diseñó originalmente como un método para interceptar el tráfico web (HTTP) y reenviarlo a un dispositivo de caché local, donde se podía servir a un cliente desde una ubicación local y conservar el costoso ancho de banda de la WAN.

Desde el punto de vista del usuario de la red, WCCP es transparente porque se utiliza en el nivel de red, sin ninguna configuración especial por parte del usuario, para identificar y redirigir el tráfico web que atraviesa un dispositivo de capa 3 (L3) a un dispositivo de caché local. Aunque WCCP se diseñó originalmente para el tráfico web, el método transparente de redirección se ha convertido en un mecanismo muy útil para abordar otros problemas con contenido de gran volumen en links de bajo volumen. Por esta razón, se agregó soporte de protocolo adicional a las versiones WCCP posteriores. Estas tecnologías adicionales incluyen protocolos como HTTP, HTTPS, FTP, transmisión de vídeo y tecnologías de almacenamiento en caché de archivos, como el sistema de archivos comunes de Internet (CIFS). Estas tecnologías son compatibles con las nuevas soluciones y plataformas de Cisco, como Wide Area File Services (WAFS), Wide Area Application Services (WAAS), las redes orientadas a aplicaciones (AON) y las capacidades mejoradas del software de redes de contenido y aplicaciones (ACNS).

La adopción de WCCP está aumentando a medida que las empresas implementan las herramientas de productividad más recientes, como la formación y las comunicaciones basadas en vídeo, así como el vídeo en directo y a demanda. Los esfuerzos por controlar los costes, como los Data Centers consolidados, crean la necesidad de que WCCP admita servicios de ancho de banda adicionales extremadamente altos.

Debido a la importancia de WCCP con las redes con contenido enriquecido de hoy en día, algunas plataformas, como Catalyst 6500, han implementado un rendimiento asistido por hardware con WCCP para reducir la carga de CPU requerida para el protocolo. Este documento describe cómo implementar WCCP en el Catalyst 6500 para maximizar la utilización del hardware y reducir la carga de la CPU.

## Prerequisites

### Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- WCCP
- Switches Cisco Catalyst serie 6500
- Software Cisco IOS®

### Componentes Utilizados

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

- Cisco Catalyst 6500 Series Switches
- Cisco IOS Software Release 12.1(50)SY o posterior con Supervisor Engine 2T (Policy Feature Card 4)
- Cisco IOS Software Release 12.2(18)SXD1 o posterior con Supervisor Engine 720 (Policy Feature Card 3)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

## Descripción general funcional de WCCP

La funcionalidad a la que se hace referencia genéricamente como WCCP en realidad implica tres componentes:

1. Funcionalidad implementada solamente en el router o switch
2. Funcionalidad implementada solamente en la entidad de procesamiento de tráfico, como una memoria caché web
3. WCCP implementado en ambos lados

Este documento examina estas tres características operativas de WCCP:

1. El método de **asignación** determina qué tráfico WCCP y qué dispositivo WCCP se eligen para el destino del tráfico. El protocolo WCCP admite varios dispositivos agrupados.
2. El método de **redirección** reenvía el flujo de tráfico al dispositivo WCCP cuando hay una necesidad de cambiar de la trayectoria de red normal que atravesaba el tráfico.
3. El método **return** determina cómo se devuelve el tráfico al router desde el dispositivo WCCP si no se pudo mantener el tráfico. En los casos en que el dispositivo WCCP hace el servicio de la solicitud, los paquetes se devuelven directamente al solicitante.

## WCCP y Catalyst 6500

Los Catalyst 6500 Supervisor Engine 2, Supervisor Engine 32 y Supervisor Engine 720 admiten estas características y métodos WCCP:

- WCCP versión 2 (WCCPv2)
- Método de asignación basado en hash
- Método de asignación basado en máscara (acelerado por hardware)
- Método de redirección de encapsulación de routing genérico (GRE) de capa 3 (acelerado por hardware en Supervisor Engine 32 y Supervisor Engine 720)
- Método de redirección de capa 2 (L2) (acelerado por hardware en Supervisor Engine 2, Supervisor Engine 32 y Supervisor Engine 720)
- método de retorno GRE
- Método de retorno L2 con Cisco IOS Software Release 12.2SXH (acelerado por hardware en Supervisor Engine 2, Supervisor Engine 32 y Supervisor Engine 720)

Para obtener más detalles sobre estas funciones, refiérase a [Configuración de WCCP en la Guía de Configuración de Cisco 6500 Series Cisco IOS Software, 12.2SX](#).

# Método de asignación de WCCP

La asignación WCCP determina qué tráfico redirige el protocolo WCCP y qué entidad WCCP recibe tráfico redirigido.

Cuando WCCP se configura en una interfaz de un router y en una entidad WCCP, el dispositivo de redirección (Catalyst 6500) necesita saber qué tráfico se redirige y dónde se enviará el tráfico. Las entidades WCCP dentro de un agrupamiento de grupos de servicio se comunican a través del protocolo WCCP con el Catalyst 6500; sin embargo, se selecciona un dispositivo WCCP para representar el clúster a fin de controlar cómo funciona el clúster (por el método de asignación, el método de redirección, etc.). El dispositivo WCCP y el router pueden negociar el método por el cual los paquetes se distribuyen entre las memorias caché web en un grupo de servicios. Un grupo de servicios se define como una relación de muchos a muchos entre hasta 32 routers y 32 entidades WCCP. La negociación es por grupo de servicio; por lo tanto, las memorias caché web que participan en varios grupos de servicios pueden negociar un método de asignación diferente para cada grupo de servicios. Los servicios WCCP disponibles actualmente son:

## Servicio WCCP Protocolo

caché web	HTTP
53	Caché DNS
60	FTP
61	WAAS - reenviar
62	WAAS - inverso
70	HTTPS
80	Protocolo de transmisión en tiempo real (RTSP)
81	Microsoft Media Server (MMS) sobre UDP (MMSU)
82	MMS sobre TCP (MMST)
83	RTSP con UDP (RTSPU)
89	CIFS-Cache WAAS
98	Caché web personalizada
99	Proxy inverso
90-97	Configurable por el usuario *

\* Los servicios configurables por el usuario se implementan en el Catalyst 6500 con un comando de nivel de interfaz aplicado a una dirección entrante o saliente. Las implicaciones de la elección de entrante o saliente se discuten más adelante, pero el método preferido es el entrante, ya que una lista de redirección se puede combinar con WCCP para obtener el máximo rendimiento del hardware.

Una vez configurado para WCCP, un router anuncia los métodos de asignación soportados para un grupo de servicio en los mensajes de comunicaciones WCCP. La ausencia de tal mensaje implica que el Catalyst 6500 soporta solamente el método de asignación basado en hash predeterminado.

Una vez finalizada la negociación entre el Catalyst 6500 y el dispositivo WCCP, la entidad designada por WCCP, a través de WCCP, informa al Catalyst 6500 qué tráfico se redirigirá y a qué entidad o entidades WCCP se asigna el tráfico. A modo de ejemplo, la entidad WCCP puede informar al Catalyst 6500 para redirigir todo el tráfico web desde una subred determinada a los motores de caché 1 - 4 del grupo de servicio cuando hay más de cuatro dispositivos WCCP disponibles.

