

# Guida alla configurazione di WCCP sulle piattaforme Catalyst 6500 con elevato utilizzo della CPU

## Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Panoramica funzionale di WCCP](#)

[WCCP e Catalyst 6500](#)

[Metodo di assegnazione WCCP](#)

[Dettagli metodo di assegnazione basato su hash](#)

[Dettagli metodo di assegnazione basato su maschera](#)

[Metodo di reindirizzamento WCCP](#)

[Metodo di inoltro L3 \(GRE\)](#)

[Ingresso - Reindirizzamento L3 \(GRE\) + Assegnazione hash](#)

[Ingresso - Reindirizzamento L3 \(GRE\) + Assegnazione maschera](#)

[Uscita - Reindirizzamento L3 \(GRE\) + Assegnazione hash](#)

[In uscita - reindirizzamento L3 \(GRE\) + assegnazione maschera](#)

[Metodo di inoltro L2](#)

[Ingresso - L2 + Assegnazione hash](#)

[Ingresso - L2 + Assegnazione maschera](#)

[In uscita - L2 + Assegnazione hash](#)

[In uscita - L2 + Assegnazione maschera](#)

[Metodo di restituzione WCCP](#)

[L'entità WCCP può elaborare la richiesta](#)

[L'entità WCCP non può elaborare la richiesta](#)

[Restituzione GRE](#)

[Miglioramento reso L2](#)

[Riepilogo delle opzioni WCCP](#)

[Suggerimenti per la progettazione di WCCP](#)

[Riepilogo](#)

[Ulteriori suggerimenti](#)

[Soluzioni](#)

[ACN](#)

[Comandi WCCP IOS Show e Debug](#)

[Comandi NetFlow](#)

[Difetti WCCP](#)

# Introduzione

Questo documento descrive come utilizzare il protocollo WCCP (Web Cache Communication Protocol) sulla piattaforma Cisco Catalyst serie 6500.

WCCP è stato originariamente progettato come metodo per intercettare il traffico Web (HTTP) e inoltrarlo a un dispositivo di cache locale, dove potrebbe essere servito a un client da una posizione locale e conservare costosa larghezza di banda WAN.

Dal punto di vista dell'utente della rete, WCCP è trasparente in quanto viene utilizzato a livello di rete, senza alcuna configurazione speciale da parte dell'utente, per identificare e reindirizzare il traffico Web che attraversa un dispositivo di livello 3 (L3) su un dispositivo di cache locale. Anche se WCCP era stato originariamente progettato per il traffico Web, il metodo trasparente di reindirizzamento è diventato un meccanismo molto utile per affrontare altri problemi con i contenuti ad alto volume su collegamenti a basso volume. Per questo motivo, alle versioni più recenti di WCCP è stato aggiunto un supporto aggiuntivo per il protocollo. Tali tecnologie aggiuntive includono protocolli quali HTTP, HTTPS, FTP, streaming video e tecnologie di memorizzazione dei file nella cache, ad esempio CIFS (Common Internet File System). Queste tecnologie supportano le nuove soluzioni e piattaforme Cisco, quali WAFS (Wide Area File Services), WAAS (Wide Area Application Services), AON (Application Oriented Networking) e le funzionalità avanzate del software ACNS (Application and Content Networking Software).

L'adozione del protocollo WCCP è in aumento nelle aziende che implementano i più recenti strumenti di produttività, come ad esempio comunicazioni e formazione basate su video, nonché video live e on-demand. Gli sforzi per controllare i costi, come ad esempio i data center consolidati, creano la necessità per WCCP di supportare servizi aggiuntivi a larghezza di banda estremamente elevata.

Data l'importanza di WCCP con le attuali reti ricche di contenuti, alcune piattaforme, come Catalyst 6500, hanno implementato le prestazioni assistite da hardware con WCCP in modo da ridurre il carico di CPU richiesto per il protocollo. In questo documento viene descritto come implementare WCCP su Catalyst 6500 per ottimizzare l'utilizzo dell'hardware e ridurre il carico della CPU.

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

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

### Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Switch Cisco Catalyst serie 6500
- Software Cisco IOS release 12.1(50)SY o successive con Supervisor Engine 2T (Policy Feature Card 4)
- Software Cisco IOS versione 12.2(18)SXD1 o successive con Supervisor Engine 720 (Policy Feature Card 3)

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

## Panoramica funzionale di WCCP

La funzionalità generalmente nota come WCCP in realtà include tre componenti:

1. Funzionalità implementata solo sul router o sullo switch
2. Funzionalità implementata solo nell'entità di elaborazione del traffico, ad esempio una cache Web
3. WCCP implementato su entrambi i lati

In questo documento vengono esaminate le tre caratteristiche operative di WCCP seguenti:

1. Il metodo di **assegnazione** determina il traffico WCCP e i dispositivi WCCP selezionati per la destinazione del traffico. Il protocollo WCCP supporta la configurazione in cluster di più dispositivi.
2. Il metodo di **reindirizzamento** inoltra il flusso del traffico all'appliance WCCP quando è necessario modificare il percorso di rete normale attraversato dal traffico.
3. Il metodo **return** determina il modo in cui il traffico viene inviato al router dall'appliance WCCP se non è stato possibile soddisfare il traffico. Nei casi in cui l'accessorio WCCP evita la richiesta, i pacchetti vengono restituiti direttamente al richiedente.

## WCCP e Catalyst 6500

Catalyst 6500 Supervisor Engine 2, Supervisor Engine 32 e Supervisor Engine 720 supportano le seguenti funzionalità e metodi WCCP:

- WCCP versione 2 (WCCPv2)
- Metodo di assegnazione basato su hash
- Metodo di assegnazione basato su maschera (accelerato da hardware)
- Metodo di reindirizzamento GRE (Generic Routing Encapsulation) L3 (con accelerazione hardware su Supervisor Engine 32 e Supervisor Engine 720)
- Metodo di reindirizzamento layer 2 (L2) (accelerazione hardware su Supervisor Engine 2, Supervisor Engine 32 e Supervisor Engine 720)
- Metodo GRE restituito
- Metodo di ritorno L2 con software Cisco IOS versione 12.2SXH (accelerazione hardware su Supervisor Engine 2, Supervisor Engine 32 e Supervisor Engine 720)

Per ulteriori informazioni su queste funzionalità, consultare il documento sulla [configurazione di WCCP nella guida alla configurazione del software Cisco IOS serie 6500, versione 12.2SX](#).

# Metodo di assegnazione WCCP

L'assegnazione WCCP determina il traffico reindirizzato dal protocollo WCCP e l'entità WCCP che riceve il traffico reindirizzato.

Quando il protocollo WCCP è configurato su un'interfaccia di un router e su un'entità WCCP, il dispositivo di reindirizzamento (Catalyst 6500) deve sapere quale traffico deve essere reindirizzato e dove deve essere inviato. Le entità WCCP all'interno di un cluster di gruppi di servizi comunicano tutte tramite il protocollo WCCP con Catalyst 6500; viene tuttavia selezionato un accessorio WCCP per rappresentare il cluster in modo da controllarne il funzionamento (tramite il metodo di assegnazione, il metodo di reindirizzamento e così via). L'appliance WCCP e il router possono negoziare il metodo di distribuzione dei pacchetti tra le cache Web di un gruppo di servizi. Un gruppo di servizi è definito come una relazione multi-a-molti tra un massimo di 32 router e 32 entità WCCP. La negoziazione è per gruppo di servizi; pertanto, le cache web che partecipano a più gruppi di servizi possono negoziare un metodo di assegnazione diverso per ogni gruppo di servizi. I servizi WCCP attualmente disponibili sono:

## Servizio WCCP Protocollo

cache Web	HTTP
53	Cache DNS
60	FTP
61	WAAS - avanti
62	WAAS - reverse
70	HTTPS
80	Protocollo RTSP (Real-Time Streaming Protocol)
81	MMSU (Microsoft Media Server) over UDP
82	MMS over TCP (MST)
83	RTSP con UDP (RTSPU)
89	WAAS CIFS-Cache
98	Web Cache personalizzata
99	Proxy reverse
90-97	Configurabile dall'utente *

\* I servizi configurabili dall'utente sono implementati nel Catalyst 6500 con un comando a livello di interfaccia applicato alla direzione in entrata o in uscita. Le implicazioni della scelta di entrata o uscita sono discusse in seguito, ma il metodo preferito è quello in entrata, perché un elenco di reindirizzamento può essere abbinato a WCCP per ottimizzare le prestazioni dell'hardware.

