MPTCP和產品支援概述

目錄

[簡介](#)
[MPTCP概述](#)
[背景資訊](#)
[會話建立](#)
[加入其他子流](#)
[新增地址](#)
[分段、多路徑和重組](#)
[對流量檢測的影響](#)
[受MPTCP影響的思科產品](#)
[ASA](#)
[TCP操作](#)
[通訊協定檢查](#)
[Cisco Firepower威脅防禦](#)
[TCP操作](#)
[Cisco IOS 防火牆](#)
[內容型存取控制(CBAC)](#)
[區域型防火牆(ZBFW)](#)
[ACE](#)
[不受MPTCP影響的思科產品](#)

簡介

本檔案將提供多路徑TCP(MPTCP)的概覽、其對流量檢查的影響以及受多路徑TCP影響和不受多路徑TCP影響的思科產品。

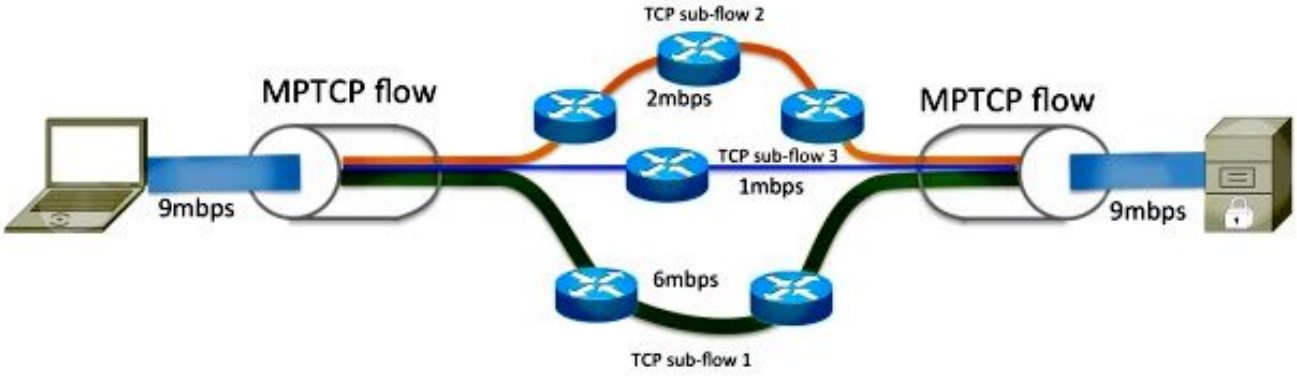
MPTCP概述

背景資訊

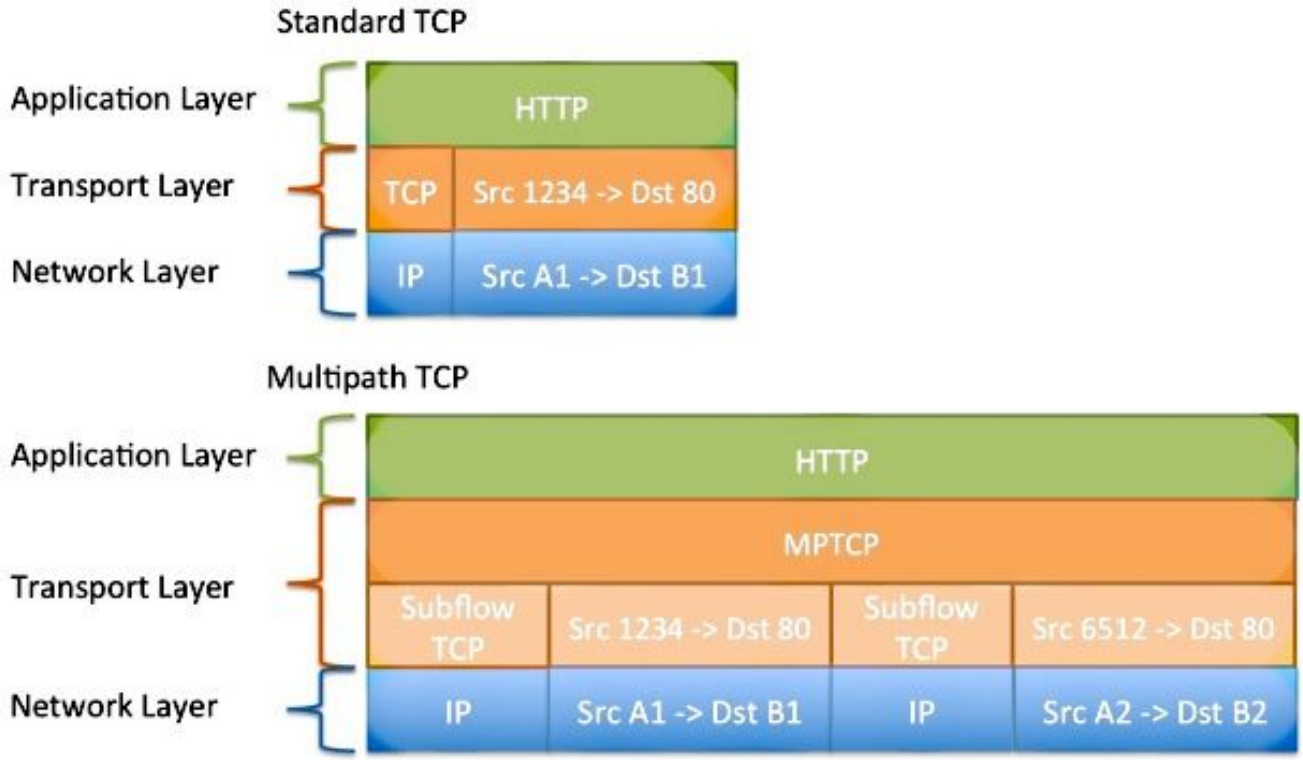
連線到Internet或資料中心環境內的主機通常通過多個路徑連線。但是，當使用TCP進行資料傳輸時，通訊將限於一條網路路徑。兩個主機之間的某些路徑可能會擁塞，但備用路徑未得到充分利用。如果同時使用這些多個路徑，則可能會更有效地使用網路資源。此外，多連線的使用增強了使用者體驗，因為它提供了更高的吞吐量並提高了對網路故障的可復原性。

MPTCP是對常規TCP進行的一組擴展，它允許單個資料流在多個連線上分離和傳輸。請參閱[RFC6824:如需詳細資訊，請參閱使用多個位址的多路徑操](#)作的TCP擴充模組。