Hay dos métodos de asignación disponibles para WCCP:

1. **La asignación basada en hash** (predeterminada) utiliza un algoritmo hash basado en software junto con las directivas del dispositivo designado por WCCP para determinar qué dispositivo WCCP recibe tráfico. En una plataforma Supervisor Engine 32 o Supervisor Engine 720, los recursos de hardware de NetFlow se utilizan para aplicar algún nivel de asistencia de hardware.
2. **La asignación basada en máscara** utiliza las capacidades de hardware del Catalyst 6500, específicamente la memoria direccionable de contenido ternario (TCAM) de la lista de control de acceso (ACL), para asignar tráfico a las entidades WCCP. Éste es el método preferido.

Todos los dispositivos dentro de un grupo de servicios WCCP deben utilizar el mismo método de asignación. Los métodos de asignación se configuran en la entidad WCCP y son aprendidos por Catalyst 6500. Consulte [Recomendaciones de diseño de WCCP](#) para obtener más detalles.

## Detalles del método de asignación basado en hash

El mecanismo de asignación basado en hash se basa en un algoritmo realizado en el software. Para aprovechar el algoritmo hash, el primer paquete en un flujo determinado se envía desde la trayectoria de hardware a la trayectoria de software donde se realiza el hash.

El software realiza un hash XOR de varios componentes del flujo y viene con un hash que divide los flujos de tráfico en las diversas entidades WCCP. El mecanismo hash determina cómo se distribuye el tráfico entre las entidades WCCP disponibles.

El resultado del hash se programa en la tabla de NetFlow de hardware donde se reenvían los paquetes subsiguientes en ese flujo. Independientemente de los campos disponibles para hashing por WCCP, se utiliza el tuplo completo de cinco tuplas. Esto significa que NetFlow se pone en modo de interfaz y flujo completo cuando se habilita WCCP. Esto tiene implicaciones en otras funciones que pueden requerir recursos de NetFlow. Consulte la sección [Defectos WCCP](#) para obtener más detalles.

Una pregunta común sobre WCCP en Catalyst 6500 es: "¿Por qué aumenta la utilización de la CPU cuando habilito WCCP?" Cuando se utilizan asignaciones basadas en hash, el procesamiento basado en software del paquete inicial en cada flujo supone una carga para la CPU y, con frecuencia, es la causa del aumento de la utilización. Con el hardware de reenvío de la tarjeta de función de política 3 (PFC3) disponible actualmente, si WCCP está configurado como función de egreso o si la asignación basada en hash está en uso (entrada o salida), siempre se requiere cierto nivel de procesamiento de software.

El uso del método de asignación basado en hash afecta a estas características:

- **Tabla NetFlow:** el número de entradas soportadas por la PFC es limitado, y la máscara de flujo cambia a la interfaz de flujo completo para toda la tabla de NetFlow.
- **Utilización de CPU:** hay un aumento en el uso de CPU, ya que el primer paquete en cada flujo se conmuta por software.
- **Rendimiento:** la velocidad a la que se envía el tráfico a la CPU para la búsqueda está limitada de modo que la CPU esté protegida.
- **Funciones de NetFlow:** otras funciones que utilizan recursos de NetFlow podrían verse afectadas si WCCP consume los recursos de NetFlow.

Las limitaciones e implicaciones causadas por el requisito de asignación basada en hash para el

procesamiento de software son aplicables tanto al tráfico de entrada como al de salida. El impacto en la CPU se puede exacerbar si la red experimenta patrones de tráfico atípicos, como un ataque de denegación de servicio (DoS). En un ataque típico o brote de gusanos, cada paquete enviado por un host se envía a un nuevo destino o puerto, lo que hace que cada paquete se procese en el software. Dado que el tráfico redirigido WCCP se envía explícitamente a la CPU para el procesamiento del primer paquete, hay métodos de protección limitados. El uso de entradas ACL 'deny' en la interfaz puede limitar lo que se envía a la CPU; sin embargo, no hay limitadores de velocidad ni otras protecciones contra estos tipos de ataques.

## Detalle del método de asignación basado en máscara

La asignación basada en la máscara se maneja de manera diferente dependiendo de si está configurada en el ingreso o en la salida.

Con la asignación basada en máscara de ingreso, la máscara se programa en la ACL TCAM antes del reenvío de paquetes, por lo que no se necesitan la tabla NetFlow ni el procesamiento de software. La entidad WCCP elige un número de bloques hash y asigna una máscara de dirección y un dispositivo WCCP a cada bloque de memoria. Una vez completadas las asignaciones, el supervisor programa una entrada TCAM y una adyacencia de hardware para cada bloque de memoria y redirige los paquetes que coinciden con la máscara de dirección al dispositivo WCCP asociado mediante una reescritura L2.

Si WCCP se configura como una función de ingreso, puede utilizar una entrada de adyacencia de redirección ACL en la tabla de ACL de hardware. Una vez que WCCP coincide con la entrada, utiliza una adyacencia apropiada para realizar una reescritura L2 o una encapsulación GRE. Por lo tanto, cuando se utiliza la asignación de máscara en el ingreso, tanto la reescritura L2 (Supervisor Engine 2, Supervisor Engine 32 y Supervisor Engine 720) como la encapsulación GRE (Supervisor Engine 32 y Supervisor Engine 720 solamente) se realizan en el hardware.

Si WCCP se configura como una función de salida, las adyacencias de redirección ACL no se soportan en el hardware porque los paquetes en el flujo ya han sido enrutados por el sistema. El primer paquete de un flujo se envía al software para su procesamiento. Una vez determinada la adyacencia de redirección adecuada, se programa en el hardware de NetFlow (en lugar de ACL TCAM), donde la entrada señala a una adyacencia que realiza una reescritura de L2 o una encapsulación GRE. Los paquetes subsiguientes en el flujo son redirigidos en hardware por el hardware de NetFlow.

**Nota:** Si WCCP se configura como una función de egreso, la asignación de máscara requiere el procesamiento de software, lo que anula cualquier beneficio del método de asignación basado en máscara.

De las dos opciones basadas en la máscara, sólo la asignación basada en la máscara de ingreso permite el reenvío completo basado en hardware para los paquetes iniciales y subsiguientes. Cualquier otra opción, como el uso de la asignación basada en hash o el procesamiento de egreso, causa el switching de software del paquete inicial y el reenvío conmutado de hardware de NetFlow de los paquetes subsiguientes.