Una volta configurato per WCCP, un router annuncia i metodi di assegnazione supportati per un gruppo di servizi nei messaggi di comunicazione WCCP. L'assenza di un messaggio di questo tipo implica che Catalyst 6500 supporta solo il metodo di assegnazione basato su hash predefinito.

Al termine della negoziazione tra lo switch Catalyst 6500 e l'appliance WCCP, l'entità designata WCCP informa lo switch Catalyst 6500 in merito al traffico da reindirizzare e alle entità WCCP a cui il traffico è assegnato. Ad esempio, l'entità WCCP può informare Catalyst 6500 di reindirizzare tutto il traffico Web da una particolare subnet ai motori di cache 1 - 4 nel gruppo di servizi quando sono disponibili più di quattro dispositivi WCCP.

Per WCCP sono disponibili due metodi di assegnazione:

1. Per impostazione predefinita, l'**assegnazione basata su hash** utilizza un algoritmo hash basato su software insieme alle direttive dell'appliance designata WCCP per determinare

quale appliance WCCP riceve traffico. In una piattaforma Supervisor Engine 32 o Supervisor Engine 720, le risorse hardware NetFlow vengono utilizzate per applicare un determinato livello di assistenza hardware.

2. L'**assegnazione basata su maschera** utilizza le funzionalità hardware di Catalyst 6500, in particolare la TCAM (Ternary Content Indirissable Memory) dell'elenco di controllo di accesso (ACL), per assegnare il traffico alle entità WCCP. Questo è il metodo preferito.

Tutti i dispositivi all'interno di un gruppo di servizi WCCP devono utilizzare lo stesso metodo di assegnazione. I metodi di assegnazione vengono configurati sull'entità WCCP e appresi da Catalyst 6500. Per ulteriori informazioni, fare riferimento a [Suggerimenti per la progettazione WCCP](#).

## Dettagli metodo di assegnazione basato su hash

Il meccanismo di assegnazione basato su hash si basa su un algoritmo eseguito nel software. Per utilizzare l'algoritmo hash, il primo pacchetto di un particolare flusso viene inviato dal percorso hardware al percorso software in cui viene eseguito l'hash.

Il software esegue un hash XOR di vari componenti del flusso e viene fornito con un hash che divide i flussi di traffico verso le varie entità WCCP. Il meccanismo hash determina la modalità di distribuzione del traffico tra le entità WCCP disponibili.

Il risultato dell'hash viene programmato nella tabella hardware NetFlow dove vengono inoltrati i pacchetti successivi in tale flusso. Indipendentemente dai campi disponibili per l'hashing da WCCP, viene utilizzata la cinque tupla completa. Ciò significa che NetFlow viene messo in modalità interfaccia, flusso completo quando WCCP è abilitato. Questo ha implicazioni su altre funzionalità che potrebbero richiedere risorse NetFlow. Per ulteriori informazioni, vedere la sezione [Difetti WCCP](#).

Una domanda comune su WCCP su Catalyst 6500 è: "Perché l'utilizzo della CPU aumenta quando si abilita WCCP?" Quando vengono utilizzate assegnazioni basate su hash, l'elaborazione basata su software del pacchetto iniziale in ogni flusso rappresenta un carico per la CPU ed è molto spesso la causa di un maggiore utilizzo. Con l'hardware di inoltre PFC3 (Policy Feature Card 3) attualmente disponibile, se WCCP è configurato come funzione di uscita o se è in uso un'assegnazione basata su hash (in entrata o in uscita), è sempre necessario un certo livello di elaborazione software.

L'utilizzo del metodo di assegnazione basato su hash influisce sulle seguenti funzionalità:

- **Tabella NetFlow:** il numero di voci supportate dal PFC è limitato e la maschera di flusso cambia in full-flow dell'interfaccia per l'intera tabella NetFlow.
- **Utilizzo CPU** - L'utilizzo della CPU aumenta man mano che il primo pacchetto in ogni flusso viene commutato dal software.
- **Prestazioni:** la velocità con cui il traffico viene inviato alla CPU per la ricerca è limitata in modo da proteggere la CPU.
- **Funzioni NetFlow** - Altre funzionalità che utilizzano risorse NetFlow potrebbero essere interessate se le risorse NetFlow vengono consumate da WCCP.

Le limitazioni e le implicazioni causate dai requisiti di assegnazione basati su hash per l'elaborazione software sono applicabili sia al traffico in entrata che in uscita. L'impatto sulla CPU può essere esacerbato se la rete è soggetta a modelli di traffico atipici, ad esempio un attacco Denial of Service (DoS). In un attacco tipico o in un'epidemia di worm, ogni pacchetto inviato da

un host è indirizzato a una nuova destinazione o porta, causando l'elaborazione di ogni pacchetto nel software. Poiché il traffico reindirizzato WCCP viene inviato esplicitamente alla CPU per l'elaborazione del primo pacchetto, esistono metodi di protezione limitati. L'uso di voci ACL "deny" sull'interfaccia può limitare l'invio di dati alla CPU; tuttavia, non esistono limitatori di velocità o altre protezioni contro questo tipo di attacchi.

## Dettagli metodo di assegnazione basato su maschera

L'assegnazione basata su maschera viene gestita in modo diverso a seconda che sia configurata in ingresso o in uscita.

Con l'assegnazione basata su maschera in entrata, la maschera viene programmata nel TCAM ACL prima dell'inoltro dei pacchetti, quindi non sono necessarie la tabella NetFlow e l'elaborazione del software. L'entità WCCP sceglie un numero di bucket di hash e assegna una maschera di indirizzo e un accessorio WCCP a ogni bucket. Una volta completate le assegnazioni, il supervisore programma una voce TCAM e una adiacenza hardware per ciascun bucket e reindirizza i pacchetti che corrispondono alla maschera dell'indirizzo all'accessorio WCCP associato tramite una riscrittura L2.

Se WCCP è configurato come funzione in entrata, potrebbe utilizzare una voce ACL redirect-adjacency nella tabella ACL hardware. Una volta che WCCP corrisponde alla voce, usa un'adiacenza appropriata per eseguire una riscrittura L2 o un incapsulamento GRE. Pertanto, quando si utilizza l'assegnazione della maschera in entrata, sia la riscrittura L2 (Supervisor Engine 2, Supervisor Engine 32 e Supervisor Engine 720) che l'incapsulamento GRE (Supervisor Engine 32 e Supervisor Engine 720) vengono eseguiti nell'hardware.

Se WCCP è configurato come funzione di uscita, le adiacenze di reindirizzamento ACL non sono supportate nell'hardware perché i pacchetti nel flusso sono già stati instradati dal sistema. Il primo pacchetto di un flusso viene inviato al software per l'elaborazione. Una volta determinata la corretta adiacenza di reindirizzamento, viene programmata nell'hardware NetFlow (anziché ACL TCAM), dove l'ingresso punta a un'adiacenza che esegue una riscrittura L2 o un incapsulamento GRE. I pacchetti successivi nel flusso vengono reindirizzati nell'hardware dall'hardware NetFlow.