如圖所示，MPTCP能夠在傳送方節點上將9mbps流分成三個不同的子流，然後將其聚合回接收節點上的原始資料流。



進入MPTCP連線的資料的作用與通過常規TCP連線時完全相同；所傳輸的資料保證按序傳送。由於MPTCP可調整網路堆疊並在傳輸層內運行，因此應用可透明使用該協定。

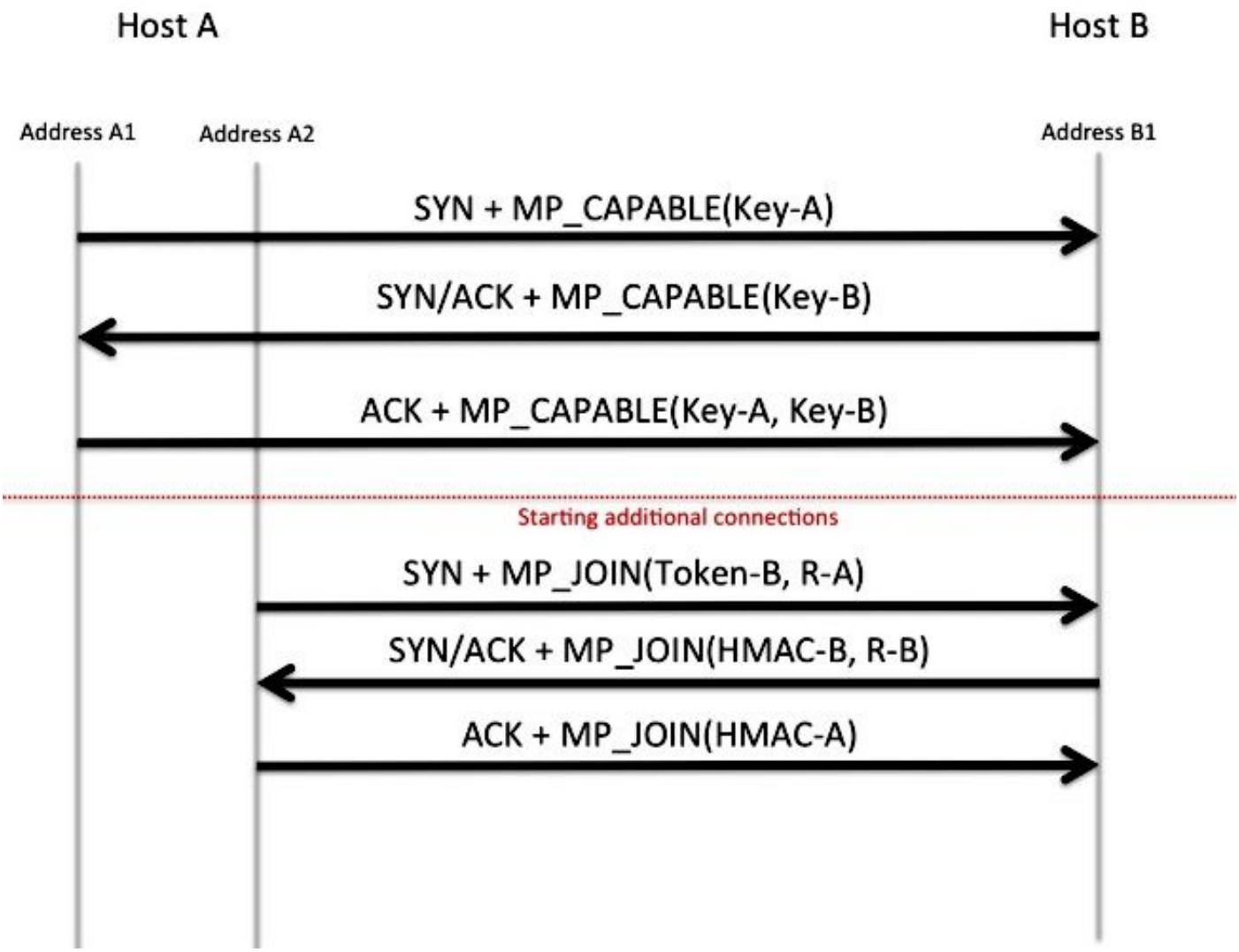


會話建立

MPTCP使用TCP選項來協商和協調多個子流上資料的分離和重組。**TCP選項30**由Internet編號指派機構(IANA)保留，供MPTCP獨佔使用。如需詳細資訊，請參閱傳輸控制通訊協定(TCP)引數。在建立常規TCP作業階段時，初始同步(SYN)封包中包含一個**MP_CAPABLE**選項。如果回應者支援並選擇交涉MPTCP，它也會使用SYN-acknowledge(ACK)封包中的**MP_CAPABLE**選項進行回應。在此握手過程中交換的金鑰將在未來使用，以驗證將其他TCP會話加入和刪除到此MPTCP流的過程。