## Método de redirección WCCP

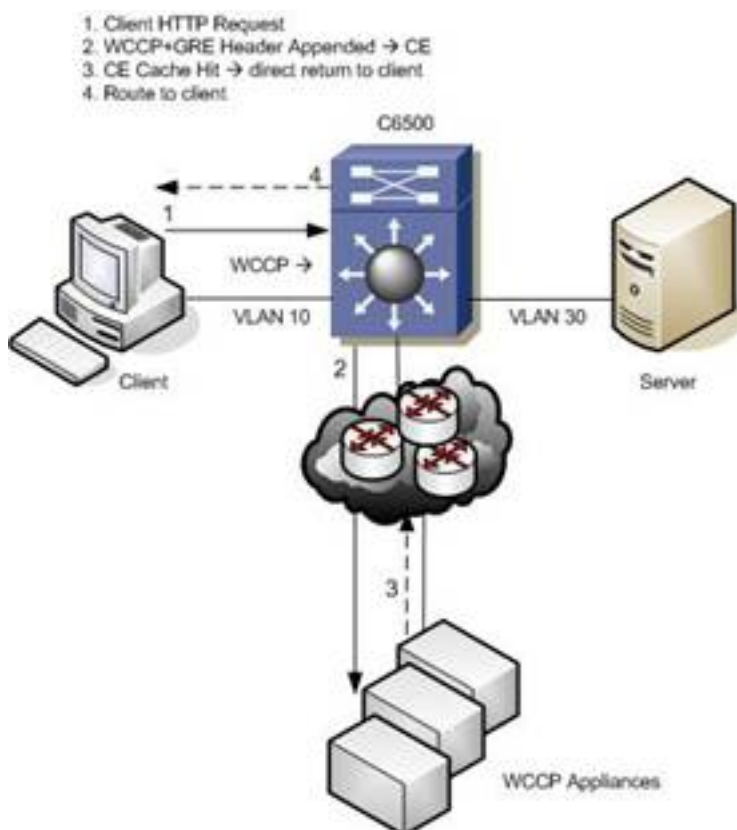
La entidad WCCP, no el Catalyst 6500, dicta las tablas hash y los conjuntos de máscara/valor al Catalyst 6500, por lo que la configuración del método de redirección se realiza en ese dispositivo y no en el switch Catalyst 6500. El Catalyst 6500 determina el mejor método de redirección disponible, basado en las comunicaciones WCCP con la entidad/grupo WCCP. Esta negociación determina cómo se reenvía el tráfico redirigido al dispositivo. Hay dos opciones de redirección: L3 (GRE) y L2 (dirección MAC reescribe).

Con WCCPv1, la única opción es la redirección L3, también conocida como encapsulación GRE. Con la redirección L3, cada paquete redirigido WCCP se encapsula en un encabezado GRE marcado con un tipo de protocolo 0x883E seguido de un encabezado de redirección WCCP de cuatro octetos, que se envía posteriormente al dispositivo WCCP (como un motor de caché).

Con la introducción de WCCPv2, se agregó la redirección L2, también conocida como redirección WCCP acelerada, para aprovechar las plataformas de switching de hardware como Catalyst 6500. Cuando WCCP utiliza la redirección L2, el dispositivo WCCP y Catalyst 6500 deben ser adyacentes L2 (dentro de la misma VLAN L2). El tráfico L2 redirigido no utiliza la encapsulación GRE; en su lugar, el Catalyst 6500 reescribe la dirección de destino MAC a la de la entidad WCCP conectada a L2 y la reenvía a través de conmutación de hardware normal.

**Nota:** El método de reenvío al dispositivo WCCP puede no ser el mismo que el dispositivo WCCP utiliza para enviar el tráfico de vuelta al Catalyst 6500. WCCP se utiliza para negociar un método de reenvío y devolución que ambos dispositivos soportan. Consulte [Método de devolución WCCP](#).

## Método de reenvío L3 (GRE)



La operación WCCP L3 implica el uso de GRE como método de encapsulación. Los paquetes redirigidos se encapsulan en un encabezado GRE con un tipo de protocolo 0x883e, junto con un

encabezado de redirección WCCP de 4 bytes que incluye un ID de servicio y una cubeta hash coincidentes (sólo WCCPv2). El uso de GRE permite que el cliente WCCP esté separado del Catalyst 6500 por varios saltos L3 (enrutados).

En este escenario, las opciones disponibles para la redirección WCCP incluyen:

1. Entrada: redirección L3 (GRE) + asignación de hash; esto requiere el procesamiento del software.
2. Entrada: redirección L3 (GRE) + asignación de máscara; esto requiere el procesamiento completo del hardware y sólo está disponible en Supervisor Engine 32 o Supervisor Engine 720.
3. Salida - redirección L3 (GRE) + asignación de hash; esto requiere el procesamiento del software.
4. Salida: redirección L3 (GRE) + asignación de máscara; esto requiere el procesamiento del software.

### **Entrada - Redirección L3 (GRE) + Asignación de hash**

En Supervisor Engine 2, cada paquete GRE se envía a la tarjeta de función de switch multicapa (MSFC) para su procesamiento. Debido a que la encapsulación GRE no se soporta en el hardware, la MSFC debe aplicar los encabezados GRE y WCCP, lo que fuerza el switching de software para todo el tráfico.

Con el método de asignación basado en hash, Supervisor Engine 32 y Supervisor Engine 720 reenvían el primer paquete de cada flujo en el software para que se establezca una entrada de tabla de NetFlow. El paquete se encapsula luego en GRE (la encapsulación y el reenvío del paquete inicial se realiza en software) y se reenvía al dispositivo WCCP.

El establecimiento de la entrada de NetFlow afecta la utilización de la CPU, pero el reenvío de paquetes subsiguiente se realiza en hardware para Supervisor Engine 720 y Supervisor Engine 32. Los patrones de tráfico, especialmente el número de flujos únicos, dictan cuánto se utiliza la CPU. Si se consumen los recursos de NetFlow del Catalyst 6500, todo el tráfico se reenvía en el software.

Los recursos de NetFlow del PFC supervisor difieren entre las distintas plataformas. Actualmente, los recursos de NetFlow más grandes están disponibles en PFC-3BXL en la plataforma Supervisor Engine 720.

### **Entrada - Redirección L3 (GRE) + Asignación de máscara**

En el Supervisor Engine 2, cada paquete GRE se envía a la MSFC para su procesamiento. Debido a que la encapsulación GRE no se soporta en el hardware, la MSFC debe aplicar los encabezados GRE y WCCP, lo que fuerza el switching de software para todo el tráfico.

Con el método de asignación basada en máscara, Supervisor Engine 32 y Supervisor Engine 720 reenvían los paquetes iniciales y subsiguientes en el hardware, porque GRE es soportado de forma nativa, y la asignación de máscara utiliza el hardware TCAM ACL para el reenvío.

### **Salida - Redirección L3 (GRE) + Asignación de hash**



En el Supervisor Engine 2, cada paquete se envía a la MSFC para su procesamiento. Debido a que la encapsulación GRE no se soporta en el hardware, la MSFC debe aplicar los encabezados GRE y WCCP, lo que fuerza el switching de software para todo el tráfico.

Con el método de asignación basado en hash con Supervisor Engine 32 y Supervisor Engine 720, Catalyst 6500 reenvía el paquete inicial de cada flujo en el software de modo que se establezca la entrada de tabla de NetFlow. El paquete se encapsula luego en GRE y se reenvía a la entidad WCCP.

El establecimiento de la entrada de NetFlow afecta la utilización de la CPU, pero el reenvío de paquetes subsiguiente se realiza en hardware. Los patrones de tráfico, especialmente el número de flujos únicos, dictan cuánto se utiliza la CPU. Si se consumen los recursos de NetFlow del Catalyst 6500, todo el tráfico se reenvía en el software.

Los recursos de NetFlow del PFC supervisor difieren entre las diversas plataformas. Actualmente, los recursos de NetFlow más grandes están disponibles en PFC-3BXL en la plataforma Supervisor Engine 720.

