使用Null0和MSS鉗位排除故障

目錄

簡介

本文檔介紹在Catalyst 9K上調整最大網段大小(MSS)和指向空值0的靜態路由的含義。

必要條件

需求

思科建議您瞭解以下主題：

- 關於TCP和MSS調整的概念知識
- 平台瞭解Cisco Catalyst 9K，用於控制平面轉發和調試。

支援的平台

本檔案適用於執行Cisco IOS® XE 17.3.x和更新版本的所有Catalyst 9K平台。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 執行IOS-XE 17.3.4版的Catalyst 9300系列交換器
- 執行IOS-XE 17.3.4版的Catalyst 9400系列交換器
- 用於生成流量的IXIA

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

故障排除方法

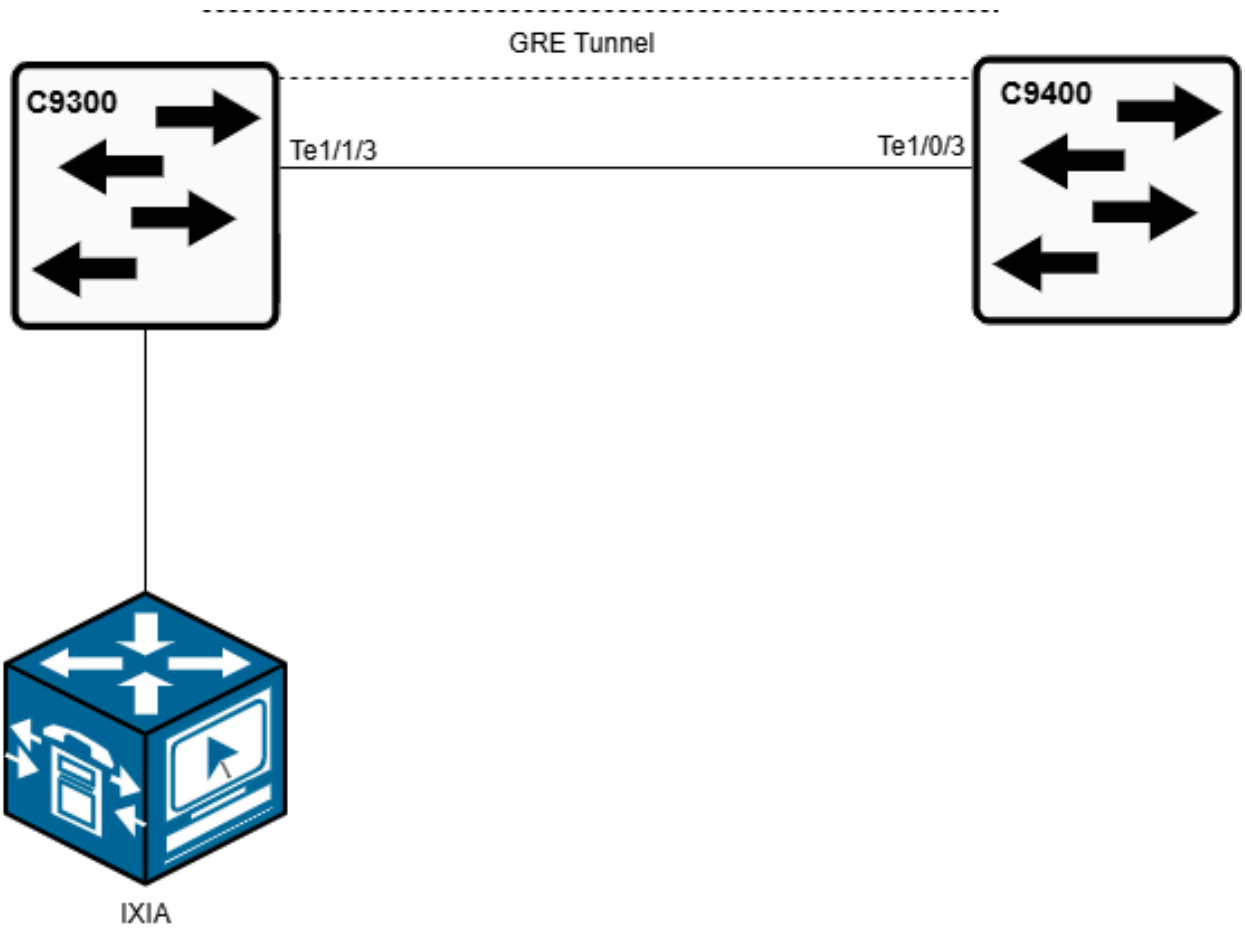
拓撲

該設定包含帶有流量發生器的C9000交換機，用於重現問題。包含用於進一步隔離的測試：

條件1:沒有「Null0」或「MSS adjust」
條件2:當靜態路由指向Null0時，無MSS調整
條件3:已啟用Null0和MSS調整

軟體和硬體版本

- 執行Cisco IOS XE 17.3.4版的Catalyst 9300和9400
- 用於生成流量的IXIA



配置要求

- 未配置「ip tcp adjust-mss」和「null0路由」
- 僅配置了「null0 route」
- 配置了「ip tcp adjust-mss」和「null0 route」
  'ip tcp adjust-mss value'(值小於最大傳輸單位(MTU))(在通道介面或交換器虛擬介面(SVI)上（輸入）)
  'ip route X.X.X.X X.X.X.X Null0'（指向Null0的靜態路由）

根據所描述的條件，您會觀察到到直接連線的邊界網關協定(BGP)對等體以及到在同一裝置上或直接連線對等體上配置的SVI的間歇性連線。在運行控制平面策略(CoPP)命令和調試時，軟體(SW)轉發隊列中的丟棄計數器也會持續增加。調查表明，發往Null0的流量將改為發往CPU。此行為阻止TCP三次握手完成，從而中斷了BGP協定。此外，對交換機上配置的SVI IP地址執行ping操作失敗。

案例

案例1.不帶「Null0」或「MSS Adjust」

