

WCCP auf Catalyst 6500-Plattformen mit Konfigurationsleitfaden für hohe CPU-Auslastung

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[WCCP-Funktionsübersicht](#)

[WCCP und Catalyst 6500](#)

[WCCP-Zuweisungsmethode](#)

[Hash-Based Assignment Method Detail](#)

[Maskenbasierte Zuordnungsmethodendetails](#)

[WCCP-Weiterleitungsmethode](#)

[L3 \(GRE\)-Weiterleitungsmethode](#)

[Eingehend - L3 \(GRE\)-Umleitung + Hash-Zuweisung](#)

[Eingehend - L3 \(GRE\)-Umleitung + Maskenzuweisung](#)

[Ausgehend - L3 \(GRE\)-Umleitung + Hash-Zuweisung](#)

[Ausgehend - L3 \(GRE\)-Umleitung + Maskenzuweisung](#)

[L2-Weiterleitungsmethode](#)

[Eingehend - L2 + Hash-Zuweisung](#)

[Eingang - L2 + Maskenzuweisung](#)

[Ausgehend - L2 + Hash-Zuweisung](#)

[Ausgehend - L2 + Maskenzuweisung](#)

[WCCP-Rückgabemethode](#)

[WCCP-Entität kann Anforderung bearbeiten](#)

[WCCP-Entität kann Anforderung nicht bearbeiten](#)

[GRE-Rückgabe](#)

[L2-Optimierung der Rückgabe](#)

[Zusammenfassung der WCCP-Optionen](#)

[WCCP-Designempfehlungen](#)

[Zusammenfassung](#)

[Zusätzliche Empfehlungen](#)

[Lösungen](#)

[ACNS](#)

[Befehle zum Anzeigen und Debuggen von WCCP IOS](#)

[NetFlow-Befehle](#)

[WCCP-Fehler](#)

Einführung

Dieses Dokument beschreibt die Verwendung des Web Cache Communication Protocol (WCCP) auf der Plattform der Cisco Catalyst Serie 6500.

WCCP wurde ursprünglich als Methode zum Abfangen von Web-Datenverkehr (HTTP) entwickelt und an ein lokales Cache-Gerät weitergeleitet, wo er von einem lokalen Standort aus an einen Client weitergeleitet werden konnte, um die kostspielige WAN-Bandbreite zu sparen.

Aus Sicht der Netzwerkbenutzer ist WCCP transparent, da es auf Netzwerkebene ohne spezielle Konfiguration durch den Benutzer verwendet wird, um den Webdatenverkehr, der ein Layer 3 (L3)-Gerät passiert, zu identifizieren und an ein lokales Cache-Gerät umzuleiten. Obwohl WCCP ursprünglich für Webdatenverkehr konzipiert wurde, ist die transparente Weiterleitungsmethode inzwischen ein sehr nützlicher Mechanismus zur Behebung anderer Probleme mit umfangreichen Inhalten über Links mit geringem Volumen geworden. Aus diesem Grund wurde in späteren WCCP-Versionen zusätzliche Protokollunterstützung hinzugefügt. Zu diesen zusätzlichen Technologien gehören Protokolle wie HTTP, HTTPS, FTP, Video-Streaming und Technologien zum Zwischenspeichern von Dateien, z. B. das Common Internet File System (CIFS). Diese Technologien unterstützen neuere Lösungen und Plattformen von Cisco, z. B. Wide Area File Services (WAFS), Wide Area Application Services (WAAS), Application Oriented Networking (AONs) und erweiterte Funktionen der Application and Content Networking Software (ACNS).

Mit der Implementierung der neuesten Produktivitätstools wie videobasierter Kommunikation und Schulungen sowie Live- und On-Demand-Videofunktionen gewinnt die WCCP-Nutzung immer mehr an Bedeutung. Die Bemühungen zur Kostenkontrolle, wie z. B. konsolidierte Rechenzentren, erfordern WCCP, zusätzliche Services mit extrem hoher Bandbreite zu unterstützen.

Aufgrund der Bedeutung von WCCP in den heutigen, inhaltsreichen Netzwerken haben einige Plattformen wie der Catalyst 6500 eine hardwareunterstützte Leistung mit WCCP implementiert, um die für das Protokoll erforderliche CPU-Last zu reduzieren. In diesem Dokument wird beschrieben, wie WCCP auf dem Catalyst 6500 bereitgestellt wird, um die Hardwareauslastung zu maximieren und die CPU-Auslastung zu reduzieren.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- WCCP
- Cisco Catalyst Switches der Serie 6500
- Cisco IOS[®] Software

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco Catalyst Switches der Serie 6500
- Cisco IOS Software Release 12.1(50)SY oder höher mit Supervisor Engine 2T (Policy Feature Card 4)
- Cisco IOS Softwareversion 12.2(18)SXD1 oder höher mit Supervisor Engine 720 (Policy Feature Card 3)

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

WCCP-Funktionsübersicht

Die Funktionalität, die allgemein als WCCP bezeichnet wird, umfasst drei Komponenten:

1. Nur am Router oder Switch implementierte Funktionen
2. Funktionen, die nur in der Datenverkehrsverarbeitungseinheit implementiert sind, z. B. ein Webcache
3. WCCP wird auf beiden Seiten implementiert

In diesem Dokument werden die folgenden drei WCCP-Betriebsmerkmale untersucht:

1. Die **Zuweisungsmethode** bestimmt, welcher WCCP-Datenverkehr und welches WCCP-Gerät für das Ziel des Datenverkehrs ausgewählt werden. Das WCCP-Protokoll unterstützt mehrere Geräte, die in einem Cluster zusammengefasst sind.
2. Die **Umleitungsmethode** leitet den Datenverkehrsfluss an die WCCP-Appliance weiter, wenn eine Änderung vom normalen Netzwerkpfad erforderlich ist, über den der Datenverkehr übertragen wurde.
3. Die **Rückgabemethode** bestimmt, wie der Datenverkehr von der WCCP-Appliance an den Router zurückgesendet wird, wenn der Datenverkehr nicht gewartet werden konnte. In Fällen, in denen die WCCP-Appliance die Anforderung übernimmt, werden die Pakete direkt an den Anforderer zurückgegeben.

WCCP und Catalyst 6500

Die Catalyst 6500 Supervisor Engine 2, Supervisor Engine 32 und Supervisor Engine 720 unterstützen die folgenden WCCP-Funktionen und -Methoden:

- WCCP Version 2 (WCCPv2)
- Hash-basierte Zuweisungsmethode
- Maskenbasierte Zuweisungsmethode (hardwarebeschleunigt)
- L3 Generic Routing Encapsulation (GRE) Redirection (hardwarebeschleunigt auf der Supervisor Engine 32 und der Supervisor Engine 720)
- Layer-2-Umleitungsverfahren (hardwarebeschleunigt auf Supervisor Engine 2, Supervisor Engine 32 und Supervisor Engine 720)
- GRE-Rückgabemethode
- L2-Rückgabemethode mit Cisco IOS Software, Version 12.2SXH (hardwarebeschleunigt auf Supervisor Engine 2, Supervisor Engine 32 und Supervisor Engine 720)

Weitere Informationen zu diesen Funktionen finden Sie im [Konfigurationsleitfaden zur Cisco IOS Software der Cisco Serie 6500, 12.2SX](#), unter [Konfigurieren von WCCP](#).

WCCP-Zuweisungsmethode

Die WCCP-Zuweisung bestimmt, welcher Datenverkehr vom WCCP-Protokoll umgeleitet wird und welche WCCP-Einheit den umgeleiteten Datenverkehr empfängt.

Wenn WCCP auf einer Schnittstelle eines Routers und einer WCCP-Einheit konfiguriert wird, muss das Umleitungsgerät (der Catalyst 6500) wissen, welcher Datenverkehr umgeleitet werden soll und wo der Datenverkehr gesendet werden soll. Die WCCP-Einheiten in einem Service-Group-Cluster kommunizieren alle über das WCCP-Protokoll mit dem Catalyst 6500. Es wird jedoch ein WCCP-Gerät ausgewählt, das den Cluster darstellt, um zu steuern, wie der Cluster arbeitet (über die Zuweisungsmethode, die Weiterleitungsmethode usw.). Die WCCP-Appliance und der Router können die Methode aushandeln, mit der Pakete auf die Web-Caches einer Service-Gruppe verteilt werden. Eine Servicegruppe ist eine Many-to-Many-Beziehung zwischen bis zu 32 Routern und 32 WCCP-Einheiten. Die Aushandlung erfolgt nach Servicegruppe. Daher können Webcaches, die an mehreren Servicegruppen teilnehmen, für jede Servicegruppe eine andere Zuweisungsmethode aushandeln. Die derzeit verfügbaren WCCP-Dienste sind:

WCCP-Dienst Protokoll

Webcache	HTTP
53	DNS-Cache
60	FTP
81	WAAS - Vorwärts
62	WAAS - Rückseite
70	HTTPS
80	Real-Time Streaming Protocol (RTSP)
81	Microsoft Media Server (MMS) über UDP (MMSU)
82	MMS über TCP (MMST)
83	RTSP mit UDP (RTSPU)
89	CIFS-Cache-WAAS
98	Benutzerdefinierter Webcache
99	Reverse Proxy
90-97	Vom Benutzer konfigurierbar *

* Vom Benutzer konfigurierbare Services werden im Catalyst 6500 implementiert. Dabei wird ein Schnittstellenebenenbefehl auf ein- oder ausgehende Richtungen angewendet. Die Auswirkungen der Auswahl von ein- oder ausgehenden Anrufen werden später erörtert. Eingehend ist jedoch die bevorzugte Methode, da eine Umleitungsliste für maximale Hardware-Leistung mit WCCP verknüpft werden kann.