### **Salida - Redirección L3 (GRE) + Asignación de máscara**

En el Supervisor Engine 2, cada paquete se envía a la MSFC para su procesamiento. Debido a que la encapsulación GRE no se soporta en el hardware, la MSFC debe aplicar los encabezados GRE y WCCP, lo que fuerza el switching de software para todo el tráfico.

Con el método de asignación basado en máscara con Supervisor Engine 32 y Supervisor Engine 720, el primer paquete de cada flujo se conmuta por software de modo que se establezca la entrada de la tabla NetFlow. Ninguno de los supervisores admite la programación de adyacencia de ACL de salida, lo que fuerza este procesamiento de software y utiliza recursos de NetFlow (en lugar de hardware ACL TCAM) para el paquete inicial en cada flujo. El paquete se encapsula luego en GRE y se reenvía al dispositivo WCCP.

El establecimiento de la entrada de NetFlow afecta la utilización de la CPU, pero el reenvío de paquetes subsiguiente se realiza en hardware. Los patrones de tráfico, especialmente el número de flujos únicos, dictan cuánto se utiliza la CPU. Si se consumen los recursos de NetFlow del Catalyst 6500, todo el tráfico se reenvía en el software.

Los recursos de NetFlow del PFC supervisor difieren entre las diversas plataformas. Actualmente, los recursos de NetFlow más grandes están disponibles en PFC-3BXL en la plataforma Supervisor Engine 720.

### **Método de reenvío L2**

Con el reenvío de L2, las entidades WCCP (ACNS, WAFS, WAAS, etc.) dentro de un grupo de servicios forman parte de la misma subred y son L2 adyacentes al Catalyst 6500. Esto permite un alto rendimiento y una baja redirección del tráfico de latencia. La interfaz de ingreso (donde se configura WCCP) y la interfaz donde se ubican los dispositivos WCCP deben estar en diferentes VLAN.

**Nota:** Con la redirección L2, el paquete se reescribe con el MAC de origen configurado en el router y el MAC de destino configurado en el motor de memoria caché. La única desventaja

de este método de redirección es que el motor de memoria caché debe ser **L2 alcanzable** por el Catalyst 6500 y debe residir en una **interfaz L3 diferente** que la interfaz WCCP de ingreso configurada.

**Nota:** El método de reenvío al dispositivo WCCP puede no ser el mismo que el dispositivo WCCP utiliza para enviar el tráfico de vuelta al Catalyst 6500. WCCP se utiliza para negociar un método de reenvío y devolución que ambos dispositivos soportan. Consulte [Método de devolución WCCP](#).

Las opciones disponibles para la redirección WCCP en este escenario incluyen:

- Ingreso - redirección L2 + asignación de hash; esto requiere el procesamiento del software.
- Ingreso: redirección L2 + asignación de máscara, esto requiere un procesamiento de hardware completo y se recomienda.
- Salida - redirección L2 + asignación de hash; esto requiere el procesamiento del software.
- Salida - redirección L2 + asignación de máscara; esto requiere el procesamiento del software.

### **Entrada - L2 + Asignación de hash**

Cuando se configura en el ingreso con asignación de troceo L2 +, el tráfico WCCP envía el primer paquete en cada flujo que se conmuta por software, lo que crea una entrada de NetFlow en la tabla NetFlow de hardware.

**Nota:** La máscara de flujo de NetFlow se establece en el modo de flujo completo de la interfaz, lo que podría afectar a otras funciones de NetFlow configuradas en el switch.

Dado que WCCP es un mecanismo sin estado, la información no se mantiene en el software; más bien, se mantiene en el hardware como entradas en la tabla NetFlow. El tráfico subsiguiente en el flujo se reenvía en el hardware mientras exista una entrada de tabla de NetFlow.

El establecimiento de la entrada de NetFlow afecta la utilización de la CPU, pero el reenvío de paquetes subsiguiente se realiza en hardware. Los patrones de tráfico, especialmente el número de flujos únicos, dictan cuánto se utiliza la CPU. Si se consumen los recursos de NetFlow del Catalyst 6500, todo el tráfico se reenvía en el software.

Los recursos de NetFlow del PFC supervisor difieren entre las diversas plataformas. Actualmente, los recursos de NetFlow más grandes están disponibles en PFC-3BXL en la plataforma Supervisor Engine 720.

### **Entrada - L2 + Asignación de máscara**

Cuando se configura en el ingreso, la asignación de máscara L2 + es el método WCCP más eficiente admitido en el Catalyst 6500. Todo el tráfico es conmutado por hardware, incluido el paquete inicial en cada flujo. No se requiere redirección de software; el reenvío de paquetes inicial y subsiguiente son provistos por el hardware.

Los recursos TCAM de ACL de hardware del Catalyst 6500 se utilizan para preprogramar las entradas de hardware antes de que se reciban los paquetes WCCP.

Para utilizar este método y utilizar la conmutación de hardware completa, la entidad WCCP también debe soportar la redirección L2 y el método de asignación basado en máscara. La configuración de este método se completa en la entidad WCCP, y Catalyst 6500 negocia el mejor método durante las comunicaciones iniciales WCCP con la entidad/grupo WCCP.

### Salida - L2 + Asignación de hash

Con la asignación de hash de salida L2 +, el tráfico WCCP envía el primer paquete en cada flujo para ser conmutado por software, lo que crea una entrada de NetFlow en la tabla NetFlow de hardware.

**Nota:** La máscara de flujo de NetFlow se establece en el modo de flujo completo de la interfaz, lo que podría afectar a otras funciones de NetFlow configuradas en el switch.

Además, cuando se configura en la dirección de salida, se requiere una búsqueda adicional de la base de información de reenvío (FIB) en el primer paquete del flujo para determinar la adyacencia asociada con el CE, que requiere la recirculación de paquetes dentro del Catalyst 6500. Los paquetes subsiguientes son conmutados por NetFlow en el hardware.

El establecimiento de la entrada de NetFlow afecta la utilización de la CPU, pero el reenvío de paquetes subsiguiente se realiza en hardware. Los patrones de tráfico, especialmente el número de flujos únicos, dictan cuánto se utiliza la CPU. Si se consumen los recursos de NetFlow del Catalyst 6500, todo el tráfico se reenvía en el software.

Los recursos de NetFlow del PFC supervisor difieren entre las diversas plataformas. Actualmente, los recursos de NetFlow más grandes están disponibles en PFC-3BXL en la plataforma Supervisor Engine 720.

### Salida - L2 + Asignación de máscara

Cuando se configura en la dirección de salida, la asignación de máscara L2 + conmuta el primer paquete en cada flujo en el software, al igual que el caso de asignación de hash L2 +. Los paquetes subsiguientes son conmutados por NetFlow en el hardware.

**Nota:** La máscara de flujo de NetFlow se establece en el modo de flujo completo de la interfaz, lo que podría afectar a otras funciones de NetFlow configuradas en el switch.

El PFC2 y el PFC3 no soportan la programación de adyacencia de ACL de salida, lo que fuerza el procesamiento de software para el paquete inicial en cada flujo; los paquetes subsiguientes en el flujo se reenvían en el hardware.