如果未配置「ip tcp adjust-mss」或「null route」，則在從IXIA生成的流量之後，SW轉發隊列中的丟棄計數器將保留為「0」（如預期的那樣）。

請參閱以下日誌：

```
Cat-9400-1# Show platform hardware fed active qos queue stats internal cpu policer
CPU Queue Statistics
============================================================================================
(default) (set) Queue Queue
QId PlcIdx Queue Name Enabled Rate Rate Drop(Bytes) Drop(Frames)
--------------------------------------------------------------------------------------------
14 13 Sw forwarding Yes 1000 200 0 0>>>>>>>>>>>>>>>>>>>>>>>>>>>>No increment
```

案例2.如果靜態路由指向Null0，則無MSS調整

如果只配置了Null0路由，則在IXIA生成的流量之後，SW轉發隊列中的丟棄計數器將如預期一樣保留為「0」。

請參閱以下日誌：

```
Cat-9400-1# Show platform hardware fed active qos queue stats internal cpu policer
CPU Queue Statistics
============================================================================================
(default) (set) Queue Queue
QId PlcIdx Queue Name Enabled Rate Rate Drop(Bytes) Drop(Frames)
--------------------------------------------------------------------------------------------
14 13 Sw forwarding Yes 1000 200 0 0>>>>>>>>>>>>>>>>>>>>>>>>>>>>No increment
```