Nach der Konfiguration für WCCP kündigt ein Router die unterstützten Zuweisungsmethoden für eine Servicegruppe in den WCCP-Kommunikationsnachrichten an. Das Fehlen einer solchen Meldung impliziert, dass der Catalyst 6500 nur die Hash-basierte Standardzuweisungsmethode unterstützt.

Sobald die Verhandlungen zwischen dem Catalyst 6500 und der WCCP-Appliance abgeschlossen sind, informiert die benannte WCCP-Stelle über WCCP den Catalyst 6500 darüber, welcher Datenverkehr umgeleitet werden soll und welchen WCCP-Einheiten der Datenverkehr zugewiesen wird. Als Beispiel kann die WCCP-Einheit den Catalyst 6500 informieren, dass der gesamte

Webdatenverkehr von einem bestimmten Subnetz an die Cache-Engines 1 - 4 in der Service-Gruppe umgeleitet wird, wenn mehr als vier WCCP-Geräte verfügbar sind.

Für WCCP stehen zwei Zuweisungsmethoden zur Verfügung:

1. **Bei der Hash-basierten Zuweisung** (Standard) wird ein softwarebasierter Hash-Algorithmus zusammen mit Direktiven der WCCP-designierten Appliance verwendet, um zu bestimmen, welche WCCP-Appliance Datenverkehr empfängt. Bei einer Supervisor Engine 32 oder Supervisor Engine 720-Plattform werden NetFlow-Hardwareressourcen eingesetzt, um eine gewisse Hardware-Unterstützung zu gewähren.
2. **Bei der Maskenzuweisung** werden die Hardwarefunktionen des Catalyst 6500, insbesondere die Zugriffskontrollliste (ACL) Ternary Content Addressable Memory (TCAM), verwendet, um Datenverkehr an WCCP-Einheiten zuzuweisen. Dies ist die bevorzugte Methode.

Alle Geräte in einer WCCP-Servicegruppe müssen dieselbe Zuweisungsmethode verwenden. Zuweisungsmethoden werden auf der WCCP-Einheit konfiguriert und vom Catalyst 6500 gelernt. Weitere Informationen finden Sie in den [WCCP-Designempfehlungen](#).

Hash-Based Assignment Method Detail

Der Hash-basierte Zuweisungsmechanismus beruht auf einem in der Software ausgeführten Algorithmus. Um den Hash-Algorithmus zu nutzen, wird das erste Paket in einem bestimmten Fluss vom Hardwarepfad an den Softwarepfad gesendet, in dem der Hash ausgeführt wird.

Die Software führt einen XOR-Hash verschiedener Komponenten des Datenflusses durch und erstellt einen Hash, der die Datenflüsse zu den verschiedenen WCCP-Einheiten aufteilt. Der Hash-Mechanismus legt fest, wie der Datenverkehr auf die verfügbaren WCCP-Entitäten verteilt wird.

Das Hash-Ergebnis wird in die Hardware-NetFlow-Tabelle programmiert, in der nachfolgende Pakete in diesem Fluss weitergeleitet werden. Unabhängig von den Feldern, die für das Hashing durch WCCP verfügbar sind, wird der vollständige Fünf-Tupel-Modus verwendet. Dies bedeutet, dass NetFlow bei Aktivierung von WCCP in den Modus "interface, full-flow" gesetzt wird. Dies hat Auswirkungen auf andere Funktionen, die möglicherweise NetFlow-Ressourcen erfordern. Weitere Informationen finden Sie im Abschnitt [WCCP-Defekte](#).

Eine häufige Frage zu WCCP auf dem Catalyst 6500 lautet: "Warum erhöht sich die CPU-Auslastung, wenn ich WCCP aktiviere?" Wenn Hash-basierte Zuweisungen verwendet werden, belastet die softwarebasierte Verarbeitung des ursprünglichen Pakets in jedem Datenfluss die CPU und ist meistens die Ursache für eine erhöhte Auslastung. Bei der derzeit verfügbaren Weiterleitungshardware für Policy Feature Card 3 (PFC3) ist WCCP als Ausgangs-Funktion konfiguriert oder wird Hash-basierte Zuweisungen verwendet (ein- oder ausgehend), ist immer eine gewisse Softwareverarbeitung erforderlich.

Die Verwendung der Hash-basierten Zuweisungsmethode wirkt sich auf folgende Features aus:

- **NetFlow-Tabelle** - Die Anzahl der von der PFC unterstützten Einträge ist begrenzt, und die Flussmaske ändert sich in "interface full-flow" für die gesamte NetFlow-Tabelle.
- **CPU-Auslastung** - Die CPU-Auslastung wird erhöht, da das erste Paket in jedem Datenfluss per Software-Switching betrieben wird.
- **Leistung** - Die Geschwindigkeit, mit der Datenverkehr zur Suche an die CPU gesendet wird,

ist so beschränkt, dass die CPU geschützt ist.

- **NetFlow-Funktionen** - Andere Funktionen, die NetFlow-Ressourcen verwenden, können davon betroffen sein, wenn die NetFlow-Ressourcen von WCCP genutzt werden.

Die Einschränkungen und Auswirkungen, die durch die Hash-basierte Zuweisungsanforderung für die Softwareverarbeitung entstehen, gelten für den ein- und ausgehenden Datenverkehr. Die Auswirkungen auf die CPU können sich verschärfen, wenn das Netzwerk atypische Datenverkehrsmuster durchläuft, z. B. ein DoS-Angriff (Denial of Service). Bei einem typischen Angriff oder Wurmausbruch wird jedes von einem Host gesendete Paket an ein neues Ziel oder einen neuen Port gesendet, wodurch jedes Paket in der Software verarbeitet wird. Da der WCCP-umgeleitete Datenverkehr explizit zur Verarbeitung des ersten Pakets an die CPU gesendet wird, gibt es nur begrenzte Schutzmethoden. Die Verwendung von "deny"-ACL-Einträgen auf der Schnittstelle kann die an die CPU gesendete Nachricht einschränken. Es gibt jedoch keine Ratenlimitierungen oder andere Schutzmechanismen gegen diese Angriffsarten.

Maskenbasierte Zuordnungsmethodendetails

Die Maskenzuweisung wird unterschiedlich behandelt, je nachdem, ob sie beim Ein- oder Ausgang konfiguriert wird.

Bei einer Zuordnung auf Eingangsmaske basierenden Zuordnung wird die Maske vor der Paketweiterleitung in den ACL TCAM programmiert, sodass die NetFlow-Tabelle und die Softwareverarbeitung nicht erforderlich sind. Die WCCP-Einheit wählt eine Reihe von Hash-Buckets aus und weist jeder Gruppe eine Adressmaske und eine WCCP-Appliance zu. Nach Abschluss der Zuweisungen programmiert der Supervisor einen TCAM-Eintrag und eine Hardware-Adjacency für jede Gruppe und leitet Pakete, die der Adressmaske entsprechen, mithilfe einer L2-Umschreibung an die zugeordnete WCCP-Appliance um.

Wenn WCCP als Eingangs-Funktion konfiguriert ist, kann in der Hardware-ACL-Tabelle ein Eintrag für die ACL-Umleitung verwendet werden. Wenn WCCP mit dem Eintrag übereinstimmt, wird eine entsprechende Adjacency verwendet, um entweder eine L2-Umschreibung oder eine GRE-Kapselung auszuführen. Wenn also die Maskenzuweisung beim Eingang verwendet wird, werden sowohl L2-Rewrite (Supervisor Engine 2, Supervisor Engine 32 und Supervisor Engine 720) als auch GRE-Kapselung (nur Supervisor Engine 32 und Supervisor Engine 720) in der Hardware ausgeführt.

Wenn WCCP als Ausgangs-Funktion konfiguriert ist, werden ACL-Redirect-Adjacencies in der Hardware nicht unterstützt, da die Pakete im Fluss bereits vom System geroutet wurden. Das erste Paket eines Datenflusses wird zur Verarbeitung an die Software gesendet. Sobald die richtige Redirect-Adjacency bestimmt wurde, wird sie in die NetFlow-Hardware (anstelle von ACL TCAM) programmiert, wo der Eintrag auf eine Adjacency zeigt, die entweder eine L2-Rewrite- oder GRE-Kapselung ausführt. Nachfolgende Pakete im Fluss werden in der Hardware von der NetFlow-Hardware umgeleitet.