**Nota:** Se WCCP è configurato come funzione di uscita, l'assegnazione della maschera richiede l'elaborazione del software, che nega qualsiasi vantaggio del metodo di assegnazione basato sulla maschera.

Delle due opzioni basate su maschera, solo l'assegnazione basata su maschera in entrata consente l'inoltro completo basato su hardware per i pacchetti iniziali e successivi. Qualsiasi altra opzione, come l'uso dell'assegnazione basata su hash o dell'elaborazione in uscita, causa la commutazione software del pacchetto iniziale e l'inoltro a commutazione hardware dei pacchetti successivi.

## Metodo di reindirizzamento WCCP

L'entità WCCP, non Catalyst 6500, detta le tabelle hash e gli insiemi mask/valori su Catalyst 6500, quindi il metodo di reindirizzamento viene configurato su tale appliance e non sullo switch Catalyst 6500. Catalyst 6500 determina il miglior metodo di reindirizzamento disponibile, in base alle comunicazioni WCCP con l'entità/il gruppo WCCP. Questa negoziazione determina la modalità di

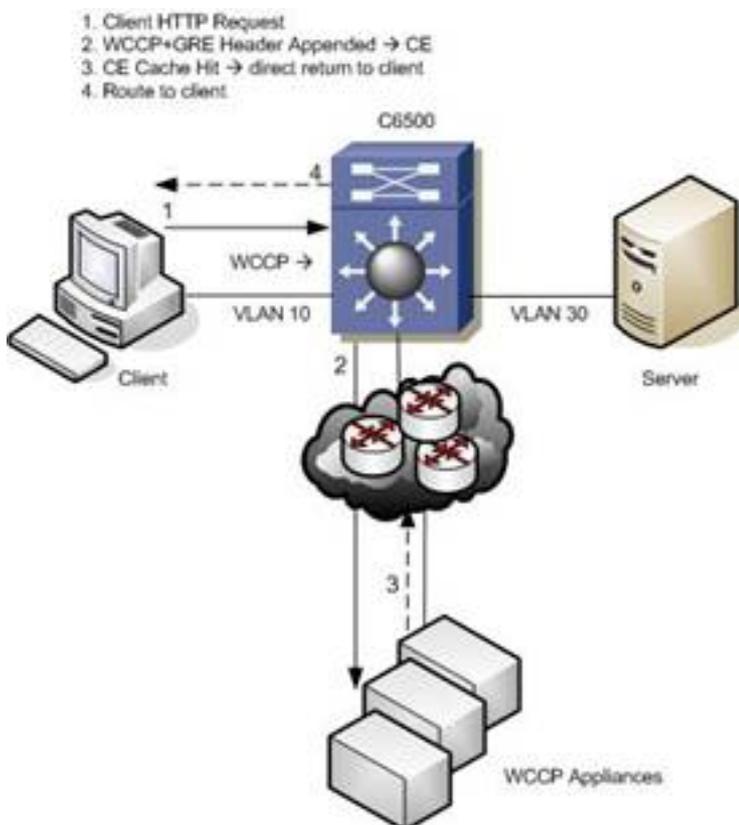
inoltro del traffico reindirizzato all'accessorio. Sono disponibili due opzioni di reindirizzamento: L3 (GRE) e L2 (riscrittura dell'indirizzo MAC).

Con WCCPv1, l'unica opzione è il reindirizzamento L3, noto anche come incapsulamento GRE. Con il reindirizzamento L3, ciascun pacchetto reindirizzato WCCP è incapsulato in un'intestazione GRE contrassegnata da un protocollo di tipo 0x883E seguito da un'intestazione di reindirizzamento WCCP a quattro ottetti, che viene successivamente inviata all'appliance WCCP (ad esempio un motore di cache).

Con l'introduzione di WCCPv2, è stato aggiunto il reindirizzamento L2, noto anche come reindirizzamento WCCP accelerato, per sfruttare i vantaggi delle piattaforme di switching hardware come Catalyst 6500. Quando WCCP utilizza il reindirizzamento L2, l'appliance WCCP e Catalyst 6500 devono essere L2 adiacenti (all'interno della stessa VLAN L2). Il traffico L2 reindirizzato non usa l'incapsulamento GRE; al contrario, l'indirizzo di destinazione MAC viene riscritto dallo switch Catalyst 6500 su quello dell'entità WCCP connessa all'L2 e inoltrato tramite la normale commutazione hardware.

**Nota:** il metodo di inoltro al dispositivo WCCP potrebbe non essere lo stesso utilizzato dal dispositivo WCCP per rimandare il traffico al Catalyst 6500. WCCP viene utilizzato per negoziare un metodo forward e return supportato da entrambi i dispositivi. Vedere [Metodo di restituzione WCCP](#).

## Metodo di inoltro L3 (GRE)



L'operazione WCCP L3 implica l'uso del GRE come metodo di incapsulamento. I pacchetti reindirizzati sono incapsulati in un'intestazione GRE con un tipo di protocollo 0x883e e un'intestazione di reindirizzamento WCCP da 4 byte che include un ID servizio e un bucket di hash corrispondenti (solo WCCPv2). L'uso del GRE consente di separare il client WCCP dallo

switch Catalyst 6500 con più hop L3 (indirizzati).

In questo scenario, le opzioni disponibili per il reindirizzamento WCCP includono:

1. In ingresso - reindirizzamento L3 (GRE) + assegnazione hash; è necessaria l'elaborazione del software.
2. In ingresso - reindirizzamento L3 (GRE) + assegnazione maschera; questa operazione richiede l'elaborazione hardware completa ed è disponibile solo sul Supervisor Engine 32 o sul Supervisor Engine 720.
3. uscita - reindirizzamento L3 (GRE) + assegnazione hash; è necessaria l'elaborazione del software.
4. uscita - reindirizzamento L3 (GRE) + assegnazione maschera; è necessaria l'elaborazione del software.

### **Ingresso - Reindirizzamento L3 (GRE) + Assegnazione hash**

Sul Supervisor Engine 2, ciascun pacchetto GRE viene inviato all'MSFC (Multilayer Switch Feature Card) per essere elaborato. Poiché l'incapsulamento GRE non è supportato nell'hardware, l'MSFC deve applicare entrambe le intestazioni GRE e WCCP, forzando la commutazione software per tutto il traffico.

Con il metodo di assegnazione basato su hash, Supervisor Engine 32 e Supervisor Engine 720 inoltrano il primo pacchetto di ogni flusso nel software in modo da stabilire una voce della tabella NetFlow. Il pacchetto viene quindi incapsulato nel GRE (l'incapsulamento e l'inoltro del pacchetto iniziale vengono eseguiti nel software) e inoltrato all'appliance WCCP.

La definizione della voce NetFlow influisce sull'utilizzo della CPU, ma il successivo inoltro dei pacchetti viene eseguito nell'hardware per Supervisor Engine 720 e Supervisor Engine 32. I modelli di traffico, in particolare il numero di flussi univoci, determinano la quantità di CPU utilizzata. Se le risorse NetFlow dello switch Catalyst 6500 sono utilizzate, tutto il traffico viene inoltrato nel software.

Le risorse NetFlow del supervisor PFC variano a seconda della piattaforma in uso. Al momento, le risorse NetFlow più grandi sono disponibili sul PFC-3BXL sulla piattaforma Supervisor Engine 720.

### **Ingresso - Reindirizzamento L3 (GRE) + Assegnazione maschera**

Sul Supervisor Engine 2, ciascun pacchetto GRE viene inviato all'MSFC per l'elaborazione. Poiché l'incapsulamento GRE non è supportato nell'hardware, l'MSFC deve applicare entrambe le intestazioni GRE e WCCP, forzando la commutazione software per tutto il traffico.