案例3.啟用「Null0」和「MSS Adjust」

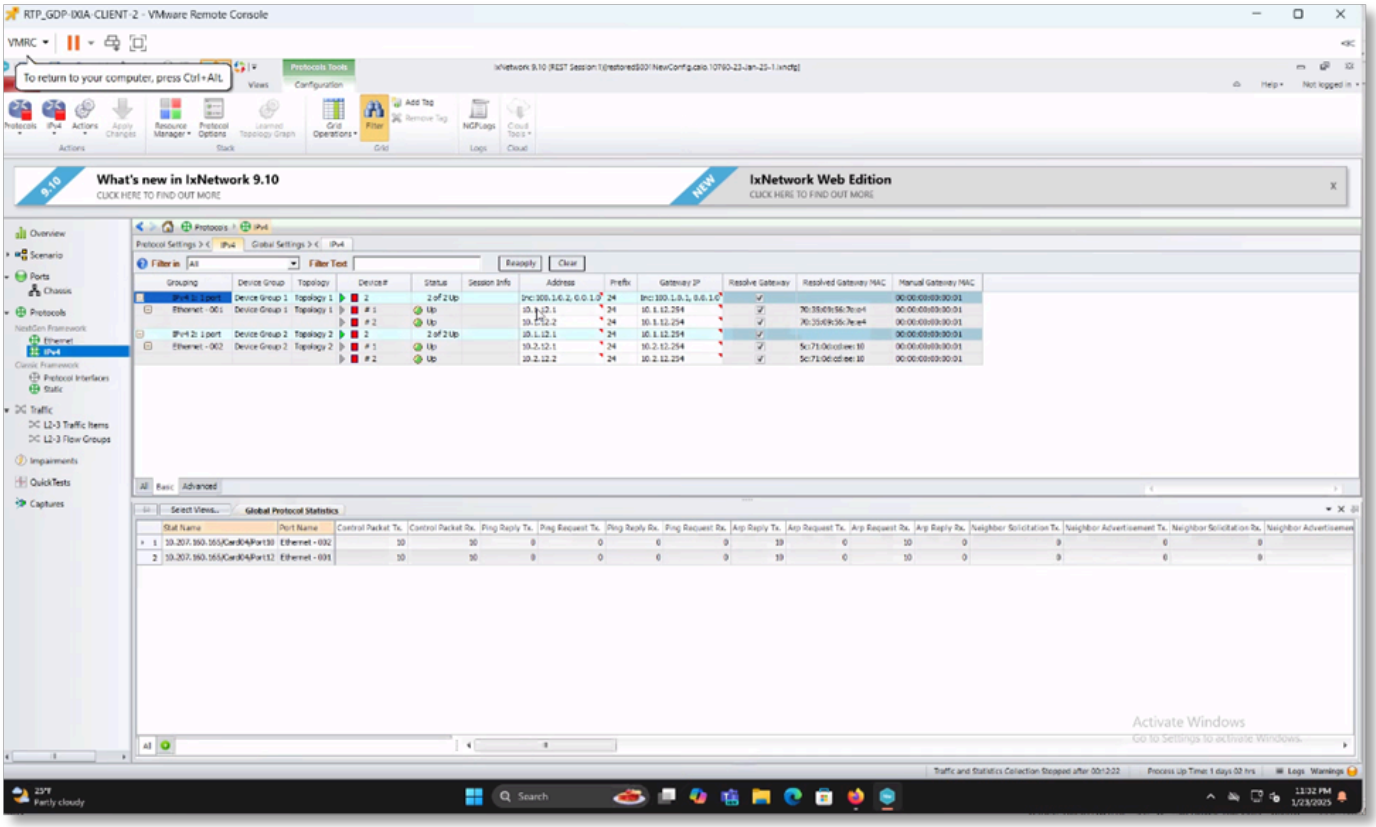
```
With both "ip tcp adjust-mss" and a "null route" configured:
```

```
Configuration:

On Cat 9300:
Cat-9300-1#show run interface twoGigabitEthernet 1/0/1
interface TwoGigabitEthernet1/0/1 (Interface connected to IXIA)
no switchport
ip address 10.1.12.xx 255.255.255.0
end
Cat-9300-1#show run interface tenGigabitEthernet 1/1/3
interface TenGigabitEthernet1/1/3 (Physical interface connected to C9400)
no switchport
mtu 9000
ip address 203.63.147.xx 255.255.255.0
no ip redirects
no ip unreachables
```

```
ip mtu 1500
load-interval 30
end

Cat-9300-1#show run interface tunnel421
interface Tunnel421
description Tunnel 421 to Scrubbing Center - SYD EDGE 1 and 2 - AR1 Tunnel 30
ip address 10.88.178.xx 255.255.255.0
ip mtu 1470
load-interval 30
Cisco Confidential
keepalive 10 3
tunnel source 203.63.147.xx
tunnel destination 203.63.147.xx
end

On cat 9400:
Cat-9400-1#show run interface tenGigabitEthernet 1/0/3
interface TenGigabitEthernet1/0/3 (Interface connected to C9300)
description CN,ISP,S1 AAPT, Superloop Circuit ID SID565199 - AAPT Circuit ID 5804194
no switchport
mtu 9000
ip address 203.63.147.xx 255.255.255.0
no ip redirects
no ip unreachables
ip mtu 1500
load-interval 30
end

interface Tunnel421
description Tunnel 421 to Scrubbing Center - SYD EDGE 1 and 2 - AR1 Tunnel 30
ip address 10.88.178.xx 255.255.255.0
ip mtu 1470
ip tcp adjust-mss 500>>>>>>>>>>>>
load-interval 30
keepalive 10 3
tunnel source 203.63.147.xx
tunnel destination 203.63.147.xx
end

Null0 Routes:
ip route 10.2.12.xx 255.255.255.255 null0>>>>>>>>Destination IP is of IXIA connected to 9300

Cat-9400-1#show ip route
Gateway of last resort is 203.63.147.xx to network 0.0.0.0
S* 0.0.0.0/0 [1/0] via 203.63.147.xx
10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
S 10.2.12.0/24 [1/0] via 192.168.12.xx
S 10.2.12.xx/32 is directly connected, Null0
C 10.88.178.0/24 is directly connected, Tunnel421
L 10.88.178.xx/32 is directly connected, Tunnel421
```