Hinweis: Wenn WCCP als Ausgangs-Funktion konfiguriert ist, erfordert die Maskenzuweisung eine Softwareverarbeitung, wodurch alle Vorteile der maskenbasierten Zuweisungsmethode zunichte gemacht werden.

Von den beiden maskenbasierten Optionen ermöglicht nur die auf der Eingangsmaske basierende Zuweisung eine vollständige hardwarebasierte Weiterleitung für erste und nachfolgende Pakete. Jede andere Option, z. B. die Hash-basierte Zuweisung oder Ausgangsverarbeitung, verursacht

das Software-Switching des ursprünglichen Pakets und die hardwarebasierte NetFlow-Switched Forwarding nachfolgender Pakete.

WCCP-Weiterleitungsmethode

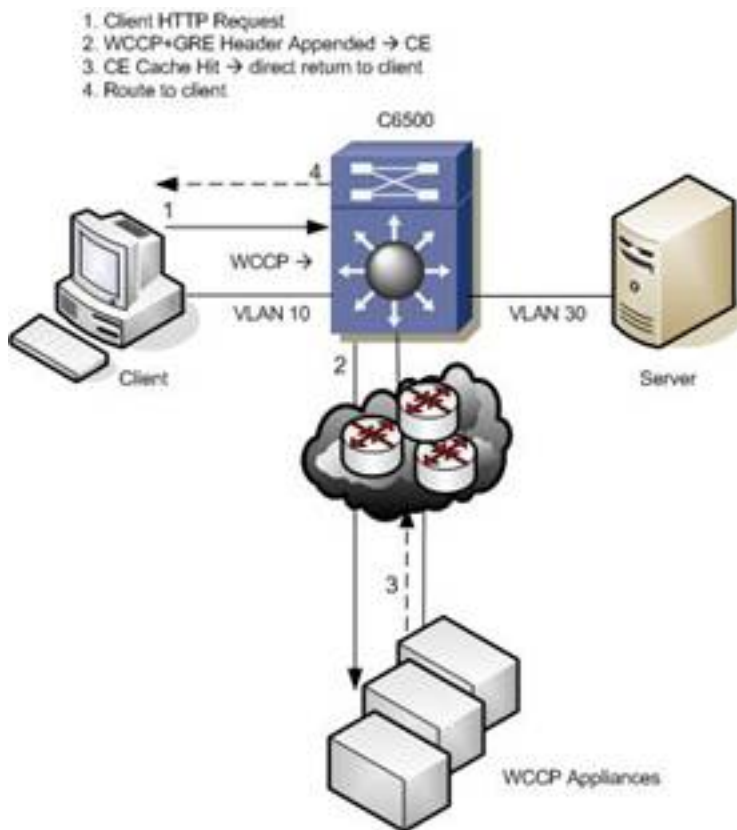
Die WCCP-Einheit, nicht der Catalyst 6500, legt die Hashtabellen und Maske/Wert-Sets für den Catalyst 6500 fest, sodass die Redirect-Methode auf dieser Appliance und nicht auf dem Catalyst 6500-Switch konfiguriert wird. Der Catalyst 6500 bestimmt anhand der WCCP-Kommunikation mit der WCCP-Einheit/Gruppe die beste verfügbare Umleitungsmethode. Diese Aushandlung legt fest, wie der umgeleitete Datenverkehr an die Appliance weitergeleitet wird. Es gibt zwei Umleitungsoptionen: L3 (GRE) und L2 (MAC-Adresse wird umgeschrieben).

Bei WCCPv1 ist die einzige Option die L3-Umleitung, auch als GRE-Kapselung bekannt. Bei der L3-Umleitung wird jedes umgeleitete WCCP-Paket in einen GRE-Header eingekapselt, der mit dem Protokolltyp 0x883E markiert ist, gefolgt von einem WCCP-Redirect-Header mit vier Oktetten, der anschließend an die WCCP-Appliance (z. B. eine Cache-Engine) gesendet wird.

Mit der Einführung von WCCPv2 wurde eine L2-Umleitung, auch beschleunigte WCCP-Umleitung genannt, hinzugefügt, um Hardware-Switching-Plattformen wie den Catalyst 6500 nutzen zu können. Wenn WCCP eine L2-Umleitung verwendet, müssen die WCCP-Appliance und der Catalyst 6500 über eine L2-Nachbarschaft verfügen (innerhalb desselben L2-VLAN). Umgeleiteter L2-Datenverkehr verwendet keine GRE-Kapselung. Stattdessen wird die MAC-Zieladresse vom Catalyst 6500 an die Adresse der WCCP-Einheit mit L2-Verbindung umgeschrieben und über normale Hardware-Switches weitergeleitet.

Hinweis: Die Methode der Weiterleitung an das WCCP-Gerät ist möglicherweise nicht die gleiche, die das WCCP-Gerät verwendet, um den Datenverkehr an den Catalyst 6500 zurückzusenden. WCCP wird verwendet, um eine Weiterleitungs- und Rückgabemethode auszuhandeln, die von beiden Geräten unterstützt wird. Siehe [WCCP-Rückgabemethode](#).

L3 (GRE)-Weiterleitungsmethode



WCCP L3-Betrieb umfasst die Verwendung von GRE als Kapselungsmethode. Umgeleitete Pakete werden in einem GRE-Header mit dem Protokolltyp 0x883e gekapselt, zusammen mit einem 4-Byte-WCCP-Umleitungs-Header, der eine Dienst-ID und einen übereinstimmenden Hash-Bucket enthält (nur WCCPv2). Durch die Verwendung von GRE kann der WCCP-Client durch mehrere L3-Hops (geroutet) vom Catalyst 6500 getrennt werden.

In diesem Szenario stehen folgende Optionen für die WCCP-Umleitung zur Verfügung:

1. Ingress - L3 (GRE)-Umleitung + Hash-Zuweisung; Dies erfordert eine Softwareverarbeitung.
2. Eingehend - L3 (GRE)-Umleitung + Maskenzuweisung; Dies erfordert eine vollständige Hardware-Verarbeitung und ist nur auf der Supervisor Engine 32 oder der Supervisor Engine 720 verfügbar.
3. Ausgehend - L3 (GRE-Umleitung) + Hash-Zuweisung; Dies erfordert eine Softwareverarbeitung.
4. Ausgehend - L3 (GRE)-Umleitung + Maskenzuweisung; Dies erfordert eine Softwareverarbeitung.

Eingehend - L3 (GRE)-Umleitung + Hash-Zuweisung

Auf der Supervisor Engine 2 wird jedes GRE-Paket zur Verarbeitung an die Multilayer Switch Feature Card (MSFC) gesendet. Da die GRE-Kapselung in der Hardware nicht unterstützt wird, muss die MSFC sowohl GRE- als auch WCCP-Header anwenden, wodurch das Software-Switching für den gesamten Datenverkehr erzwungen wird.

Bei der Hash-basierten Zuweisungsmethode leiten die Supervisor Engine 32 und die Supervisor Engine 720 das erste Paket jedes Softwareflusses weiter, sodass ein NetFlow-Tabelleneintrag erstellt wird. Das Paket wird dann in GRE gekapselt (die Kapselung und Weiterleitung des ursprünglichen Pakets erfolgt in der Software) und an die WCCP-Appliance weitergeleitet.

Die Einrichtung des NetFlow-Eintrags wirkt sich auf die CPU-Auslastung aus, die nachfolgende Paketweiterleitung erfolgt jedoch in der Hardware für die Supervisor Engine 720 und die Supervisor Engine 32. Datenverkehrsmuster, insbesondere die Anzahl eindeutiger Datenflüsse, bestimmen, wie viel CPU genutzt wird. Wenn die NetFlow-Ressourcen des Catalyst 6500 verbraucht werden, wird der gesamte Datenverkehr in der Software weitergeleitet.

Die NetFlow-Ressourcen der Supervisor-PFC unterscheiden sich von Plattform zu Plattform. Derzeit sind die größten NetFlow-Ressourcen auf dem PFC-3BXL der Supervisor Engine 720-Plattform verfügbar.

Eingehend - L3 (GRE)-Umleitung + Maskenzuweisung

Auf der Supervisor Engine 2 wird jedes GRE-Paket zur Verarbeitung an die MSFC gesendet. Da die GRE-Kapselung in der Hardware nicht unterstützt wird, muss die MSFC sowohl GRE- als auch WCCP-Header anwenden, wodurch das Software-Switching für den gesamten Datenverkehr erzwungen wird.

Bei der Maskenzuweisungsmethode leiten die Supervisor Engine 32 und die Supervisor Engine 720 die anfänglichen und nachfolgenden Pakete in die Hardware weiter, da GRE nativ unterstützt wird und die Maskenzuweisung die ACL TCAM-Hardware für die Weiterleitung verwendet.