Con il metodo di assegnazione basato su maschera, Supervisor Engine 32 e Supervisor Engine 720 inoltrano i pacchetti iniziali e successivi nell'hardware, perché il GRE è supportato a livello nativo e l'assegnazione della maschera utilizza l'hardware ACL TCAM per l'inoltro.

### **Uscita - Reindirizzamento L3 (GRE) + Assegnazione hash**

Sul Supervisor Engine 2, ciascun pacchetto viene inviato all'MSFC per l'elaborazione. Poiché

l'incapsulamento GRE non è supportato nell'hardware, l'MSFC deve applicare entrambe le intestazioni GRE e WCCP, forzando la commutazione software per tutto il traffico.

Con il metodo di assegnazione basato su hash con Supervisor Engine 32 e Supervisor Engine 720, Catalyst 6500 inoltra il pacchetto iniziale di ogni flusso nel software in modo da stabilire la voce della tabella NetFlow. Il pacchetto viene quindi incapsulato nel GRE e inoltrato all'entità WCCP.

La definizione della voce NetFlow influisce sull'utilizzo della CPU, ma il successivo inoltrato dei pacchetti viene eseguito nell'hardware. I modelli di traffico, in particolare il numero di flussi univoci, determinano la quantità di CPU utilizzata. Se le risorse NetFlow dello switch Catalyst 6500 sono utilizzate, tutto il traffico viene inoltrato nel software.

Le risorse NetFlow del supervisor PFC differiscono tra le varie piattaforme. Al momento, le risorse NetFlow più grandi sono disponibili sul PFC-3BXL sulla piattaforma Supervisor Engine 720.

### **In uscita - reindirizzamento L3 (GRE) + assegnazione maschera**

Sul Supervisor Engine 2, ciascun pacchetto viene inviato all'MSFC per l'elaborazione. Poiché l'incapsulamento GRE non è supportato nell'hardware, l'MSFC deve applicare entrambe le intestazioni GRE e WCCP, forzando la commutazione software per tutto il traffico.

Con il metodo di assegnazione basato su maschera con Supervisor Engine 32 e Supervisor Engine 720, il primo pacchetto di ogni flusso viene commutato dal software in modo da stabilire la voce della tabella NetFlow. Nessuno dei supervisor supporta la programmazione delle adiacenze ACL in uscita, che forza l'elaborazione del software e usa le risorse NetFlow (anziché l'ACL TCAM hardware) per il pacchetto iniziale in ciascun flusso. Il pacchetto viene quindi incapsulato nel GRE e inoltrato all'appliance WCCP.

La definizione della voce NetFlow influisce sull'utilizzo della CPU, ma il successivo inoltrato dei pacchetti viene eseguito nell'hardware. I modelli di traffico, in particolare il numero di flussi univoci, determinano la quantità di CPU utilizzata. Se le risorse NetFlow dello switch Catalyst 6500 sono utilizzate, tutto il traffico viene inoltrato nel software.

Le risorse NetFlow del supervisor PFC differiscono tra le varie piattaforme. Al momento, le risorse NetFlow più grandi sono disponibili sul PFC-3BXL sulla piattaforma Supervisor Engine 720.

### **Metodo di inoltrato L2**

Con l'inoltrato L2, le entità WCCP (ACNS, WAFS, WAAS e così via) all'interno di un gruppo di servizi fanno parte della stessa subnet e sono L2 adiacenti allo switch Catalyst 6500. Ciò consente un elevato throughput e il reindirizzamento del traffico a bassa latenza. L'interfaccia in entrata (se WCCP è configurato) e l'interfaccia in cui si trovano gli accessori WCCP devono essere su VLAN diverse.

**Nota:** Con il reindirizzamento L2, il pacchetto viene riscritto con l'indirizzo MAC di origine impostato sul router e l'indirizzo MAC di destinazione impostato sul motore di cache. L'unico svantaggio di questo metodo di reindirizzamento è che il motore di cache deve essere **L2 raggiungibile** da Catalyst 6500 e deve risiedere su un'**interfaccia L3 diversa** da quella WCCP in entrata configurata.

**Nota:** il metodo di inoltro al dispositivo WCCP potrebbe non essere lo stesso utilizzato dal dispositivo WCCP per rimandare il traffico al Catalyst 6500. WCCP viene utilizzato per negoziare un metodo forward e return supportato da entrambi i dispositivi. Vedere [Metodo di restituzione WCCP](#).

Le opzioni disponibili per il reindirizzamento WCCP in questo scenario includono:

- In ingresso - reindirizzamento L2 + assegnazione hash; è necessaria l'elaborazione del software.
- In ingresso - Reindirizzamento L2 + assegnazione maschera: questa operazione richiede l'elaborazione hardware completa ed è consigliata.
- In uscita - reindirizzamento L2 + assegnazione hash; è necessaria l'elaborazione del software.
- uscita - reindirizzamento L2 + assegnazione maschera; è necessaria l'elaborazione del software.

### **Ingresso - L2 + Assegnazione hash**

Quando configurato in entrata con l'assegnazione di hash L2 +, il traffico WCCP invia il primo pacchetto in ogni flusso ad essere commutato dal software, creando una voce NetFlow nella tabella hardware NetFlow.

**Nota:** La maschera di flusso di NetFlow è impostata sulla modalità di flusso completo dell'interfaccia, che potrebbe influire su altre funzionalità NetFlow configurate sullo switch.

Poiché WCCP è un meccanismo senza stato, le informazioni non vengono mantenute nel software; viene invece mantenuto nell'hardware come voci nella tabella NetFlow. Il traffico successivo nel flusso viene inoltrato nell'hardware finché esiste una voce della tabella NetFlow.

La definizione della voce NetFlow influisce sull'utilizzo della CPU, ma il successivo inoltro dei pacchetti viene eseguito nell'hardware. I modelli di traffico, in particolare il numero di flussi univoci, determinano la quantità di CPU utilizzata. Se le risorse NetFlow dello switch Catalyst 6500 sono utilizzate, tutto il traffico viene inoltrato nel software.

Le risorse NetFlow del supervisor PFC differiscono tra le varie piattaforme. Al momento, le risorse NetFlow più grandi sono disponibili sul PFC-3BXL sulla piattaforma Supervisor Engine 720.

### **Ingresso - L2 + Assegnazione maschera**

Se configurato in entrata, l'assegnazione di una maschera L2 + è il metodo WCCP più efficiente supportato su Catalyst 6500. Tutto il traffico viene commutato tramite hardware, incluso il pacchetto iniziale in ciascun flusso. Non è necessario alcun reindirizzamento del software; l'inoltro dei pacchetti iniziale e successivo è fornito dall'hardware.

Le risorse hardware ACL TCAM dello switch Catalyst 6500 vengono usate per preprogrammare le voci hardware prima di ricevere i pacchetti WCCP.

Per utilizzare questo metodo e utilizzare la commutazione hardware completa, l'entità WCCP deve supportare anche il reindirizzamento L2 e il metodo di assegnazione basato su maschera. La

configurazione di questo metodo viene completata sull'entità WCCP e Catalyst 6500 negozia il metodo migliore durante le comunicazioni iniziali WCCP con l'entità/il gruppo WCCP.

### In uscita - L2 + Assegnazione hash

Con l'assegnazione dell'hash L2 + in uscita, il traffico WCCP invia il primo pacchetto in ogni flusso ad essere commutato dal software, creando una voce NetFlow nella tabella hardware NetFlow.

**Nota:** La maschera di flusso di NetFlow è impostata sulla modalità di flusso completo dell'interfaccia, che potrebbe influire su altre funzionalità NetFlow configurate sullo switch.