在C9400的輸入隧道介面上，Null0路由和MSS調整配置後，流量從IXIA生成，丟棄計數器增加CPU隊列標識(QID)14，如下圖所示。

IXIA



C9400 CoPP輸出：

```
Cat-9400-1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Cat-9400-1(config)#ip route 10.2.12.1 255.255.255.255 Null0
Cat-9400-1(config)#end
Cat-9400-1#
*Jan 23 16:03:00.697: %SYS-5-CONFIG_I: Configured from console by console
Cat-9400-1#$ hardware fed active qos queue stats internal cpu policer

                        CPU Queue Statistics
============================================================================================

                                                (default) (set)      Queue          Queue
QId PlcIdx  Queue Name                  Enabled   Rate      Rate     Drop(Bytes)    Drop(Frames)
--------------------------------------------------------------------------------------------

0     11    DOT1X Auth                  Yes       1000      1000     0              0
1     1     L2 Control                  Yes       2000      2000     0              0
2     14    Forus traffic               Yes       4000      4000     0              0
3     0     ICMP GEN                    Yes       600       600      0              0
4     2     Routing Control             Yes       5400      5400     0              0
5     14    Forus Address resolution    Yes       4000      4000     0              0
6     0     ICMP Redirect               Yes       600       600      0              0
7     16    Inter FED Traffic           Yes       2000      2000     0              0
8     4     L2 LVX Cont Pack            Yes       1000      1000     0              0
9     19    EWLC Control                Yes       13000     13000    0              0
10    16    EWLC Data                   Yes       2000      2000     0              0
11    13    L2 LVX Data Pack            Yes       1000      200      0              0
12    0     BROADCAST                   Yes       600       600      0              0
13    10    Openflow                    Yes       200       200      0              0
14    13    Sw forwarding               Yes       1000      200      55596020348    54936779
15    8     Topology Control            Yes       13000     13000    0              0
16    12    Proto Snooping              Yes       2000      2000     0              0
17    6     DHCP Snooping               Yes       400       400      0              0
18    13    Transit Traffic             Yes       1000      200      0              0
19    10    RPF Failed                  Yes       200       200      0              0
20    15    MCAST END STATION           Yes       2000      2000     0              0
21    13    LOGGING                     Yes       1000      200      0              0
22    7     Punt Webauth                Yes       1000      1000     0              0
23    18    High Rate App               Yes       13000     13000    0              0
24    10    Exception                   Yes       200       200      0              0
25    3     System Critical             Yes       1000      1000     0              0
26    10    NFL SAMPLED DATA            Yes       200       200      0              0
27    2     Low Latency                 Yes       5400      5400     0              0
28    10    EGR Exception               Yes       200       200      0              0
29    5     Stackwise Virtual OOB       Yes       8000      8000     0              0
30    9     MCAST Data                  Yes       400       400      0              0
31    3     Gold Pkt                    Yes       1000      1000     0              0
--More--
```

```
Cat-9400-1# show platform hardware fed active qos queue stats internal cpu policer
================================================================================
(default) (set) Queue Queue
QId PlcIdx Queue Name Enabled Rate Rate Drop(Bytes) Drop(Frames)
--------------------------------------------------------------------------------
14 13 Sw forwarding Yes 1000 200 3252568000 3214000>>>>>> Drops increasing in this Queue

Cat-9400-1# show platform hardware fed active qos queue stats internal cpu policer

                        CPU Queue Statistics

================================================================================

                                          (default) (set)     Queue        Queue

QId PlcIdx  Queue Name                Enabled   Rate     Rate      Drop(Bytes)  Drop(Frames)

--------------------------------------------------------------------------------

0    11     DOT1X Auth                  Yes     1000      1000     0            0

1    1      L2 Control                  Yes     2000      2000     0            0

2    14     Forus traffic               Yes     4000      4000     0            0

3    0      ICMP GEN                    Yes     600       600      0            0

4    2      Routing Control             Yes     5400      5400     0            0

5    14     Forus Address resolution    Yes     4000      4000     0            0

6    0      ICMP Redirect               Yes     600       600      0            0

7    16     Inter FED Traffic           Yes     2000      2000     0            0

8    4      L2 LVX Cont Pack            Yes     1000      1000     0            0

9    19     EWLC Control                Yes     13000     13000    0            0

10   16     EWLC Data                   Yes     2000      2000     0            0

11   13     L2 LVX Data Pack            Yes     1000      200      0            0

12   0      BROADCAST                   Yes     600       600      0            0

13   10     Openflow                    Yes     200       200      0            0

14   13     Sw forwarding               Yes     1000      200      40147794808 39671734>>>>>>With MSS a

15   8      Topology Control            Yes     13000     13000    0            0

16   12     Proto Snooping              Yes     2000      2000     0            0

17   6      DHCP Snooping               Yes     400       400      0            0
```