Ausgehend - L3 (GRE)-Umleitung + Hash-Zuweisung

Auf der Supervisor Engine 2 wird jedes Paket zur Verarbeitung an die MSFC gesendet. Da die GRE-Kapselung in der Hardware nicht unterstützt wird, muss die MSFC sowohl GRE- als auch WCCP-Header anwenden, wodurch das Software-Switching für den gesamten Datenverkehr erzwungen wird.

Bei der Hash-basierten Zuweisungsmethode mit der Supervisor Engine 32 und der Supervisor Engine 720 leitet der Catalyst 6500 das erste Paket jedes Softwareflusses weiter, sodass der NetFlow-Tabelleneintrag eingerichtet wird. Das Paket wird dann in GRE gekapselt und an die WCCP-Einheit weitergeleitet.

Die Einrichtung des NetFlow-Eintrags wirkt sich auf die CPU-Auslastung aus, die nachfolgende Paketweiterleitung erfolgt jedoch in der Hardware. Datenverkehrsmuster, insbesondere die Anzahl eindeutiger Datenflüsse, bestimmen, wie viel CPU genutzt wird. Wenn die NetFlow-Ressourcen des Catalyst 6500 verbraucht werden, wird der gesamte Datenverkehr in der Software weitergeleitet.

Die NetFlow-Ressourcen der Supervisor-PFC unterscheiden sich von Plattform zu Plattform. Derzeit sind die größten NetFlow-Ressourcen auf dem PFC-3BXL der Supervisor Engine 720-Plattform verfügbar.

Ausgehend - L3 (GRE)-Umleitung + Maskenzuweisung

Auf der Supervisor Engine 2 wird jedes Paket zur Verarbeitung an die MSFC gesendet. Da die GRE-Kapselung in der Hardware nicht unterstützt wird, muss die MSFC sowohl GRE- als auch WCCP-Header anwenden, wodurch das Software-Switching für den gesamten Datenverkehr erzwungen wird.

Bei der Maskenzuweisungsmethode mit der Supervisor Engine 32 und der Supervisor Engine 720 wird das erste Paket jedes Datenflusses per Software-Switching konfiguriert, sodass der NetFlow-Tabelleneintrag erstellt wird. Keiner der Supervisoren unterstützt die Adjacency-Programmierung für die Ausgangszugriffskontrollliste, die diese Softwareverarbeitung erzwingt und für das erste Paket in jedem Datenfluss NetFlow-Ressourcen (anstelle von Hardware-ACL-TCAM) verwendet. Das Paket wird dann in GRE gekapselt und an die WCCP-Appliance weitergeleitet.

Die Einrichtung des NetFlow-Eintrags wirkt sich auf die CPU-Auslastung aus, die nachfolgende Paketweiterleitung erfolgt jedoch in der Hardware. Datenverkehrsmuster, insbesondere die Anzahl eindeutiger Datenflüsse, bestimmen, wie viel CPU genutzt wird. Wenn die NetFlow-Ressourcen des Catalyst 6500 verbraucht werden, wird der gesamte Datenverkehr in der Software weitergeleitet.

Die NetFlow-Ressourcen der Supervisor-PFC unterscheiden sich von Plattform zu Plattform. Derzeit sind die größten NetFlow-Ressourcen auf dem PFC-3BXL der Supervisor Engine 720-Plattform verfügbar.

L2-Weiterleitungsmethode

Bei der L2-Weiterleitung sind die WCCP-Entitäten (ACNS, WAFS, WAAS usw.) innerhalb einer Servicegruppe Teil desselben Subnetzes und L2 neben dem Catalyst 6500. Dies ermöglicht einen hohen Durchsatz und eine Umleitung des Datenverkehrs mit niedriger Latenz. Die Eingangsschnittstelle (in der WCCP konfiguriert ist) und die Schnittstelle, in der sich die WCCP-Appliance(s) befindet, müssen sich in unterschiedlichen VLANs befinden.

Hinweis: Bei der L2-Umleitung wird das Paket neu geschrieben, wobei die Quell-MAC auf den Router und die Ziel-MAC auf die Cache-Engine festgelegt ist. Der einzige Nachteil dieser Umleitungsmethode besteht darin, dass die Cache-Engine **L2** vom Catalyst 6500 **erreichbar** sein muss und sich auf einer **anderen L3-Schnittstelle** als der konfigurierten Eingang-WCCP-Schnittstelle befinden muss.

Hinweis: Die Methode der Weiterleitung an das WCCP-Gerät ist möglicherweise nicht die gleiche, die das WCCP-Gerät verwendet, um den Datenverkehr an den Catalyst 6500 zurückzusenden. WCCP wird verwendet, um eine Weiterleitungs- und Rückgabemethode auszuhandeln, die von beiden Geräten unterstützt wird. Siehe [WCCP-Rückgabemethode](#).

In diesem Szenario stehen folgende Optionen für die WCCP-Umleitung zur Verfügung:

- Eingehend - L2-Umleitung + Hash-Zuweisung; Dies erfordert eine Softwareverarbeitung.
- Eingehend - L2-Umleitung + Maskenzuweisung erfordert vollständige Hardwareverarbeitung und wird empfohlen.
- Ausgehend - L2-Umleitung + Hash-Zuweisung; Dies erfordert eine Softwareverarbeitung.
- Ausgehend - L2-Umleitung + Maskenzuweisung; Dies erfordert eine Softwareverarbeitung.

Eingehend - L2 + Hash-Zuweisung

Wenn der WCCP-Datenverkehr beim Eingang mit L2 + Hash-Zuweisung konfiguriert wird, sendet er in jedem Fluss das erste Paket, das per Software-Switching weitergeleitet werden soll. Dadurch wird ein NetFlow-Eintrag in der Hardware-NetFlow-Tabelle erstellt.

Hinweis: Die NetFlow-Flow-Maske ist auf den Volllaufmodus für die Schnittstelle festgelegt, was Auswirkungen auf andere NetFlow-Funktionen haben kann, die auf dem Switch konfiguriert sind.

Da WCCP ein Stateless-Mechanismus ist, werden die Informationen nicht in der Software verwaltet. Stattdessen wird sie in der Hardware als Einträge in der NetFlow-Tabelle beibehalten. Der nachfolgende Datenverkehr im Datenfluss wird in der Hardware weitergeleitet, solange ein NetFlow-Tabelleneintrag vorhanden ist.

Die Einrichtung des NetFlow-Eintrags wirkt sich auf die CPU-Auslastung aus, die nachfolgende Paketweiterleitung erfolgt jedoch in der Hardware. Datenverkehrsmuster, insbesondere die Anzahl eindeutiger Datenflüsse, bestimmen, wie viel CPU genutzt wird. Wenn die NetFlow-Ressourcen des Catalyst 6500 verbraucht werden, wird der gesamte Datenverkehr in der Software weitergeleitet.

Die NetFlow-Ressourcen der Supervisor-PFC unterscheiden sich von Plattform zu Plattform. Derzeit sind die größten NetFlow-Ressourcen auf dem PFC-3BXL der Supervisor Engine 720-Plattform verfügbar.

Eingang - L2 + Maskenzuweisung

Bei der Konfiguration beim Eingang ist die L2 +-Maskenzuweisung die effizienteste vom Catalyst 6500 unterstützte WCCP-Methode. Der gesamte Datenverkehr ist hardwarebasiert, einschließlich des ursprünglichen Pakets in jedem Datenfluss. Es ist keine Software-Umleitung erforderlich. Die erste und nachfolgende Paketweiterleitung erfolgt über Hardware.

Die Hardware-ACL-TCAM-Ressourcen des Catalyst 6500 werden verwendet, um die Hardwareeinträge vor dem Empfang von WCCP-Paketen vorzuprogrammieren.

Um diese Methode verwenden und das vollständige Hardware-Switching nutzen zu können, muss die WCCP-Einheit auch die L2-Umleitung und die Maskenzuweisungsmethode unterstützen. Die Konfiguration dieser Methode ist für die WCCP-Einheit abgeschlossen, und der Catalyst 6500 handelt die beste Methode während der ersten WCCP-Kommunikation mit der WCCP-Einheit/Gruppe aus.

Ausgehend - L2 + Hash-Zuweisung

Bei der ausgehenden L2 +-Hash-Zuweisung sendet WCCP-Datenverkehr das erste Paket in jedem Fluss, das per Software-Switching weitergeleitet wird. Dadurch wird ein NetFlow-Eintrag in der Hardware-NetFlow-Tabelle erstellt.

Hinweis: Die NetFlow-Flow-Maske ist auf den Volllaufmodus für die Schnittstelle festgelegt, was Auswirkungen auf andere NetFlow-Funktionen haben kann, die auf dem Switch konfiguriert sind.