Inoltre, se configurato nella direzione di uscita, è necessaria una ricerca FIB (Forwarding Information Base) aggiuntiva sul primo pacchetto del flusso per determinare le adiacenze associate al CE, che richiede il ricircolo dei pacchetti all'interno del Catalyst 6500. I pacchetti successivi vengono commutati da NetFlow nell'hardware.

La definizione della voce NetFlow influisce sull'utilizzo della CPU, ma il successivo inoltramento dei pacchetti viene eseguito nell'hardware. I modelli di traffico, in particolare il numero di flussi univoci, determinano la quantità di CPU utilizzata. Se le risorse NetFlow dello switch Catalyst 6500 sono utilizzate, tutto il traffico viene inoltrato nel software.

Le risorse NetFlow del supervisor PFC differiscono tra le varie piattaforme. Al momento, le risorse NetFlow più grandi sono disponibili sul PFC-3BXL sulla piattaforma Supervisor Engine 720.

### In uscita - L2 + Assegnazione maschera

Quando configurato nella direzione di uscita, L2 + assegnazione maschera commuta il primo pacchetto in ogni flusso nel software, proprio come la richiesta di assegnazione dell'hash L2 +. I pacchetti successivi vengono commutati da NetFlow nell'hardware.

**Nota:** La maschera di flusso di NetFlow è impostata sulla modalità di flusso completo dell'interfaccia, che potrebbe influire su altre funzionalità NetFlow configurate sullo switch.

il PFC2 e il PFC3 non supportano la programmazione adiacente all'ACL in uscita, che forza l'elaborazione software del pacchetto iniziale in ciascun flusso; i pacchetti successivi nel flusso vengono inoltrati nell'hardware.

La definizione della voce NetFlow influisce sull'utilizzo della CPU, ma il successivo inoltramento dei pacchetti viene eseguito nell'hardware. I modelli di traffico, in particolare il numero di flussi univoci, determinano la quantità di CPU utilizzata. Se le risorse NetFlow dello switch Catalyst 6500 sono utilizzate, tutto il traffico viene inoltrato nel software.

Le risorse NetFlow del supervisor PFC differiscono tra le varie piattaforme. Al momento, le risorse NetFlow più grandi sono disponibili sul PFC-3BXL sulla piattaforma Supervisor Engine 720.

## Metodo di restituzione WCCP

## L'entità WCCP può elaborare la richiesta

Quando il protocollo WCCP viene utilizzato per intercettare il traffico e l'entità WCCP esegue un'operazione completa su tali pacchetti, i pacchetti sono pronti per essere inviati al client dal dispositivo WCCP. Il traffico normalmente elaborato, destinato di nuovo al client sulla rete, non richiede alcun incapsulamento speciale quando viene inviato dal dispositivo WCCP di nuovo al client.

Poiché l'intercettazione WCCP ha determinato il completamento del servizio della richiesta client (file dalla cache, flusso suddiviso dalla cache, file da WAAS), è possibile rimandarla alla rete come traffico normale con l'indirizzo di destinazione nei pacchetti che costituiscono il richiedente originale. Questo traffico può in genere essere L3/switched da Catalyst 6500 se è nel percorso di rete tra l'appliance WCCP e il client; con un accessorio WCCP L2 collegato, il traffico si trova nel percorso di rete. Non è necessario alcun incapsulamento per restituirla dal dispositivo WCCP allo switch Catalyst 6500 perché la destinazione è il client originale anziché un server su Internet o sulla Intranet. La rete gestisce questo flusso come qualsiasi altro flusso di traffico IP e utilizza l'inoltro hardware nello switch Catalyst 6500 per restituire il traffico richiesto al client.

## L'entità WCCP non può elaborare la richiesta

In alcuni casi, se l'entità WCCP non è in grado di eseguire l'operazione richiesta, è possibile che l'appliance WCCP debba rinviare il traffico al Catalyst 6500 e mantenere la destinazione originale dei pacchetti. L'inoltro del traffico dall'entità WCCP senza incapsulamento può causare loop di traffico. Per nascondere al client un tentativo di servizio non riuscito e inviare i pacchetti alla destinazione originale per l'assistenza, i pacchetti devono rimanere invariati, essere riposizionati nel percorso di inoltro originale e inoltrati alla destinazione originale senza intercettazione WCCP.

Nel metodo di ritorno WCCP, i pacchetti possono essere incapsulati, rimandati al dispositivo che li ha intercettati, eliminando l'incapsulamento e reindirizzati al percorso di inoltro da cui sono stati intercettati. Questi pacchetti devono essere inviati normalmente come se non fossero mai stati intercettati da WCCP.

Esempi di tali casi includono:

- Traffico di overload della cache, in cui il traffico viene ignorato
- Regole sui dispositivi di cache che impediscono all'entità WCCP di gestire il traffico
- Traffico ignorato durante la ricerca di un servizio non disponibile nel dispositivo

Al momento, questo metodo restituito può essere eseguito solo con l'incapsulamento GRE e non è ancora supportato su alcun hardware Catalyst 6500. Se si inviano grandi quantità di traffico a Catalyst 6500 con questo metodo, si potrebbe verificare un elevato utilizzo della CPU perché il traffico viene elaborato nel software. Nel software Cisco IOS versione 12.1(18)SXH, è disponibile un metodo di ritorno L2 supportato dall'hardware Catalyst 6500.

## Restituzione GRE

Nel software Cisco IOS versioni precedenti alla 12.2(18)SXH, l'unico metodo restituito supportato per Catalyst 6500 è l'incapsulamento GRE. Oltre all'intercettazione GRE aggiunta al traffico di ritorno, viene aggiunta un'intercettazione WCCP. Sebbene GRE sia supportato in modo nativo

nell'hardware Supervisor Engine 32 e Supervisor Engine 720, questa intestazione aggiuntiva impedisce che il GRE sia assistito dall'hardware. Notare che sia Catalyst 6500 che l'accessorio WCCP devono supportare e negoziare il metodo di restituzione L2.

Il Supervisor Engine 2 non prevede supporto hardware GRE per richieste di ritorno GRE, in entrata, in uscita o WCCP. Per elaborare questo tipo di deincapsulamento GRE, il software Cisco IOS programma l'adiacenza di ricezione del tunnel WCCP GRE sull'interfaccia abilitata a WCCP in modo che punti al processore di routing (RP), con conseguente elaborazione software del traffico di ritorno.

L'uso di elenchi di reindirizzamento sullo switch Catalyst 6500 per evitare il traffico che potrebbe essere necessario restituire tramite GRE è un metodo efficace per ridurre i requisiti di elaborazione software del traffico che verrebbe inviato indietro dall'entità WCCP. Ciò è molto più efficace di aver rifiutato il traffico sull'entità WCCP e averlo forzato a essere incapsulato dal GRE e rinviato al Catalyst 6500.

Tenere presente che il gruppo di servizi WCCP è scalabile. Se il traffico in eccesso viene ignorato a causa del carico, viene rinviato al sistema, creando un carico sulla CPU dello switch Catalyst 6500. L'unico modo per evitare questa situazione consiste nell'adattare correttamente il gruppo di servizi WCCP o addirittura nel sovradimensionarlo.

## Miglioramento reso L2

Nella versione 12.2(18)SXH, un'opzione consente all'entità WCCP di riscrivere l'indirizzo MAC L2 anziché incapsulare il traffico di ritorno. Questa funzionalità L2 return enhancement (ID bug Cisco CSCuk59825) consente l'elaborazione hardware del traffico restituito quando WCCP è configurato per l'utilizzo del reindirizzamento in entrata con assegnazione della maschera.