El establecimiento de la entrada de NetFlow afecta la utilización de la CPU, pero el reenvío de paquetes subsiguiente se realiza en hardware. Los patrones de tráfico, especialmente el número de flujos únicos, dictan cuánto se utiliza la CPU. Si se consumen los recursos de NetFlow del Catalyst 6500, todo el tráfico se reenvía en el software.

Los recursos de NetFlow del PFC supervisor difieren entre las diversas plataformas. Actualmente, los recursos de NetFlow más grandes están disponibles en PFC-3BXL en la plataforma

## Método de devolución WCCP

### La entidad WCCP puede atender la solicitud

Cuando WCCP se utiliza para interceptar el tráfico y la entidad WCCP realiza una operación completa en esos paquetes, los paquetes están listos para ser enviados de vuelta al cliente desde el dispositivo WCCP. Este tráfico procesado normalmente, que se dirige de vuelta al cliente en la red, no requiere ninguna encapsulación especial cuando se envía de vuelta del dispositivo WCCP hacia el cliente.

Debido a que la intercepción de WCCP ha dado como resultado que la solicitud del cliente se haya atendido correctamente (archivo de la caché, flujo dividido de la caché, archivo de WAAS), se puede enviar de vuelta a la red como tráfico normal con la dirección de destino en los paquetes como el solicitante original. Este tráfico puede ser normalmente L3/conmutado por el Catalyst 6500 si está en la trayectoria de red del dispositivo WCCP al cliente; con un dispositivo WCCP conectado a L2, el tráfico se encuentra en la ruta de red. No se necesita encapsulación para enviarla de vuelta desde el dispositivo WCCP al Catalyst 6500 porque el destino es ahora el cliente original en lugar de un servidor en Internet o la intranet. La red entonces maneja esto como cualquier otro flujo de tráfico IP y utiliza el reenvío de hardware en el Catalyst 6500 para devolver el tráfico solicitado al cliente.

### La entidad WCCP no puede atender la solicitud

En algunos casos en los que la entidad WCCP no puede realizar la operación solicitada, es posible que el dispositivo WCCP deba enviar el tráfico de vuelta al Catalyst 6500 y conservar el destino original de los paquetes. El reenvío de este tráfico desde la entidad WCCP sin encapsulación puede dar lugar a loops de tráfico. Para ocultar un intento de servicio infructuoso del cliente y enviar los paquetes al destino original para ser atendidos, los paquetes deben permanecer inalterados, ser colocados nuevamente en su trayectoria de reenvío original y reenviados sin intercepción WCCP al destino original.

En el método de retorno WCCP, WCCP se puede utilizar para encapsular estos paquetes, enviarlos de vuelta al dispositivo que los interceptó en primer lugar, eliminar cualquier encapsulación y colocarlos nuevamente en la trayectoria de reenvío desde la que fueron interceptados. Estos paquetes deben enviarse normalmente como si nunca hubieran sido interceptados por WCCP.

Algunos ejemplos de estos casos son:

- Caché de tráfico sobrecargado, donde se omite el tráfico
- Reglas en dispositivos de caché que niegan a la entidad WCCP el servicio del tráfico
- Tráfico omitido que busca un servicio no disponible en el dispositivo

En este momento, este método de retorno se puede hacer solamente con encapsulación GRE y todavía no se soporta en ningún hardware Catalyst 6500. Si se envían grandes cantidades de tráfico de vuelta al Catalyst 6500 con este método, podría producirse una alta utilización de la CPU porque este tráfico se procesa en el software. En Cisco IOS Software Release 12.1(18)SXH,

existe un método de retorno L2 soportado por el hardware Catalyst 6500.

## Devolución de GRE

En las versiones de software del IOS de Cisco anteriores a 12.2(18)SXH, el único método de retorno admitido para el Catalyst 6500 es la encapsulación GRE. Además del encabezado GRE agregado al tráfico de retorno, también se agrega un encabezado WCCP. Aunque el GRE se soporta nativamente en el hardware de Supervisor Engine 32 y Supervisor Engine 720, este encabezado adicional hace que el GRE no esté asistido por hardware. Tenga en cuenta que tanto el Catalyst 6500 como el dispositivo WCCP deben soportar y negociar el método de retorno L2.

No existe soporte de hardware GRE en el Supervisor Engine 2 para cualquier retorno GRE, ingreso, egreso o WCCP. Para procesar este tipo de desencapsulación GRE, el software Cisco IOS programa la adyacencia de recepción del túnel WCCP GRE en la interfaz habilitada para WCCP para apuntar al procesador de ruta (RP), lo que da como resultado el procesamiento de software del tráfico de retorno.

El uso de listas de redirección en el Catalyst 6500 para evitar el tráfico que puede ser necesario devolver a través de GRE es un método efectivo para reducir los requisitos de procesamiento de software del tráfico que se enviaría de regreso desde la entidad WCCP. Esto es mucho más efectivo que tener el tráfico denegado en la entidad WCCP y obligarlo a ser encapsulado GRE y enviado de vuelta al Catalyst 6500.

Recuerde que el grupo de servicios WCCP es escalable. Si se omite el exceso de tráfico debido a la carga, se devuelve este tráfico, lo que crea carga de CPU en el Catalyst 6500. El único método para evitar esta situación es la correcta ampliación o incluso la generación excesiva del grupo de servicios WCCP.

## Mejora de la devolución L2

En 12.2(18)SXH, una opción permite a la entidad WCCP reescribir la dirección MAC L2 en lugar de encapsular el tráfico de retorno. Esta mejora de retorno de L2 (ID de bug Cisco CSCuk59825) permite el procesamiento de hardware del tráfico devuelto cuando WCCP está configurado para utilizar la redirección de ingreso con asignación de máscara.

## Resumen de las opciones WCCP

Cuando se implementa en Catalyst 6500, WCCP ofrece muchas opciones de configuración, como se muestra en esta tabla. Tenga en cuenta que el dispositivo WCCP negocia estas opciones y controla qué opciones utiliza el Catalyst 6500. La configuración se realiza en el lado del dispositivo WCCP de la conexión WCCP.

Método de redirección	Asignación Método	Acceso/ Egress	Resultado de switching
L2	Hash	Acceso	Procesamiento de software
<b>L2 (recomendado)</b>	<b>Máscara</b>	<b>Acceso</b>	<b>Procesamiento de hardware completo con ACL TCAM</b>
L2	Hash	Egress	Procesamiento de software
L2	Máscara	Egress	Procesamiento de software

GRE	Hash	Acceso	Procesamiento de software
GRE (PFC3 o posterior)	Máscara	Acceso	Procesamiento completo de hardware con flujo completo de NetFlow
GRE	Hash	Egress	Procesamiento de software
GRE	Máscara	Egress	Procesamiento de software

Desde el punto de vista del hardware, todas las configuraciones WCCP de salida requieren el procesamiento del software y el impacto en el uso de la CPU. El procesamiento de software también se requiere en el ingreso cuando se utiliza el método de asignación basado en hash y produce el mismo impacto potencial en la utilización de la CPU.

El método recomendado para la implementación de WCCP en el Catalyst 6500 es la redirección L2 con asignación de máscara y, cuando está disponible, la devolución L2.