Darüber hinaus ist bei der Konfiguration in Egress-Richtung eine zusätzliche FIB-Suche (Forwarding Information Base) für das erste Paket des Datenflusses erforderlich, um die mit dem CE verbundene Adjacency zu ermitteln, die eine Paketumwälzung innerhalb des Catalyst 6500

erfordert. Nachfolgende Pakete werden in der Hardware NetFlow-Switching ausgeführt.

Die Einrichtung des NetFlow-Eintrags wirkt sich auf die CPU-Auslastung aus, die nachfolgende Paketweiterleitung erfolgt jedoch in der Hardware. Datenverkehrsmuster, insbesondere die Anzahl eindeutiger Datenflüsse, bestimmen, wie viel CPU genutzt wird. Wenn die NetFlow-Ressourcen des Catalyst 6500 verbraucht werden, wird der gesamte Datenverkehr in der Software weitergeleitet.

Die NetFlow-Ressourcen der Supervisor-PFC unterscheiden sich von Plattform zu Plattform. Derzeit sind die größten NetFlow-Ressourcen auf dem PFC-3BXL der Supervisor Engine 720-Plattform verfügbar.

Ausgehend - L2 + Maskenzuweisung

Bei der Konfiguration in Ausgangs-Richtung schaltet die L2 +-Maskenzuweisung das erste Paket in jedem Softwarefluss um, genau wie beim L2 + Hash-Zuweisungsfall. Nachfolgende Pakete werden in der Hardware NetFlow-Switching ausgeführt.

Hinweis: Die NetFlow-Flow-Maske ist auf den Volllaufmodus für die Schnittstelle festgelegt, was Auswirkungen auf andere NetFlow-Funktionen haben kann, die auf dem Switch konfiguriert sind.

PFC2 und PFC3 unterstützen keine Programmierung der ACL-Adjacency für den Ausgangs-Datenverkehr, wodurch die Softwareverarbeitung für das erste Paket in jedem Datenfluss erzwungen wird. nachfolgende Pakete im Fluss werden in der Hardware weitergeleitet.

Die Einrichtung des NetFlow-Eintrags wirkt sich auf die CPU-Auslastung aus, die nachfolgende Paketweiterleitung erfolgt jedoch in der Hardware. Datenverkehrsmuster, insbesondere die Anzahl eindeutiger Datenflüsse, bestimmen, wie viel CPU genutzt wird. Wenn die NetFlow-Ressourcen des Catalyst 6500 verbraucht werden, wird der gesamte Datenverkehr in der Software weitergeleitet.

Die NetFlow-Ressourcen der Supervisor-PFC unterscheiden sich von Plattform zu Plattform. Derzeit sind die größten NetFlow-Ressourcen auf dem PFC-3BXL der Supervisor Engine 720-Plattform verfügbar.

WCCP-Rückgabemethode

WCCP-Entität kann Anforderung bearbeiten

Wenn WCCP zum Abfangen von Datenverkehr verwendet wird und die WCCP-Einheit einen vollständigen Vorgang für diese Pakete durchführt, können die Pakete vom WCCP-Gerät an den Client zurückgesendet werden. Dieser normalerweise verarbeitete Datenverkehr, der zurück zum Client im Netzwerk geleitet wird, erfordert keine spezielle Kapselung, wenn er vom WCCP-Gerät zurück zum Client gesendet wird.

Da die WCCP-Interception dazu geführt hat, dass die Client-Anfrage erfolgreich bearbeitet wurde

(Datei aus dem Cache, Split-Stream aus dem Cache, Datei aus WAAS), kann sie als normaler Datenverkehr an das Netzwerk zurückgesendet werden, wobei die Zieladresse in den Paketen der ursprüngliche Anforderer ist. Dieser Datenverkehr kann normalerweise vom Catalyst 6500 L3/Switch-Modus geleitet werden, wenn er sich im Netzwerkpfad vom WCCP-Gerät zum Client befindet. Bei einer mit L2 verbundenen WCCP-Appliance befindet sich der Datenverkehr im Netzwerkpfad. Es ist keine Kapselung erforderlich, um die Daten vom WCCP-Gerät an den Catalyst 6500 zurückzusenden, da das Ziel nun der ursprüngliche Client ist und nicht mehr ein Server im Internet oder Intranet. Das Netzwerk verarbeitet diesen wie jeder andere IP-Datenverkehrsfluss und verwendet die Hardware-Weiterleitung im Catalyst 6500, um den angeforderten Datenverkehr an den Client zurückzugeben.

WCCP-Entität kann Anforderung nicht bearbeiten

In einigen Fällen, in denen die WCCP-Einheit den angeforderten Vorgang nicht ausführen kann, muss die WCCP-Appliance den Datenverkehr möglicherweise an den Catalyst 6500 zurücksenden und das ursprüngliche Ziel der Pakete beibehalten. Wenn dieser Datenverkehr ohne Kapselung von der WCCP-Einheit weitergeleitet wird, kann dies zu Datenverkehrsschleifen führen. Um einen fehlgeschlagenen Dienstversuch vom Client ausblenden und die Pakete an das ursprüngliche Ziel senden zu können, das bedient werden soll, müssen die Pakete unverändert bleiben, in ihren ursprünglichen Weiterleitungspfad zurückgesetzt und ohne WCCP-Abfangen an das ursprüngliche Ziel weitergeleitet werden.

In der WCCP-Rückgabemethode kann WCCP verwendet werden, um diese Pakete zu kapseln, sie an das Gerät zurückzusenden, das sie überhaupt abgefangen hat, alle Kapselungen zu entfernen und sie in den Weiterleitungspfad zurückzusetzen, von dem sie abgefangen wurden. Diese Pakete müssen normal gesendet werden, als wären sie nie von WCCP abgefangen worden.

Beispiele für solche Fälle:

- Cache-überladener Datenverkehr, bei dem Datenverkehr umgangen wird
- Regeln für Cache-Geräte, die der WCCP-Einheit die Bedienung des Datenverkehrs verweigern
- Umgehung von Datenverkehr, der einen Dienst sucht, der auf dem Gerät nicht verfügbar ist

Zurzeit kann diese Rückgabemethode nur mit GRE-Kapselung durchgeführt werden und wird von keiner Catalyst 6500-Hardware unterstützt. Wenn mit dieser Methode große Mengen an Datenverkehr an den Catalyst 6500 zurückgesendet werden, kann eine hohe CPU-Auslastung auftreten, da dieser Datenverkehr in der Software verarbeitet wird. In der Cisco IOS Softwareversion 12.1(18)SXH wird eine L2-Rückgabemethode von der Catalyst 6500-Hardware unterstützt.

GRE-Rückgabe

In Cisco IOS-Softwareversionen vor 12.2(18)SXH ist die einzige für den Catalyst 6500 unterstützte Rückgabemethode die GRE-Kapselung. Neben dem an den Rückverkehr angehängten GRE-Header wird auch ein WCCP-Header angefügt. Obwohl GRE nativ in der Hardware der Supervisor Engine 32 und der Supervisor Engine 720 unterstützt wird, führt dieser zusätzliche Header dazu, dass die GRE nicht hardwaregestützt wird. Beachten Sie, dass sowohl der Catalyst 6500 als auch die WCCP-Appliance die L2-Rückgabemethode unterstützen und aushandeln müssen.

Die Supervisor Engine 2 bietet keine GRE-Hardwareunterstützung für GRE-, Eingangs-, Ausgangs- oder WCCP-Rückgaben. Um diese Art der GRE-Entkapselung zu verarbeiten, programmiert die Cisco IOS-Software die Empfangs-Adjacency für den WCCP GRE-Tunnel auf der WCCP-fähigen Schnittstelle, um auf den Routingprozessor (RP) zu verweisen. Dies führt zur Softwareverarbeitung des Rückverkehrs.

Die Verwendung von Umleitungslisten beim Catalyst 6500, um Datenverkehr zu vermeiden, der möglicherweise über GRE zurückgegeben werden muss, ist eine effektive Methode, um die Anforderungen an die Softwareverarbeitung des Datenverkehrs zu reduzieren, der von der WCCP-Einheit zurückgesendet wird. Dies ist wesentlich effektiver, als den Datenverkehr der WCCP-Einheit zu verweigern und die GRE-Kapselung zu erzwingen und an den Catalyst 6500 zurückzusenden.

Denken Sie daran, dass die WCCP-Servicegruppe skalierbar ist. Wenn übermäßiger Datenverkehr aufgrund von Auslastung umgangen wird, wird dieser Datenverkehr zurückgesendet, was eine CPU-Auslastung für den Catalyst 6500 verursacht. Eine ordnungsgemäße Skalierung oder sogar Überkompilierung der WCCP-Servicegruppe ist die einzige Möglichkeit, diese Situation zu vermeiden.

L2-Optimierung der Rückgabe

In 12.2(18)SXH ermöglicht es eine Option der WCCP-Einheit, die L2-MAC-Adresse neu zu schreiben, anstatt den Rückgabeverkehr zu kapseln. Diese L2-Rückgabeverbesserung (Cisco Bug ID CSCuk59825) ermöglicht die Hardwareverarbeitung von zurückgesendetem Datenverkehr, wenn WCCP für die Verwendung der Ingress-Umleitung mit Maskenzuweisung konfiguriert ist.