## Riepilogo delle opzioni WCCP

Quando implementato su Catalyst 6500, WCCP offre molte opzioni di configurazione, come mostrato nella tabella. L'appliance WCCP negozia queste opzioni e controlla quali opzioni vengono utilizzate da Catalyst 6500. La configurazione viene effettuata sul lato dell'appliance WCCP della connessione WCCP.

Redirect, metodo	Assegnazione Metodo	In ingresso/ In uscita	Risultato cambio
L2	Hash	In ingresso	Elaborazione software
<b>L2 (scelta consigliata)</b>	<b>Maschera</b>	<b>In ingresso</b>	<b>Elaborazione hardware completa con ACL TCAM</b>
L2	Hash	In uscita	Elaborazione software
L2	Maschera	In uscita	Elaborazione software
GRE	Hash	In ingresso	Elaborazione software
<b>GRE (PFC3 o versione successiva)</b>	<b>Maschera</b>	<b>In ingresso</b>	<b>Elaborazione hardware completa con NetFlow full-flow</b>
GRE	Hash	In uscita	Elaborazione software
GRE	Maschera	In uscita	Elaborazione software

Dal punto di vista dell'hardware, tutte le configurazioni WCCP in uscita richiedono l'elaborazione software e influiscono sull'utilizzo della CPU. L'elaborazione del software è inoltre necessaria

quando si utilizza il metodo di assegnazione basato su hash e produce lo stesso impatto potenziale sull'utilizzo della CPU.

Il metodo consigliato per l'implementazione di WCCP su Catalyst 6500 è il reindirizzamento L2 con assegnazione di maschera e, quando disponibile, il ritorno L2.

**Suggerimento:** Solo un'opzione assicura l'inoltro ad alte prestazioni basato su hardware completo: il **reindirizzamento L2 basato su ingresso con assegnazione della maschera** su Supervisor Engine 2, Supervisor Engine 32 e Supervisor Engine 720.

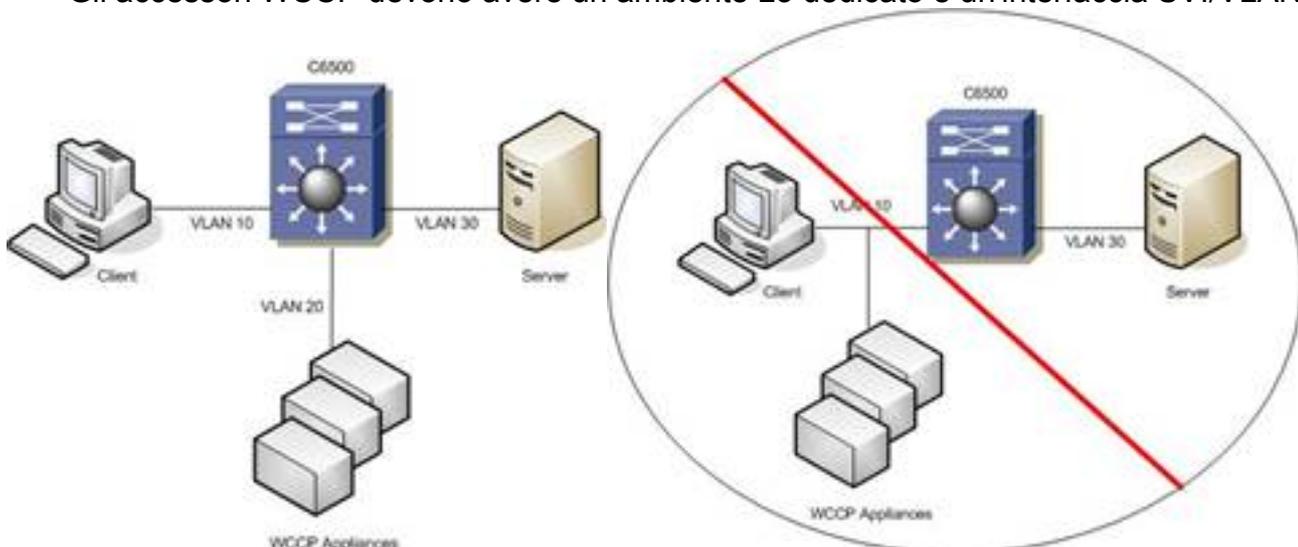
## Suggerimenti per la progettazione di WCCP

Utilizzare i suggerimenti di configurazione riportati di seguito per determinare il metodo di distribuzione WCCP più adatto alla propria situazione.

### Riepilogo

Progettare la rete in modo che l'ingresso WCCP possa essere utilizzato come metodo di reindirizzamento. Un buon metodo di progettazione consiste nell'inserire un blocco di commutazione nella cache in una rete di distribuzione L3 gerarchica. In questo modo, il traffico gestito da WCCP può essere identificato in alcune delle principali porte in entrata.

- Usare il software Cisco IOS versione 12.2(18)SXF7 o successive.
- Identifica e reindirizza il traffico sulle interfacce in entrata.
- Utilizzare appliance WCCP che supportano il metodo di reindirizzamento L2.
- Utilizzare appliance WCCP che supportano il metodo di assegnazione basato su maschera.
- Se possibile, utilizzare un elenco di reindirizzamento su Catalyst 6500 per il traffico che non può essere gestito dall'appliance WCCP.
- Modificare i timer NetFlow con le configurazioni di assegnazione basate su hash o in uscita con Supervisor Engine 720.
- Gli accessori WCCP devono avere un ambiente L3 dedicato e un'interfaccia SVI/VLAN.



Inoltre, Cisco Advanced Service consiglia le seguenti considerazioni di progettazione:

- In un ambiente in cui il reindirizzamento L2 non è completo con l'assegnazione della maschera, Supervisor Engine 720 non offre prestazioni migliori della piattaforma Supervisor Engine 2. Non aggiornare l'hardware e aspettarti prestazioni migliori in questa situazione.
- Per installazioni in siti centrali di grandi dimensioni con requisiti di traffico elevati, prendere in considerazione una progettazione con PBR (Policy-Based Routing) e Cisco Content Switching Model (CSM)/Application Control Engine (ACE) per l'intercettazione e l'inoltro del traffico.
- WCCPv2 funziona come previsto in circostanze perfette. Tuttavia, in alcune circostanze, l'utilizzo della CPU sul router può raggiungere livelli elevati che rendono il dispositivo inutilizzabile e che richiedono il ricaricamento:

WCCPv2 consente di tornare dalla modalità di assegnazione basata su maschera L2 con accelerazione hardware in qualsiasi altra modalità che richiede la CPU dell'MSFC. WCCP non è configurato correttamente (ad esempio, in uscita anziché in entrata o hash L2 anziché assegnazione di maschera).

- Qualsiasi distribuzione WCCP con elevati volumi di dati con Catalyst 6500 (caching, streaming, WAAS o altri scenari con traffico elevato) deve essere sottoposta a test delle prestazioni con traffico in tempo reale prima dell'implementazione completa della produzione.

## Ulteriori suggerimenti

Per evitare che i pacchetti vengano rimandati allo switch Catalyst 6500, usare un elenco di reindirizzamento. Se è possibile spostare una qualsiasi regola dei dispositivi cache su Catalyst 6500 come elenco di reindirizzamento, è possibile ottenere prestazioni hardware migliori.

Le risorse NetFlow sulla piattaforma Supervisor Engine 720 possono esaurirsi rapidamente se si utilizza un metodo diverso dall'assegnazione della maschera in entrata-L2. Supervisor Engine 720 non offre prestazioni migliori rispetto a Supervisor Engine 2 con altri metodi.

Nei casi in cui occorre usare Supervisor Engine 720 o Supervisor Engine 32 in una progettazione non ottimale, valutare l'opportunità di usare il comando **mls ip netflow creation software-mode fast** per velocizzare l'elaborazione NetFlow del pacchetto iniziale WCCP. In questo modo vengono rimossi i miglioramenti aggiunti a Supervisor Engine 32 e Supervisor Engine 720 NetFlow e vengono fornite prestazioni uguali a quelle dell'hardware Supervisor Engine 2 NetFlow.