**Consejo:** Solo una opción garantiza un reenvío completo y de alto rendimiento basado en hardware: la **redirección L2 basada en ingreso con asignación de máscara** en Supervisor Engine 2, Supervisor Engine 32 y Supervisor Engine 720.

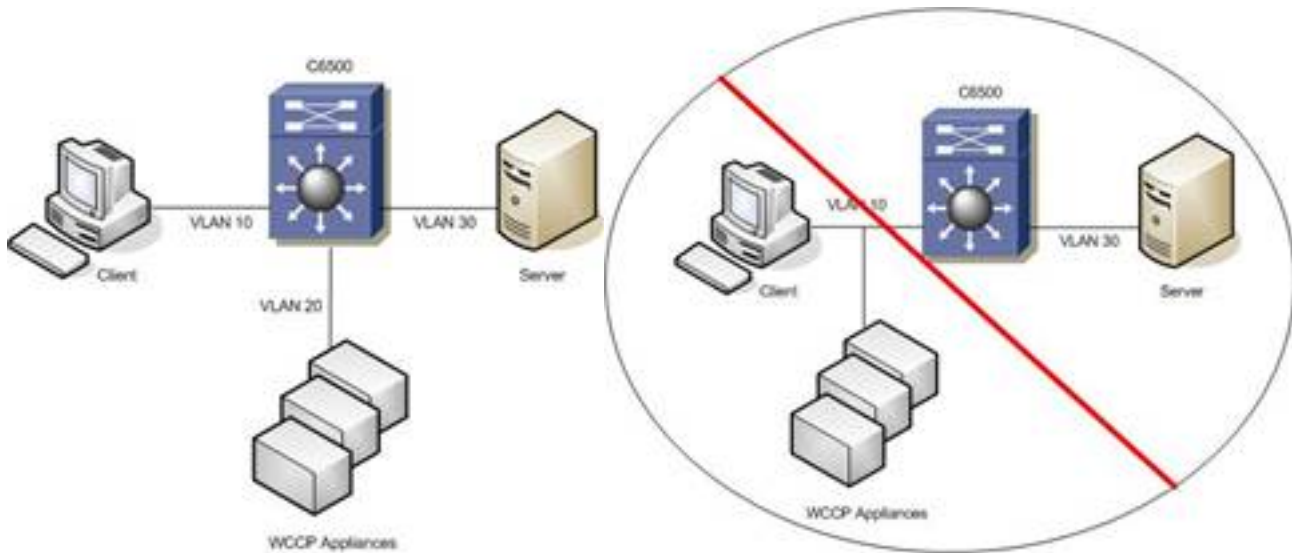
## Recomendaciones de diseño de WCCP

Utilice estas recomendaciones de configuración para determinar el mejor método de implementación de WCCP para su situación.

### Summary

Diseñe la red de modo que el ingreso WCCP se pueda utilizar como método de redirección. Un buen método de diseño es tener un switchblock de almacenamiento en caché como parte de una red de distribución jerárquica de L3; esto garantiza que el tráfico con servicio WCCP se pueda identificar en unos pocos puertos de ingreso importantes.

- Utilice 12.2(18)SXF7 o el software Cisco IOS más reciente.
- Identifique y redirija el tráfico en las interfaces de ingreso.
- Utilice dispositivos WCCP que admitan el método de redirección L2.
- Utilice dispositivos WCCP que admitan el método de asignación basado en máscara.
- Si es posible, utilice una lista de redirección en el Catalyst 6500 para el tráfico que no puede ser atendido por el dispositivo WCCP.
- Ajuste los temporizadores de NetFlow con la salida o cualquier configuración de asignación basada en hash con Supervisor Engine 720.
- Los dispositivos WCCP deben tener un entorno L3 dedicado y una interfaz SVI/VLAN.



Además, Cisco Advanced Service recomienda estas consideraciones de diseño:

- En un entorno que no es completamente redireccionado de L2 con asignación de máscara, Supervisor Engine 720 no funciona mejor que la plataforma Supervisor Engine 2. No actualice el hardware y espere un mejor rendimiento en esta situación.
- Para implementaciones de sitios centrales de gran tamaño con requisitos de tráfico de gran volumen, considere un diseño con routing basado en políticas (PBR) y Cisco Content Switching Model (CSM)/Application Control Engine (ACE) para la interceptación y el reenvío de tráfico.
- WCCPv2 funciona como se espera en circunstancias perfectas. Sin embargo, en algunas circunstancias, el uso de la CPU en el router puede alcanzar altos niveles que hacen que el dispositivo no se pueda utilizar y que requieren recarga:

WCCPv2 se remonta al modo de asignación basado en máscara L2 acelerada por hardware de ingreso a cualquier otro modo que requiera la CPU en la MSFC. WCCP está configurado incorrectamente (por ejemplo, egress en lugar de ingress o hash L2 en lugar de asignación de máscara).

- Cualquier implementación de WCCP de gran volumen con Catalyst 6500 (almacenamiento en caché, transmisión, WAAS u otros escenarios de "alta velocidad de tráfico") debe probarse el rendimiento con tráfico en directo antes de la implementación de producción completa.

## Recomendaciones adicionales

Utilice una lista de redirección en el switch para evitar los paquetes que se envían de vuelta al Catalyst 6500. Si alguna regla de los dispositivos de caché se puede mover al Catalyst 6500 como una lista de redirección, esto puede proporcionar un mejor rendimiento del hardware.

Los recursos de NetFlow en la plataforma Supervisor Engine 720 se pueden agotar rápidamente si utiliza cualquier método que no sea la asignación de máscara de entrada-L2. Supervisor Engine 720 no proporciona un mejor rendimiento que Supervisor Engine 2 con cualquier otro método.

En los casos en los que el Supervisor Engine 720 o el Supervisor Engine 32 se deben utilizar en un diseño no óptimo, considere el uso del comando **mls ip netflow create software-mode fast** para acelerar el procesamiento de NetFlow del paquete inicial WCCP. Esto elimina las mejoras agregadas a Supervisor Engine 32 y Supervisor Engine 720 NetFlow y proporciona un

rendimiento igual al del hardware de NetFlow de Supervisor Engine 2.

La configuración para un motor de contenido (CE) de Cisco para la asignación de máscara es:

- **wccp versión 2**
- **lista del router WCCP** *number ip-address*
- **wccp servicio router-list-num número mask-assigned**

Utilice estos comandos para revisar la utilización de NetFlow y determinar si WCCP está utilizando las entradas de NetFlow y está utilizando el procesamiento de software:

- **show mls netflow table-contention detailed**
- **show mls netflow ip sw-installed**
- **show mls netflow aging**
- **show mls netflow ip dynamic count**
- **show mls netflow ip count**
- **show mls ip**
- **show fm netflow counters**

Si experimenta problemas con el software WCCP porque se están consumiendo los recursos de NetFlow, estos comandos podrían eliminar agresivamente las entradas existentes y crear espacio para nuevas entradas. (Esto no ayuda si simplemente hay más entradas que espacio de NetFlow.)

- **mls aging fast time 3 threshold 1**
- **mls aging long 64**
- **mls aging normal 32**
- **mls ip netflow create software-mode fast** (Esto inhabilita algunos cambios de NetFlow de Supervisor Engine 720 que no estaban en Supervisor Engine 2.)