Zusammenfassung der WCCP-Optionen

Wenn WCCP auf dem Catalyst 6500 implementiert ist, bietet es viele Konfigurationsoptionen, wie in der Tabelle dargestellt. Beachten Sie, dass die WCCP-Appliance diese Optionen aushandelt und steuert, welche Optionen vom Catalyst 6500 verwendet werden. Die Konfiguration erfolgt auf der WCCP-Appliance-Seite der WCCP-Verbindung.

Umleitungsmethode	Zuweisung Methode	Eingang/ Ausgehend	Switching-Ergebnis
L2	Hash	Eingang	Softwareverarbeitung
L2 (empfohlen)	Maske	Eingang	Vollständige Hardware-Verarbeitung mit ACL TCAM
L2	Hash	Ausgehend	Softwareverarbeitung
L2	Maske	Ausgehend	Softwareverarbeitung
GRE	Hash	Eingang	Softwareverarbeitung
GRE (PFC3 oder höher)	Maske	Eingang	Vollständige Hardware-Verarbeitung mit NetFlow
GRE	Hash	Ausgehend	Softwareverarbeitung
GRE	Maske	Ausgehend	Softwareverarbeitung

Aus Hardwaresicht erfordern alle ausgehenden WCCP-Konfigurationen eine Softwareverarbeitung und wirken sich auf die CPU-Auslastung aus. Bei Verwendung der Hash-basierten Zuweisungsmethode ist auch die Softwareverarbeitung beim Eingang erforderlich, was zu denselben potenziellen Auswirkungen auf die CPU-Auslastung führt.

Die empfohlene Methode für die WCCP-Bereitstellung auf dem Catalyst 6500 ist die L2-Umleitung mit Maskenzuweisung und, falls verfügbar, die L2-Rückgabe.

Tipp: Nur eine Option gewährleistet eine leistungsstarke, vollständig hardwarebasierte Weiterleitung: die **Eingangsbasierte L2-Umleitung mit Maskenzuweisung** auf der Supervisor Engine 2, der Supervisor Engine 32 und der Supervisor Engine 720.

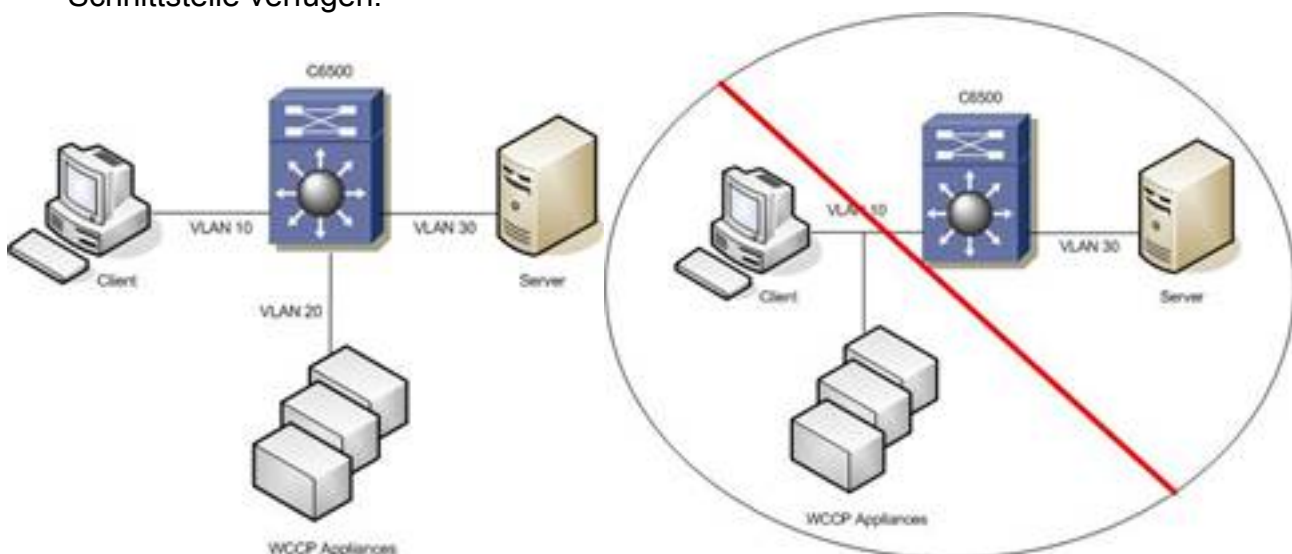
WCCP-Designempfehlungen

Verwenden Sie diese Konfigurationsempfehlungen, damit Sie die beste Methode für die WCCP-Bereitstellung für Ihre Situation ermitteln können.

Zusammenfassung

Das Netzwerk sollte so konzipiert sein, dass der WCCP-Eingang als Umleitungsmethode verwendet werden kann. Eine gute Designmethode ist ein Caching-Switch-Block als Teil eines hierarchischen L3-Verteilernetzwerks. Dadurch wird sichergestellt, dass der WCCP-Verkehr an einigen wichtigen Eingangspoints identifiziert werden kann.

- Verwenden Sie 12.2(18)SXF7 oder neuere Cisco IOS-Software.
- Identifizieren und Umleiten von Datenverkehr an Eingangs-Schnittstellen
- Verwenden Sie WCCP-Appliances, die die L2-Umleitungsmethode unterstützen.
- Verwenden Sie WCCP-Appliances, die die maskenbasierte Zuweisungsmethode unterstützen.
- Verwenden Sie möglichst eine Umleitungsliste auf dem Catalyst 6500 für Datenverkehr, der nicht von der WCCP-Appliance gewartet werden kann.
- Ändern Sie NetFlow-Timer mit Ausgangs- oder Hash-basierten Zuweisungskonfigurationen mit der Supervisor Engine 720.
- WCCP-Appliances sollten über eine dedizierte L3-Umgebung und eine SVI/VLAN-Schnittstelle verfügen.



Darüber hinaus empfiehlt Cisco Advanced Service die folgenden Designaspekte:

- In einer Umgebung, in der die L2-Umleitung mit Maskenzuweisung nicht vollständig erfolgt, ist die Leistung der Supervisor Engine 720 nicht besser als die der Supervisor Engine 2-Plattform. In diesem Fall sollten Sie keine Hardware-Upgrades durchführen und eine höhere Leistung erwarten.
- Bei großen Bereitstellungen an zentralen Standorten mit hohen Datenverkehrsanforderungen sollten Sie ein Design mit richtlinienbasiertem Routing (PBR) und Cisco Content Switching Model (CSM)/Application Control Engine (ACE) für die Überwachung und Weiterleitung von Datenverkehr in Betracht ziehen.
- WCCPv2 funktioniert wie erwartet unter perfekten Umständen. Unter bestimmten Umständen kann die CPU-Auslastung auf dem Router jedoch hoch sein, sodass das Gerät unbrauchbar wird und neu geladen werden muss:

WCCPv2 fällt aus dem hardwarebeschleunigten Eingangs-Zuweisungsmodus für die L2-Maske in jeden anderen Modus zurück, der die CPU für die MSFC erfordert. WCCP ist falsch konfiguriert (z. B. Egress statt Ingress oder L2 Hash anstelle der Maskenzuweisung).

- Bei WCCP-Bereitstellungen mit hohem Volumen und Catalyst 6500 (Caching, Streaming, WAAS oder andere Szenarien mit hoher Datenverkehrsrate) sollte die Leistung vor der vollständigen Bereitstellung des Produktionsumfangs mit Live-Datenverkehr getestet werden.

Zusätzliche Empfehlungen

Verwenden Sie eine Umleitungsliste am Switch, um zu verhindern, dass Pakete an den Catalyst 6500 zurückgesendet werden. Wenn Regeln der Cache-Geräte als Umleitungsliste auf den Catalyst 6500 verschoben werden können, kann dies zu einer besseren Hardware-Leistung führen.

NetFlow-Ressourcen auf der Supervisor Engine 720-Plattform können schnell erschöpft werden, wenn Sie eine andere Methode als die Eingangs-L2-Maskenzuweisung verwenden. Die Supervisor Engine 720 bietet mit keiner anderen Methode eine bessere Leistung als die Supervisor Engine 2.

Wenn die Supervisor Engine 720 oder die Supervisor Engine 32 in einem nicht optimalen Design verwendet werden muss, sollten Sie den Befehl **mls ip netflow create software-mode fast** verwenden, damit die NetFlow-Verarbeitung des ursprünglichen WCCP-Pakets beschleunigt werden kann. Dadurch werden die der Supervisor Engine 32 und der Supervisor Engine 720 NetFlow hinzugefügten Erweiterungen entfernt und eine Leistung bereitgestellt, die derjenigen der Supervisor Engine 2 NetFlow-Hardware entspricht.