La configurazione per un Cisco Content Engine (CE) per l'assegnazione della maschera è:

- **wccp versione 2**
- **elenco router wccp numero indirizzo-ip**
- **wccp servizio router-list-num num assegnazione maschera**

Utilizzare questi comandi per esaminare l'utilizzo di NetFlow e determinare se WCCP sta utilizzando voci di NetFlow attive e sta utilizzando l'elaborazione del software:

- **visualizzazione dei dettagli dei conflitti tra tabelle netflow mls**
- **show mls netflow ip sw-installed**
- **mostra durata netflow mls**
- **show mls netflow ip dynamic count**
- **show mls netflow ip count**
- **show mls ip**
- **mostra contatori fm netflow**

Se si verificano problemi relativi al software WCCP a causa dell'utilizzo delle risorse NetFlow, questi comandi potrebbero eliminare in modo aggressivo le voci esistenti e creare spazio per nuove voci. Ciò non è utile se il numero di voci è superiore al numero di spazio di NetFlow.

- **tempo di aging veloce mls 3 soglia 1**
- **mls aging long 64**
- **durata mls normale 32**
- **mls ip netflow creation software-mode fast** (disabilita alcune modifiche a Supervisor Engine 720 NetFlow che non erano nel Supervisor Engine 2).

Per evitare la perdita di pacchetti, le entità WCCP devono reindirizzare il traffico da un'interfaccia diversa da quella configurata per WCCP. Catalyst 6500 WCCP scarta i pacchetti in questa situazione quando vengono soddisfatte tutte le condizioni:

- Sia i client che l'entità WCCP si trovano sulla stessa interfaccia L3.
- Criteri di reindirizzamento WCCP applicati all'interfaccia.
- Viene utilizzato il metodo di reindirizzamento GRE.
- È necessario reindirizzare la frammentazione del pacchetto.
- Viene utilizzato Supervisor Engine 720.

Questa situazione è causata dai meccanismi di protezione integrati nel Catalyst 6500; il software Cisco IOS effettua controlli che impediscono al pacchetto di entrare e uscire dalla stessa interfaccia virtuale del software Cisco IOS dove potrebbe loop e causare un comportamento indesiderato. Per evitare questo problema, spostare le appliance WCCP nel proprio ambiente L3 dedicato.

Le tecnologie UBRL (User-based rate limiting) e WCCP non funzionano contemporaneamente su un'interfaccia a causa delle maschere di flusso. È disponibile una maschera di flusso per ogni interfaccia per ogni funzionalità unicast. WCCP richiede full-flow, mentre UBRL utilizza solo src o solo dst.

Il supporto WCCP è stato aggiunto per Supervisor Engine 2 e ritorno L2 nella versione 12.2(18)SXF5. Questa versione non è stata inclusa nel Supervisor Engine 720 fino alla versione 12.2(18)SXH di aprile/maggio 2007.

Solo il reindirizzamento WCCP L2 PFC è supportato con il software Cisco IOS SLB (Server Load Balancing); altre configurazioni WCCP non sono compatibili e il GRE non funziona. Il comando WCCP accelerated si applica solo al Supervisor Engine 2/MSFC2. Lo scopo del comando è forzare il router a negoziare l'assegnazione della maschera e il reindirizzamento L2, ossia tutto il reindirizzamento WCCP viene eseguito nell'hardware. La negoziazione tra Supervisor Engine 32 e Supervisor Engine 720 non è necessaria.

## Soluzioni

**Nota:** per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo [strumento di ricerca dei comandi \(solo utenti registrati\)](#).

Per il reindirizzamento standard della cache trasparente, ricordare che l'entità WCCP fornisce al router WCCP i metodi supportati e che potrebbe essere necessario configurarlo a tale scopo. Per le ACN Cisco, questa configurazione di esempio richiede i metodi di assegnazione L2-redirect e basato su maschera ottimizzati:

1. Accertarsi di disporre di WCCPv2 per le ottimizzazioni di Catalyst 6500:

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

2. Configurare un elenco di router che definisca gli switch Catalyst 6500 da utilizzare:

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

3. Configurare il servizio per l'utilizzo dei metodi di ottimizzazione:

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

Sul router, il design di Catalyst 6500 deve garantire che i dispositivi WCCP si trovino su un'interfaccia L3 dedicata che non sia nel percorso di traffico corrente (in entrata o in uscita). Per migliorare le prestazioni dell'hardware, è necessario acquisire i flussi di traffico in entrata verso Catalyst 6500, anche se questa operazione richiede la configurazione di più interfacce rispetto a una singola interfaccia in uscita. Un progetto ideale prevede l'aggregazione di tutto il traffico prima di raggiungere questo dispositivo e solo alcune interfacce richiedono la configurazione in entrata WCCP.

La configurazione WCCP su Catalyst 6500 deve essere:

1. Configurare WCCPv2:

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

2. Configurare un gruppo di servizi WCCP.

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

Usare il comando accelerato solo per le piattaforme Supervisor Engine 2 con software Cisco IOS 12.1E.

L'elenco di reindirizzamento viene usato per identificare il traffico da selezionare o non selezionare per il reindirizzamento. Tenere presente che questo ACL può essere eseguito sull'hardware; si tratta di un modo molto più efficiente per evitare il reindirizzamento del traffico che non può essere gestito dal dispositivo WCCP. Il traffico che viene inviato al dispositivo e non può essere gestito all'interno del quale deve essere restituito al Catalyst 6500 per essere reinserito nel percorso originale, che richiede un'elaborazione aggiuntiva. Gli elenchi degli accessi WCCP sono elenchi degli accessi standard o estesi.

Nell'esempio viene mostrato che le richieste da 10.1.1.1 a 12.1.1.1 ignorano la cache e che tutte le altre richieste vengono reindirizzate.

```
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
```

Configurare il metodo WCCP in entrata su ciascuna interfaccia in entrata che riceve il traffico da reindirizzare:

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

La configurazione dell'accessorio WCCP e dello switch è stata completata, quindi a questo punto deve essere in corso il reindirizzamento del traffico.

Le configurazioni finali WCCP dei dispositivi hanno questo aspetto.

Sul dispositivo	Configurazione
bootflash o slot0: appliance 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: globale	<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: ciascuna interfaccia in entrata	<pre>ip wccp redirect service in</pre>

Per controllare questa configurazione, immettere questo comando:

```
Show ip wccp service detail
```

Per ulteriori opzioni di configurazione WCCP, ad esempio l'indirizzamento di gruppo con multicast o la protezione WCCP aggiuntiva, vedere [Configurazione dei servizi Web Cache con WCCP](#).

## Comandi WCCP IOS Show e Debug

- **show ip wccp service-number**: restituisce il numero di pacchetti reindirizzati. Questo conteggio è il numero di flussi, o sessioni, che vengono reindirizzati.
- **show ip wccp service-number detail** - restituisce il numero di pacchetti reindirizzati. Il conteggio è il numero di flussi, o sessioni, che vengono reindirizzati.
- **show ip wccp web-cache detail**: fornisce un'indicazione di quanti flussi, anziché pacchetti, stanno utilizzando il reindirizzamento L2.
- **clear ip wccp** - reimposta il contatore per le informazioni 'Packets Redirection'.
- **show ip wcp service-number view**: visualizza i dispositivi WCCP che fanno parte del gruppo di servizi.
- **show ip wcp service-number service**: visualizza l'hash, le porte e la priorità WCCP del servizio. I servizi con priorità più alta vengono raggiunti per primi quando sull'interfaccia sono configurati più servizi.
- **debug ip wcp events** - risoluzione dei problemi di stato del protocollo WCCP.
- **debug ip wccp packets**: controlla le comunicazioni tra le entità di elaborazione dei pacchetti WCCP.