關於Null0靜態路由和MSS鉗位的說明

根據理論，為了處理不需要的流量（如廣播流量或阻止對特定子網的訪問），一個選項是設定靜態

路由，將流量定向到Null0。這將導致路由器丟棄要用於該網路的任何流量。

Null0命令

```
ip route <destination-network> <subnet-mask> null 0

For an example:

ip route 10.2.12.xx 255.255.255.255 null0>>>>>>Destination IP is of IXIA connected to 9300
```

Null 0語法確保不會將10.2.12.1/32轉發到任何位置。這意味著在Null0處丟棄所有目的地網路流量。

TCP MSS

另一方面，TCP MSS調整：

MSS調整會修改TCP封包的MSS。當發生MTU不相符時（通常發生在具有不同MTU設定的裝置之間或透過VPN等通道），封包可以分段。

TCP流量不需要分段，因為分段會導致封包遺失或效能下降。MSS鉗位通過調整TCP區段的大小來解決此問題，確保資料包足夠小，可以容納在路徑MTU中，從而防止分段。將MSS調整應用於隧道介面和SVI（對於TCP連線，其值設定為1360）時，可確保區段大小小於路徑MTU，從而防止分段。

理想情景

Null0是一個虛擬「黑洞」介面，它丟棄任何指向它的流量。防止路由環路或有害流量很有用。
TCP MSS adjust命令可確保TCP區段足夠小，以便在通過具有較小MTU的裝置或隧道時避免分段。

條件

雖然這兩個功能通常用於不同的用途，但是它們都可以在整體網路設計中發揮作用，以便管理流量、避免分段和最佳化效能。但是，在Catalyst 9K交換機上，同時使用Null0和MSS調整會導致衝突、使CPU過載並使CoPP策略不堪重負。

驗證

```
Show platform hardware fed active qos queue stats internal cpu policer
Identify the QID where the drop counters increments. After finding the QID (for example, QID 14), run t
#debug platform software fed switch active punt packet-capture set-filter "fed.queue == 14"
#debug platform software fed switch active punt packet-capture start
#debug platform software fed switch active punt packet-capture stop
#show platform software fed switch active punt packet-capture brief
```

```
#show platform software fed switch active punt packet-capture detailed
```