Die Konfiguration für eine Cisco Content Engine (CE) für die Maskenzuweisung lautet:

- **wccp Version 2**
- **wccp Router-Liste *Nummer IP-Adresse***
- **wccp *Dienst Router-Listennummer Num* Maskenzuweisung**

Verwenden Sie diese Befehle, um die NetFlow-Nutzung zu überprüfen und festzustellen, ob WCCP up-NetFlow-Einträge verwendet und die Softwareverarbeitung verwendet:

- **show mls netflow table-Contention im Detail**
- **show mls netflow ip sw-installiert**
- **show mls netflow aging**

- **show mls netflow ip dynamic count**
- **show mls netflow icount**
- **show mls ip**
- **fm netflow-Zähler anzeigen**

Wenn WCCP-Softwareprobleme auftreten, weil die NetFlow-Ressourcen genutzt werden, können diese Befehle vorhandene Einträge aggressiv löschen und Platz für neue Einträge schaffen. (Dies ist nicht hilfreich, wenn es einfach mehr Einträge gibt als NetFlow-Speicherplatz.)

- **Zeitüberschreitung durch Zeitüberschreitung 3 Schwellenwert 1**
- **Ältere Mädchen 64**
- **normale Säugetiere 32**
- **mls ip netflow create software-mode fast** (Dies deaktiviert einige Änderungen der Supervisor Engine 720 NetFlow, die nicht in der Supervisor Engine 2 vorhanden waren.)

Um Paketverluste zu vermeiden, müssen die WCCP-Entitäten den Datenverkehr von einer Schnittstelle umleiten, die nicht die Schnittstelle ist, auf der das WCCP konfiguriert ist. Catalyst 6500 WCCP verwirft in dieser Situation Pakete, wenn alle Bedingungen erfüllt sind:

- Sowohl Clients als auch WCCP-Einheiten befinden sich an derselben L3-Schnittstelle.
- Für diese Schnittstelle wird eine WCCP-Umleitungsrichtlinie angewendet.
- Die GRE-Umleitungsmethode wird verwendet.
- Die Paketfragmentierung muss umgeleitet werden.
- Supervisor Engine 720 wird verwendet.

Diese Situation wird durch die in den Catalyst 6500 integrierten Schutzmechanismen verursacht. Die Cisco IOS-Software verfügt über Prüfungen, die verhindern, dass das Paket in die virtuelle Cisco IOS-Software-Schnittstelle gelangt und diese verlässt, wo es möglicherweise zu einer Schleife und unerwünschtem Verhalten führen kann. Verschieben Sie WCCP-Appliances in ihre eigene dedizierte L3-Umgebung, um dies zu verhindern.

Benutzerbasierte Ratenbegrenzung (UBRL) und WCCP arbeiten aufgrund von Flow-Masken nicht gleichzeitig an einer Schnittstelle. Für jede Unicast-Funktion gibt es eine Flussmaske für jede Schnittstelle. WCCP erfordert Vollstrom, und UBRL verwendet nur src oder dst.

WCCP-Unterstützung wurde in 12.2(18)SXF5 für die Supervisor Engine 2 und L2-Rückgabe hinzugefügt. Dies war bei der Supervisor Engine 720 nicht bis zum 12.2(18)SXH im April/Mai 2007 der Fall.

Mit Cisco IOS Software Server Load Balancing (SLB) wird nur WCCP L2 PFC-Umleitung unterstützt. andere WCCP-Konfigurationen sind nicht kompatibel, und GRE funktioniert nicht. Der beschleunigte WCCP-Befehl gilt nur für die Supervisor Engine 2/MSFC2. Ihr Zweck besteht darin, den Router zu zwingen, die Maskenzuweisung und die L2-Umleitung auszuhandeln. Das bedeutet, dass die gesamte WCCP-Umleitung in der Hardware erfolgt. Die Supervisor Engine 32 und die Supervisor Engine 720 handeln dies ohne diesen Befehl aus.

Lösungen

Hinweis: Verwenden Sie das [Command Lookup Tool](#) (nur [registrierte](#) Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

ACNS

Erinnern Sie sich bei einer standardmäßigen transparenten Caching-Umleitung daran, dass die WCCP-Einheit dem WCCP-Router die unterstützten Methoden bereitstellt und möglicherweise konfiguriert werden muss. Für Cisco ACNS werden in dieser Beispielkonfiguration die optimierten Methoden für die L2-Umleitung und die maskenbasierte Zuweisung angefordert:

1. Stellen Sie sicher, dass Sie über WCCPv2 für die Catalyst 6500-Optimierungen verfügen:

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

2. Konfigurieren Sie eine Router-Liste, die die folgenden Catalyst 6500-Router definiert:

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

3. Konfigurieren Sie den Dienst für die Verwendung der Optimierungsmethoden:

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

Vom Router aus sollte das Catalyst 6500-Design sicherstellen, dass sich die WCCP-Geräte auf einer dedizierten L3-Schnittstelle befinden, die sich nicht im aktuellen Datenverkehrspfad (Eingang oder Ausgang) befindet. Zur Gewährleistung der Hardware-Leistung sollten Datenverkehrsflüsse eingehend zum Catalyst 6500 erfasst werden, selbst wenn hierfür mehr Schnittstellen konfiguriert werden müssen, als wenn eine einzige Ausgangsschnittstelle gewählt wurde. Ein ideales Design würde den gesamten Datenverkehr vor dem Erreichen dieses Geräts aggregieren, und nur wenige Schnittstellen würden die WCCP-Eingangskonfiguration erfordern.

Die WCCP-Konfiguration für den Catalyst 6500 sollte wie folgt lauten:

1. WCCPv2 konfigurieren:

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

2. Konfigurieren einer WCCP-Dienstgruppe

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

Verwenden Sie den beschleunigten Befehl nur für Supervisor Engine 2-Plattformen mit Cisco IOS 12.1E-Software.

Die Umleitungsliste dient dazu, den Datenverkehr zu identifizieren, der für die Umleitung ausgewählt oder nicht ausgewählt werden soll. Denken Sie daran, dass diese ACL in der Hardware ausgeführt werden kann. Dies ist eine wesentlich effizientere Möglichkeit, eine Umleitung für Datenverkehr zu verhindern, der vom WCCP-Gerät nicht gewartet werden kann. Datenverkehr, der an das Gerät gesendet wird und dort nicht gewartet werden kann, muss an diesen Catalyst 6500 zurückgegeben werden, um wieder in den ursprünglichen Datenverkehrspfad zurückgesetzt werden zu können. Dies erfordert eine zusätzliche Verarbeitung. Bei den WCCP-Zugriffslisten handelt es sich um Standard- oder erweiterte Zugriffslisten.

Dieses Beispiel zeigt, dass alle Anforderungen von 10.1.1.1 bis 12.1.1.1 den Cache umgehen und alle anderen Anforderungen umgeleitet werden.

```
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
```

Konfigurieren Sie die Eingangs-WCCP-Methode für jede Eingangsschnittstelle, die den umzuleitenden Datenverkehr empfängt:

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

Damit ist die Konfiguration auf der WCCP-Appliance und dem Switch abgeschlossen, sodass die Umleitung des Datenverkehrs zu diesem Zeitpunkt erfolgen sollte.

Die endgültigen WCCP-Konfigurationen der Geräte sehen wie folgt aus.

Gerät	Konfiguration
WCCP-Appliance	<pre>wccp version 2 wccp router-list 1 router-ip-addresses wccp service router-list-num 1 l2-redirect mask assign</pre>
WCCP-Router: 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>
WCCP-Router: jede Eingangs- Schnittstelle	<pre>ip wccp redirect service in</pre>

Geben Sie den folgenden Befehl ein, um diese Konfiguration zu überprüfen:

```
Show ip wccp service detail
```

Weitere WCCP-Konfigurationsoptionen, z. B. die Gruppenadressierung mit Multicast oder zusätzliche WCCP-Sicherheit, finden Sie unter [Konfigurieren von Webcache-Diensten mit WCCP](#).

Befehle zum Anzeigen und Debuggen von WCCP IOS

- **show ip wccp service-number** - zeigt die Gesamtzahl der umgeleiteten Pakete an. Diese Zahl ist die Anzahl der Flows oder Sitzungen, die umgeleitet werden.
- **show ip wccp service-number detail** - Zeigt die Anzahl der 'umgeleiteten Pakete'. Die Anzahl ist die Anzahl der Flows oder Sitzungen, die umgeleitet werden.
- **show ip wccp web-cache detail** - zeigt an, wie viele Flüsse statt Pakete L2-Umleitungen verwenden.
- **clear ip wccp**: setzt den Zähler für die 'Umgeleiteten Pakete'-Informationen zurück.
- **show ip wccp service-number view** - zeigt die WCCP-Geräte an, die Teil der Servicegruppe sind.
- **show ip wccp service-number service** - Zeigt den Hash, die Ports und die WCCP-Priorität des Dienstes an. Services mit höherer Priorität werden zuerst aufgerufen, wenn mehrere Services auf der Schnittstelle konfiguriert werden.
- **debug ip wccp events** - Fehlerbehebung für den Zustand des WCCP-Protokolls.