Para evitar caídas de paquetes, las entidades WCCP deben redirigir el tráfico desde una interfaz que no es la interfaz en la que se configura WCCP. Catalyst 6500 WCCP descarta paquetes en esta situación cuando se cumplen todas las condiciones:

- Tanto los clientes como la entidad WCCP están en la misma interfaz L3.
- La política de redirección WCCP se aplica en esta interfaz.
- Se utiliza el método de redirección GRE.
- Se requiere redireccionar la fragmentación de paquetes.
- Se utiliza Supervisor Engine 720.

Esta situación se debe a los mecanismos de protección integrados en el Catalyst 6500; el software del IOS de Cisco tiene verificaciones que impiden que el paquete entre y salga de la misma interfaz virtual del software del IOS de Cisco donde potencialmente podría conmutar y causar un comportamiento no deseado. Mueva los dispositivos WCCP a su propio entorno L3 dedicado para evitar esto.

La limitación de velocidad basada en el usuario (UBRL) y WCCP no funcionan simultáneamente en una interfaz debido a las máscaras de flujo. Hay una máscara de flujo para cada interfaz para cada función de unidifusión. WCCP requiere flujo completo y UBRL utiliza sólo src o sólo dst.

La compatibilidad con WCCP se agregó para la devolución de Supervisor Engine 2 y L2 en 12.2(18)SXF5. Esto no fue en Supervisor Engine 720 hasta 12.2(18)SXH en abril/mayo de 2007.

Solo se admite la redirección PFC L2 de WCCP con el balanceo de carga del servidor de software



Cisco IOS (SLB); otras configuraciones WCCP no son compatibles y GRE no funciona. El comando WCCP Accelerated sólo se aplica a Supervisor Engine 2/MSFC2. Su propósito es obligar al router a negociar la asignación de máscara y la redirección L2, lo que significa que toda la redirección WCCP se realiza en hardware. El Supervisor Engine 32 y el Supervisor Engine 720 negocian esto sin la necesidad de este comando.

## Soluciones

**Nota:** Use la [Command Lookup Tool \(clientes registrados solamente\)](#) para obtener más información sobre los comandos usados en esta sección.

## ACNS

Para la redirección de almacenamiento en caché transparente estándar, recuerde que la entidad WCCP proporciona al router WCCP los métodos soportados y puede que sea necesario configurarlo para hacerlo. Para Cisco ACNS, esta configuración de ejemplo solicita los métodos de asignación optimizados de redirección L2 y basados en máscara:

1. Asegúrese de tener WCCPv2 para las optimizaciones de Catalyst 6500:

```
ContentEngine(config)# wccp version 2
```

2. Configure una lista de routers que defina Catalyst 6500 para utilizar:

```
ContentEngine(config)# wccp router-list 1 172.16.16.1
```

3. Configure el servicio para utilizar los métodos de optimización:

```
ContentEngine(config)# wccp service router-list-num 1 l2-redirect mask assign
```

Desde el lado del router, el diseño de Catalyst 6500 debe asegurarse de que los dispositivos WCCP estén en una interfaz L3 dedicada que no esté en la trayectoria de tráfico actual (entrada o salida). Para el rendimiento del hardware, los flujos de tráfico deben capturarse de forma entrante en el Catalyst 6500, incluso si esto requiere la configuración de más interfaces que si se eligiera una única interfaz de salida. Un diseño ideal agregaría todo el tráfico antes de llegar a este dispositivo, y sólo unas pocas interfaces requerirían la configuración de ingreso WCCP.

La configuración WCCP en el Catalyst 6500 debe ser:

1. Configuración de WCCPv2:

```
6500Switch# ip wccp version {1 | 2}
```

2. Configure un grupo de servicios WCCP.

```
6500Switch (config)# ip wccp service [accelerated] redirect-list access-list
```

Utilice el comando acelerado solamente para las plataformas Supervisor Engine 2 con el

software 12.1E Cisco IOS.

La lista de redirección se utiliza para identificar el tráfico que se debe seleccionar o no para redirección. Recuerde que esta ACL se puede realizar en hardware, lo que es una manera mucho más eficiente de evitar la redirección para el tráfico que no puede ser atendido por el dispositivo WCCP. El tráfico que se envía al dispositivo y que no se puede mantener allí debe ser devuelto a este Catalyst 6500 para volver a colocarse en la ruta de tráfico original, que requiere procesamiento adicional. Las listas de acceso WCCP son listas de acceso estándar o extendidas.

Este ejemplo muestra que cualquier solicitud de 10.1.1.1 a 12.1.1.1 omite la memoria caché y que todas las demás solicitudes son redirigidas.

```
6500Switch(config)# ip wccp service redirect-list 120
6500Switch(config)# access-list 120 deny tcp host 10.1.1.1 any
6500Switch(config)# access-list 120 deny tcp any host 12.1.1.1
6500Switch(config)# access-list 120 permit ip any any
```

Configure el método WCCP de ingreso en cada interfaz de ingreso que recibe el tráfico que se redirige:

```
Router(config-if)# ip wccp service redirect in
```

Esto completa la configuración en el dispositivo WCCP y en el switch, por lo que la redirección del tráfico debería ocurrir en este punto.

Las configuraciones WCCP finales de los dispositivos se ven así.

Dispositivo	Configuración
dispositivo WCCP	<pre>wccp version 2 wccp router-list 1 router-ip-addresses wccp service router-list-num 1 l2-redirect mask assign</pre>
Router WCCP: global	<pre>ip wccp version 2 ip wccp service redirect-list 120 access-list 120 deny tcp ... access-list 120 deny udp ... access-list 120 permit ip any any</pre>
Router WCCP: cada interfaz de ingreso	<pre>ip wccp redirect service in</pre>

Para verificar esta configuración, ingrese este comando:

```
Show ip wccp service detail
```

Para ver opciones de configuración WCCP adicionales, tales como direccionamiento de grupo usando multicast o seguridad WCCP adicional, refiérase a [Configuración de Servicios de Caché Web con WCCP](#).

## Comandos Show y Debug de WCCP IOS

- **show ip wccp service-number**. proporciona el recuento 'Total de paquetes redirigidos'. Este recuento es el número de flujos o sesiones que se redirigen.

- **show ip wccp service-number detail** - proporciona el conteo de "paquetes redirigidos". El recuento es el número de flujos o sesiones que se redirigen.
- **show ip wccp web-cache detail** - proporciona una indicación de cuántos flujos, en lugar de paquetes, están utilizando la redirección L2.
- **clear ip wccp**: restablece el contador para la información de "paquetes redirigidos".
- **show ip wccp service-number view** - muestra los dispositivos WCCP que forman parte del grupo de servicios.
- **show ip wccp service-number service** - muestra el hash, los puertos y la prioridad WCCP del servicio. Los servicios de mayor prioridad se activan primero cuando se configuran varios servicios en la interfaz.
- **debug ip wccp events** - soluciona el estado del protocolo WCCP.
- **debug ip wccp packets** - revisa las comunicaciones entre las entidades de procesamiento de paquetes WCCP.