Quando si utilizza WCCP e l'inoltro hardware, alcuni contatori potrebbero non essere visualizzati

come previsto:

- Se l'ACL WCCP viene elaborato completamente nell'hardware, i contatori WCCP potrebbero non visualizzare i conteggi accurati dei pacchetti.
- Se WCCP utilizza l'assegnazione basata su hash e le risorse hardware NetFlow, i contatori WCCP potrebbero riflettere il numero di flussi anziché il numero di pacchetti.

## Comandi NetFlow

In presenza di configurazioni WCCP che richiedono l'utilizzo di risorse hardware NetFlow, utilizzare i seguenti comandi Multilayer Switching (MLS) e Fabric Manager (FM) per poter esaminare lo stato delle risorse NetFlow:

- **visualizzazione dei dettagli dei conflitti tra tabelle netflow mls**
- **show mls netflow ip sw-installed**
- **mostra durata netflow mls**
- **show mls netflow ip dynamic count**
- **show mls netflow ip count**
- **show mls ip**
- **mostra contatori fm netflow**

## Difetti WCCP

Questa tabella di ID e risoluzioni dei bug di Cisco supporta la raccomandazione generale di utilizzare il software Cisco IOS versione 12.2(18)SXF7 o successive per ottenere il miglior supporto di WCCP.

ID bug Cisco	Risolto nella versione software Cisco IOS	Dettagli
<a href="#">CSCsd20327</a>	12.2(18)SXF7	WCCP per il servizio 90 va su e giù e causa la perdita del servizio WCCP. Questo problema si verifica quando i servizi 81, 82 e 90 sono configurati. Le tracce del pacchetto indicano che il router potrebbe rispondere ai messaggi 'Here_I_Am' dalla cache con messaggi 'I_See_You' contenenti un indirizzo IP di destinazione errato.
<a href="#">CSCsa7785</a>	12.2(18)SXF6	Il ricaricamento può verificarsi quando si usano il reindirizzamento WCCP L2 e la modalità di assegnazione della maschera con un ACL standard basato su host come ACL di reindirizzamento WCCP.
<a href="#">CSCse69713</a>	12.2(18)SXF6	Quando tutti i motori di cache in un gruppo di servizi WCCP vengono persi, il traffico viene elaborato nel software anziché commutato nell'hardware.
<a href="#">CSCsd2870</a>	12.2(18)SXF5	In un elenco ACL di reindirizzamento WCCP, le voci ACE configurate con la parola chiave log non vengono programmate nella tabella TCAM.
<a href="#">CSCsb61021</a>	12.2(18)SXF5	Un elevato utilizzo della CPU potrebbe verificarsi su Supervisor Engine 720 o Supervisor Engine 32 quando

la funzionalità di spoofing IP è configurata su un motore di cache e quando il reindirizzamento WCCP è configurato nella direzione di uscita. I pacchetti con spoofing IP dal motore della cache, con destinazione client o server, vengono commutati in software anziché in hardware.

Per risolvere questo problema, usare il comando **ip wccp service redirect in** sia per l'interfaccia in entrata che per quella in uscita.

[CSCsb21972](#) 12.2(18)SXF2

Se sono configurati sia WCCP che NDE, è possibile che si verifichino numerosi traceback causati da errori di allineamento e che l'utilizzo della CPU sia inaccettabilmente elevato.

[CSCeh85087](#) 12.2(18)SXF

Quando è presente un'istruzione configurata dall'utente 'deny ip any any' nell'ACL di reindirizzamento WCCP e quando molti gruppi di servizi WCCP vengono serviti, il traffico associato ad alcuni gruppi di servizi non viene reindirizzato ai router CE.

[CSCeh56916](#) 12.2(18)SXF

Quando un servizio WCCP è abilitato, quando l'assegnazione della maschera è configurata come metodo di assegnazione e quando nel gruppo di servizi sono presenti cinque o più cache, i messaggi del protocollo inviati alla cache possono risultare in overflow e causare il danneggiamento della memoria e il ricaricamento.

[CSCsb18740](#) 12.2(18)SXF e SXE6

Nella modalità di inoltro basata su GRE, WCCP utilizza inutilmente una cache software che aumenta l'utilizzo della CPU MSFC.

[CSCsb2673](#) 12.2(18)SXF

Un ACL in entrata potrebbe impedire il reindirizzamento WCCP e causare la perdita di tutto il traffico reindirizzato.

[CSCsa90830](#) 12.2(18)SXE2

Il traffico WCCP in entrata-reindirizzato utilizza la tabella NetFlow per la commutazione hardware quando il motore di cache è configurato per l'inoltro GRE con la modalità di assegnazione della maschera. Quando la tabella NetFlow è piena, il reindirizzamento in entrata WCCP non riesce.

[CSCec5429](#) 12.2(18)SXE

L'analisi dell'elenco dei gruppi di servizi WCCP viene eseguita in base all'ordine di creazione dei gruppi di servizi anziché in base alla priorità. Se vengono definiti più servizi WCCP dinamici, il traffico che soddisfa i criteri di selezione per più gruppi di servizi non viene reindirizzato al gruppo di servizi con la priorità più alta.

[CSCuk50878](#) 12.2(18)SXE

In una versione in cui viene risolto l'ID bug Cisco CSCec55429, dopo che si sono verificati alcuni eventi 'cache perduta' e 'cache trovata' di WCC per tutte le cache di un gruppo di servizi, possono verificarsi gli eventi seguenti:

- È possibile che si verifichino accessi alla memoria spurie.
- L'aggiunta e l'eliminazione dei servizi WCCP potrebbe non riuscire.

- Il comando **show ip wcp** visualizza il servizio WCCP, ma l'output del comando **show ip wcp numero\_servizio** non visualizza il servizio WCCP.

- [CSCsa6761](#) 12.2(18)SXE È possibile che ai pacchetti MPLS (Multiprotocol Label Switching) in arrivo che escono da un'interfaccia non MPLS (da tag a percorso IP) su cui è configurata una funzionalità di output (ad esempio, ACL in uscita o WCCP in uscita) non siano applicate le funzionalità di output. Il problema si verifica perché la ricerca ACL di output viene ignorata.
- [CSCeh13292](#) 12.2(18)SXD4 La configurazione di WCCPv2 su un Supervisor Engine 720 provoca un elevato utilizzo della CPU.
- [CSCeb28941](#) 12.2(18)SXD1 Network Address Translation (NAT) non funziona con WCCP configurato.
- [CSCed92290](#) 12.2(17d)SXB2 I pacchetti reindirizzati WCCP che non hanno voce cache ARP (Address Resolution Protocol) dell'hop successivo vengono commutati per generare una richiesta ARP. A causa del reindirizzamento WCCP, tuttavia, non viene inviata alcuna richiesta ARP, la cache ARP non viene mai popolata per l'hop successivo e i pacchetti reindirizzati WCCP successivi continuano a essere commutati.
- [CSCuk59825](#) 12.2(17d)SXF5 -Sup2 Whitney1.0 per Sup720 In questa versione software Cisco IOS è stato aggiunto il supporto hardware per il traffico di ritorno L2. La RFC (Request for Comment) della WCCP specifica il ritorno L2 come funzionalità opzionale per la negoziazione tra router e cache. Finora, WCCP su software Cisco IOS non ha consentito la negoziazione di questa funzionalità perché il supporto hardware richiesto è assente. Poiché tale supporto è ora disponibile, è possibile abilitare la negoziazione del ritorno L2 nello scambio di protocollo WCCP tra router e cache.