- **debug ip wccp pakets** - überprüft die Kommunikation zwischen den WCCP-Paketverarbeitungseinheiten.

Wenn Sie WCCP und die Hardware-Weiterleitung verwenden, werden einige Zähler möglicherweise nicht wie erwartet angezeigt:

- Wenn die WCCP-ACL vollständig in der Hardware verarbeitet wird, zeigen die WCCP-Zähler möglicherweise keine genauen Paketzahlen an.
- Wenn das WCCP Hash-basierte Zuweisungen und NetFlow-Hardwareressourcen verwendet, können die WCCP-Zähler die Anzahl der Datenflüsse anstatt der Paketanzahl widerspiegeln.

NetFlow-Befehle

Wenn Sie über WCCP-Konfigurationen verfügen, die die Verwendung von NetFlow-Hardwareressourcen erfordern, verwenden Sie die folgenden Befehle: Multilayer Switching (MLS) und Fabric Manager (FM), damit Sie den Status der NetFlow-Ressourcen überprüfen können:

- **show mls netflow table-Contention im Detail**
- **show mls netflow ip sw-installiert**
- **show mls netflow aging**
- **show mls netflow ip dynamic count**
- **show mls netflow icount**
- **show mls ip**
- **fm netflow-Zähler anzeigen**

WCCP-Fehler

Diese Tabelle mit Bug-IDs und Auflösungen von Cisco unterstützt die allgemeine Empfehlung, die Cisco IOS Software Version 12.2(18)SXF7 oder höher zur bestmöglichen Unterstützung von WCCP zu verwenden.

Cisco Bug-ID	Lösung in Cisco IOS-Softwareversion	Details
CSCsd20327	12.2(18)SXF7	WCCP für Service 90 wird hoch- und heruntergefahren und verursacht einen Verlust des WCCP-Dienstes. Dieses Problem tritt auf, wenn die Services 81, 82 und 90 konfiguriert wurden. Die Paketspuren weisen darauf hin, dass der Router 'Here_I_Am'-Nachrichten aus dem Cache mit 'I_See_You'-Nachrichten antworten könnte, die eine falsche Ziel-IP-Adresse enthalten.
CSCsa7785	12.2(18)SXF6	Ein Neuladen kann auftreten, wenn Sie den WCCP L2-Umleitungs- und Maskenzuweisungsmodus mit einer Host-basierten Standard-ACL als WCCP-Umleitungszugriffskontrollliste verwenden.
CSCse69713	12.2(18)SXF6	Wenn alle Cache-Engines in einer WCCP-Servicegruppe verloren gehen, wird der Datenverkehr nicht in der Hardware, sondern in der Software verarbeitet.
CSCsd28870	12.2(18)SXF5	In einer WCCP-Liste für die Umleitung von ACLs werden ACEs, die mit dem log-Schlüsselwort

CSCsb61021 12.2(18)SXF5	<p>konfiguriert sind, nicht in die TCAM-Tabelle programmiert.</p> <p>Eine hohe CPU-Auslastung kann auf einer Supervisor Engine 720 oder einer Supervisor Engine 32 auftreten, wenn die IP-Spoofing-Funktion auf einer Cache-Engine konfiguriert ist und die WCCP-Umleitung in Ausgangsrichtung konfiguriert wird. IP-Spoofing-Pakete aus der Cache-Engine mit einem Ziel entweder des Clients oder des Servers werden in der Software anstatt der Hardware geschickt.</p>
CSCsb21972 12.2(18)SXF2	<p>Verwenden Sie als Problemumgehung den Befehl ip wccp service redirect in sowohl für die Eingangs- als auch die Ausgangs-Schnittstellen.</p> <p>Wenn sowohl WCCP als auch NDE konfiguriert sind, werden möglicherweise zahlreiche Trace-Backacks durch Ausrichtungsfehler verursacht, und die CPU-Auslastung kann unannehmbar hoch sein.</p>
CSCeh85087 12.2(18)SXF	<p>Wenn in der WCCP-Umleitungsliste eine benutzerdefinierte "deny ip any any any any any"-Einstellung festgelegt ist und wenn viele WCCP-Servicegruppen bedient werden, wird der mit einigen Servicegruppen verknüpfte Datenverkehr nicht an CE-Router umgeleitet.</p>
CSCeh56916 12.2(18)SXF	<p>Wenn ein WCCP-Dienst aktiviert ist, wenn die Maskenzuweisung als Zuweisungsmethode konfiguriert ist und sich mindestens fünf Caches in der Dienstgruppe befinden, können Protokollmeldungen, die an den Cache gesendet werden, überlaufen und Speicherbeschädigungen und das erneute Laden verursachen.</p>
CSCsb18740 12.2(18)SXF und SXE6	<p>Im GRE-basierten Weiterleitungsmodus verwendet WCCP unnötig einen Software-Cache, der die CPU-Auslastung von MSFC erhöht.</p>
CSCsb26773 12.2(18)SXF	<p>Eine eingehende ACL kann dazu führen, dass die WCCP-Umleitung fehlschlägt und der gesamte umgeleitete Datenverkehr verloren geht.</p>
CSCsa90830 12.2(18)SXE2	<p>Der eingehende WCCP-umgeleitete Datenverkehr verwendet die NetFlow-Tabelle für Hardware-Switching, wenn die Cache-Engine für die GRE-Weiterleitung mit dem Maskenzuweisungsmodus konfiguriert ist. Wenn die NetFlow-Tabelle voll ist, schlägt die WCCP-Eingangsumleitung fehl.</p>
CSCec55429 12.2(18)SXE	<p>Die Liste der WCCP-Servicegruppen wird in der Reihenfolge gescannt, in der die Servicegruppen erstellt werden, und nicht nach Priorität. Wenn mehrere dynamische WCCP-Dienste definiert sind, wird Datenverkehr, der die Auswahlkriterien für mehr als eine Servicegruppe erfüllt, nicht an die Servicegruppe mit der höchsten Priorität umgeleitet.</p>
CSCuk50878 12.2(18)SXE	<p>In einer Version, in der die Cisco Bug-ID</p>

CSCec55429 behoben ist, nachdem für alle Caches in einer Servicegruppe mehrere Ereignisse aufgetreten sind, die im WCC-Cache 'Loss' und 'Cache gefunden' waren, können diese Ereignisse auftreten:

- Der Zugriff auf gefälschte Speichermodule kann auftreten.
- Das Hinzufügen und Löschen von WCCP-Diensten kann fehlschlagen.
- Der Befehl **show ip wccp** zeigt den WCCP-Dienst an, aber die Ausgabe des Befehls **show ip wccp service_number** zeigt den WCCP-Dienst nicht.

[CSCsa67611](#) 12.2(18)SXE

Bei eingehenden MPLS-Paketen (Multiprotocol Label Switching), die auf einer Nicht-MPLS-Schnittstelle (Tag-zu-IP-Pfad), auf der eine Ausgabefunktion konfiguriert ist (z. B. Ausgangszugriffskontrollliste oder Ausgangs-WCCP), werden möglicherweise nicht die Ausgabefunktionen angewendet. Dieses Problem tritt auf, weil die ACL-Suche für die Ausgabe umgangen wird.

[CSCeh13292](#) 12.2(18)SXD4

Die Konfiguration von WCCPv2 auf einer Supervisor Engine 720 verursacht eine hohe CPU-Auslastung.

[CSCeb28941](#) 12.2(18)SXD1

Network Address Translation (NAT) funktioniert nicht mit konfigurierbarem WCCP.

[CSCed92290](#) 12.2(17d)SXB2

WCCP-umgeleitete Pakete, die keinen Eintrag im Next-Hop Address Resolution Protocol (ARP)-Cache enthalten, werden verarbeitet, um eine ARP-Anforderung zu generieren. Aufgrund der WCCP-Umleitung wird jedoch keine ARP-Anforderung gesendet, der ARP-Cache wird nie für den nächsten Hop aufgefüllt, und nachfolgende WCCP-umgeleitete Pakete werden weiterhin verarbeitet.

[CSCuk59825](#) 12.2(17d)SXF5 -
Sup2 Whitney1.0 für
Sup720

Diese Cisco IOS-Softwareversion bietet zusätzliche Hardware-Unterstützung für L2-Rückverkehr. Die WCCP Request for Comment (RFC) gibt die L2-Rückgabe als optionale Funktion für die Aushandlung zwischen Router und Cache an. Bisher hat WCCP für die Cisco IOS-Software die Aushandlung dieser Funktion nicht gestattet, da der erforderliche Hardwaresupport fehlt. Diese Unterstützung ist jetzt verfügbar, sodass die Aushandlung der L2-Rückgabe im WCCP-Protokollaustausch zwischen Router und Cache aktiviert werden kann.