Cuando utiliza WCCP y reenvío de hardware, es posible que algunos contadores no se muestren como se esperaba:

- Si la ACL WCCP se procesa completamente en hardware, es posible que los contadores WCCP no muestren recuentos de paquetes precisos.
- Si el WCCP está utilizando recursos de hardware de asignación basada en hash y NetFlow, los contadores WCCP pueden reflejar el número de flujos en lugar del número de paquetes.

## Comandos de NetFlow

Cuando tenga configuraciones WCCP que requieran el uso de recursos de hardware de NetFlow, utilice estos comandos de switching multicapa (MLS) y Fabric Manager (FM) para poder revisar el estado de los recursos de NetFlow:

- **show mls netflow table-contention detailed**
- **show mls netflow ip sw-installed**
- **show mls netflow aging**
- **show mls netflow ip dynamic count**
- **show mls netflow ip count**
- **show mls ip**
- **show fm netflow counters**

## Defectos WCCP

Esta tabla de ID de bug de Cisco y resoluciones soporta la recomendación general de utilizar Cisco IOS Software Release 12.2(18)SXF7 o posterior para el mejor soporte de WCCP.

ID de falla de Cisco	Resuelto en la versión de software del IOS de Cisco	Detalles
<a href="#">CSCsd20327</a>	12.2(18)SXF7	WCCP para el servicio 90 se activa y se desactiva, y causa una pérdida del servicio WCCP. Este problema ocurre cuando se configuran los servicios 81, 82 y 90. Los seguimientos de paquetes indican que el router

podría responder a los mensajes 'Here\_I\_Am' de la memoria caché con los mensajes 'I\_See\_You' que contienen una dirección IP de destino incorrecta.

- [CSCsa7785](#) 12.2(18)SXF6 Puede producirse una recarga cuando se utiliza el modo de redirección y asignación de máscara WCCP L2 con una ACL estándar basada en host como una ACL de redirección WCCP.
- [CSCse69713](#) 12.2(18)SXF6 Cuando se pierden todos los motores de caché en un grupo de servicios WCCP, el tráfico se procesa en el software en lugar de en el hardware conmutado.
- [CSCsd28870](#) 12.2(18)SXF5 En una lista de ACL de redirección WCCP, las ACE configuradas con la palabra clave log no se programan en la tabla TCAM.
- [CSCsb61021](#) 12.2(18)SXF5 El uso elevado de la CPU puede ocurrir en un Supervisor Engine 720 o en un Supervisor Engine 32 cuando la función de suplantación de IP se configura en un motor de memoria caché y cuando la redirección WCCP se configura en la dirección de salida. Los paquetes con IP simulada del motor de memoria caché, con un destino del cliente o del servidor, se conmutan en software en lugar de en hardware.
- Como solución alternativa, utilice el comando **ip wccp service redirect in** para las interfaces entrante y saliente.
- [CSCsb21972](#) 12.2(18)SXF2 Con WCCP y NDE configurados, es posible que vea numerosas pistas causadas por errores de alineación, y la utilización de la CPU puede ser inaceptablemente alta.
- [CSCeh85087](#) 12.2(18)SXF Cuando hay un 'deny ip any any' configurado por el usuario en la ACL de redirección WCCP y cuando se atienden muchos grupos de servicio WCCP, el tráfico asociado con algunos grupos de servicio no se redirige a los routers CE.
- [CSCeh56916](#) 12.2(18)SXF Cuando se habilita un servicio WCCP, cuando la asignación de máscara se configura como método de asignación y cuando cinco o más memorias caché están en el grupo de servicio, los mensajes de protocolo enviados a la memoria caché pueden desbordarse y causar corrupción y recarga de memoria.
- [CSCsb18740](#) 12.2(18)SXF y SXE6 En el modo de reenvío basado en GRE, WCCP utiliza innecesariamente una memoria caché de software que aumenta la utilización de la CPU MSFC.
- [CSCsb26773](#) 12.2(18)SXF Una ACL entrante puede hacer que la redirección WCCP falle con la pérdida de todo el tráfico redirigido.
- [CSCsa90830](#) 12.2(18)SXE2 El tráfico redirigido de ingreso WCCP utiliza la tabla NetFlow para la conmutación de hardware

<a href="#">CSCec55429</a>	12.2(18)SXE	<p>cuando el motor de memoria caché se configura para el reenvío GRE con el modo de asignación de máscara. Cuando la tabla de NetFlow está llena, falla la redirección de ingreso WCCP. La lista de grupos de servicios WCCP se analiza en el orden en que se crean los grupos de servicios, en lugar de por prioridad. Si se definen varios servicios WCCP dinámicos, el tráfico que coincide con los criterios de selección para más de un grupo de servicios no se redirige al grupo de servicios con la prioridad más alta.</p>
<a href="#">CSCuk50878</a>	12.2(18)SXE	<p>En una versión en la que se resuelve el ID de bug Cisco CSCec55429, después de que se hayan producido varios eventos WCC 'cache loss' y 'cache found' para todas las memorias caché de un grupo de servicios, estos eventos pueden ocurrir:</p> <ul style="list-style-type: none"> <li>• Se pueden producir accesos de memoria espurios.</li> <li>• La adición y eliminación de servicios WCCP podría fallar.</li> <li>• El comando <b>show ip wccp</b> muestra el servicio WCCP, pero el resultado del comando <b>show ip wccp service_number</b> no muestra el servicio WCCP.</li> </ul>
<a href="#">CSCsa67611</a>	12.2(18)SXE	<p>Los paquetes de switching de etiquetas multiprotocolo (MPLS) entrantes que salen en una interfaz que no es MPLS (etiqueta a ruta IP) en la que se configura una función de salida (por ejemplo, ACL de salida o WCCP de salida) podrían no tener las funciones de salida aplicadas. Este problema ocurre porque se omite la búsqueda de ACL de salida.</p>
<a href="#">CSCeh13292</a>	12.2(18)SXD4	<p>La configuración de WCCPv2 en un Supervisor Engine 720 causa una alta utilización de la CPU.</p>
<a href="#">CSCeb28941</a>	12.2(18)SXD1	<p>La traducción de direcciones de red (NAT) no funciona con WCCP configurado.</p>
<a href="#">CSCed92290</a>	12.2(17d)SXB2	<p>Los paquetes redirigidos por WCCP que no tienen entrada de caché de protocolo de resolución de direcciones (ARP) de salto siguiente se conmutan por proceso para generar una solicitud ARP. Debido a la redirección WCCP, sin embargo, no se envía ninguna solicitud ARP, la memoria caché ARP nunca se completa para el salto siguiente y los paquetes redirigidos por WCCP subsiguientes continúan conmutándose por proceso.</p>
<a href="#">CSCuk59825</a>	12.2(17d)SXF5 -Sup2 Whitney1.0 para Sup720	<p>Esta versión del software Cisco IOS añadió soporte de hardware para el tráfico de retorno L2. WCCP Request for Comment (RFC) especifica la devolución de L2 como una capacidad opcional para la negociación entre el router y la memoria caché. Hasta ahora, WCCP en el software Cisco</p>

IOS no ha permitido la negociación de esta capacidad porque el soporte de hardware requerido está ausente. Esa compatibilidad ahora está disponible, por lo que la negociación de retorno L2 en el intercambio de protocolo WCCP entre el router y la memoria caché puede estar habilitada.