使用debug命令檢查下一個格式的日誌，以識別攻擊者在CPU上傳送的IP地址，即使已配置Null0路由：

```
------ Punt Packet Number: XX, Timestamp: 2024/12/14 12:54:57.508 ------
interface : physical: [if-id: 0x00000000], pal: Tunnel411 [if-id: 0x000000d2]
metadata : cause: 11 [For-us data], sub-cause: 1, q-no: 14, linktype: MCP_LINK_TYPE_IP [1]
ether hdr : Partial ether header, ethertype: 0x0800 (IPv4)
Cisco Confidential
ipv4 hdr : dest ip: XX.XX.XX.XX, src ip: XX.XX.XX.XX
ipv4 hdr : packet len: 44, ttl: 242, protocol: 6 (TCP)
tcp hdr : dest port: 777, src port: 41724
```

偵錯

```
Cat-9400-1# debug platform software fed active punt packet-capture set-filter "fed.queue == 14"
Filter setup successful. Captured packets will be cleared

Cat-9400-1#debug platform software fed active punt packet-capture start
Punt packet capturing started.

Cat-9400-1#debug platform software fed active punt packet-capture stop
Punt packet capturing stopped. Captured 4096 packet(s)

Cat-9400-1#show platform software fed active punt packet-capture brief
Total captured so far: 4096 packets. Capture capacity : 4096 packets
Capture filter : "fed.queue == 14"
------ Punt Packet Number: 1, Timestamp: 2025/01/23 16:16:54.978 ------
interface : physical: [if-id: 0x00000000], pal: Tunnel421 [if-id: 0x0000002e]
metadata : cause: 11 [For-us data], sub-cause: 1, q-no: 14, linktype: MCP_LINK_TYPE_IP [1]
ether hdr : Partial ether header, ethertype: 0x0800 (IPv4)
ipv4 hdr : dest ip: 10.2.12.xx, src ip: 10.1.12.xx >>>10.2.12.xx is IXIA
ipv4 hdr : packet len: 1006, ttl: 63, protocol: 6 (TCP)
tcp hdr : dest port: 60, src port: 60
------ Punt Packet Number: 2, Timestamp: 2025/01/23 16:16:54.978 ------
interface : physical: [if-id: 0x00000000], pal: Tunnel421 [if-id: 0x0000002e]
metadata : cause: 11 [For-us data], sub-cause: 1, q-no: 14, linktype: MCP_LINK_TYPE_IP [1]
ether hdr : Partial ether header, ethertype: 0x0800 (IPv4)
ipv4 hdr : dest ip: 10.2.12.xx, src ip: 10.1.12.xx >>>10.2.12.xx is IXIA
ipv4 hdr : packet len: 1006, ttl: 63, protocol: 6 (TCP)
tcp hdr : dest port: 60, src port: 60
------ Punt Packet Number: 3, Timestamp: 2025/01/23 16:16:54.978 ------
interface : physical: [if-id: 0x00000000], pal: Tunnel421 [if-id: 0x0000002e]
metadata : cause: 11 [For-us data], sub-cause: 1, q-no: 14, linktype: MCP_LINK_TYPE_IP [1]
ether hdr : Partial ether header, ethertype: 0x0800 (IPv4)
ipv4 hdr : dest ip: 10.2.12.xx, src ip: 10.1.12.xx >>>10.2.12.xx is IXIA
Cisco Confidential
ipv4 hdr : packet len: 1006, ttl: 63, protocol: 6 (TCP)
tcp hdr : dest port: 60, src port: 60
```

結論

為了防止CPU隊列被不需要的流量淹沒，並影響TCP/安全外殼(SSH)通訊，請在這些IP地址到達Catalyst 9K交換機之前阻止它們，或者刪除入口上的MSS調整。

通常，TCP同步(SYN)封包會傳送到CPU佇列。TCP標頭中的MSS選項表示除了TCP/IP標頭外，接收者可以接受的最大區段大小。它通常設定為三次握手，具體是在SYN資料包中。

為了解決此問題，請對RADWARE/安全網關上的惡意IP進行地理阻塞，以防止CPU策略器隊列變得不堪重負，並穩定BGP對等和TCP連線。

解析

在Radware/安全網關上成功阻止惡意IP後，流量停止並會超過CPU隊列。

相關資訊

- https://www.cisco.com/c/en/us/support/docs/ip/transmission-control-protocol-tcp/222338-troubleshoot-tcp-slowness-issues-due-to.html
- 思科技術支援與下載

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。