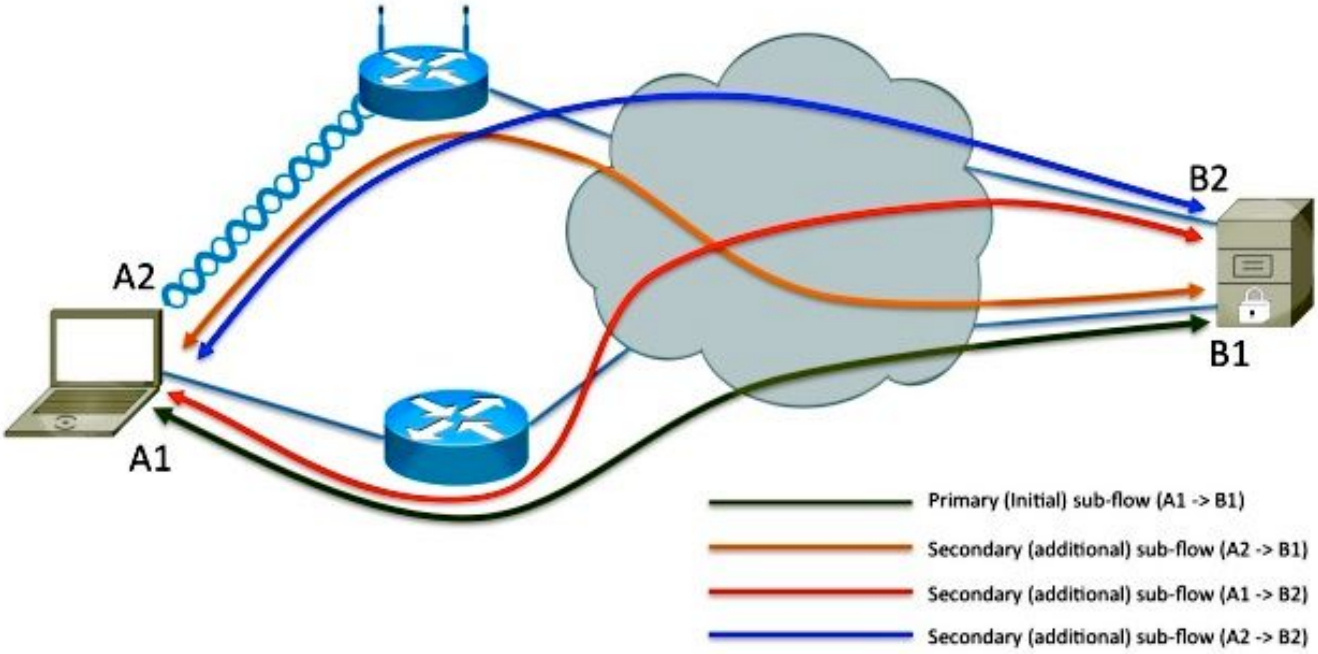
加入其他子流

在必要時，**主機A可**能會啟動從不同介面或位址到主機B的額外**子流**量。與初始子流一樣，使用TCP選項來表示希望將該子流與其他子流合併。**Host-B**使用在初始子流建立中交換的金鑰（連同雜湊演算法），以確認連線請求確實由**Host-A傳送**。次要子流4元組（源IP、目標IP、源埠和目標埠）與主要子流的不同；此流量可能採用不同的網路路徑。



新增地址

主機A有多個介面，而主機B可**能有多**個網路連線。**主機B從每個目的地為B1的地址Host-A來源子流隱式地獲知地址A1和A2。主機B可能將其附加地址(B2)通告給主機A，以便向B2生成其他子流。這通過TCP選項30完成。如下圖所示，Host-B將輔助地址(B2)通告給**Host-A，並建立兩個附加子流。因為MPTCP在開放系統互聯(OSI)堆疊的網路層上運行，所以通告的IP地址可以是IPv4、IPv6或同時是IPv4、IPv6地址。某些子流可以通過IPv4同時傳輸，而其他子流可以通過IPv6傳輸。



分段、多路徑和重組

由應用程式提供給MPTCP的資料流必須由傳送方分段並在多個子流之間分佈。然後，必須將其重組為單個資料流，然後才能將其傳遞回應用程式。

MPTCP檢查每個子流的效能和延遲，並動態調整資料分佈以獲得最高聚合吞吐量。在資料傳輸過程中，TCP報頭選項包括有關MPTCP序列/確認號、當前子流序列/確認號以及校驗和的資訊。

對流量檢測的影響

許多安全裝置可能會將未知的TCP選項清零或替換為No Option(NOOP)值。如果網路裝置對初始子流上的TCP SYN資料包執行此操作，**MP_CAPABLE通告**將被刪除。因此，伺服器認為使用者端不支援MPTCP，它會回覆為正常的TCP作業。

如果保留了此選項，並且MPTCP能夠建立多個子流，則網路裝置進行的線上資料包分析可能無法可靠地運行。這是因為只有部分資料流被轉移到每個子流。協定檢查對MPTCP的影響可能各不相同，從無到完全中斷服務。效果因檢查的資料內容和數量而異。封包分析可能包括防火牆應用層閘道（ALG或fixup）、網路位址轉譯(NAT)ALG、應用可見性與控制(AVC)、網路型應用程式辨識(NBAR)或入侵偵測服務(IDS/IPS)。 如果您的環境中需要應用檢測，建議啟用清除**TCP選項**30。

如果由於加密而無法檢查流，或者協定未知，則內聯裝置應該對MPTCP流沒有影響。

受MPTCP影響的思科產品

以下產品受MPTCP影響：

- 調適型安全裝置(ASA)
- Cisco Firepower威脅防禦
- 入侵防禦系統(IPS)
- Cisco IOS-XE和IOS®

- 應用程式控制引擎(ACE)

本文檔後面的部分將詳細介紹每個產品。

ASA

TCP操作

預設情況下，Cisco ASA防火牆將不受支援的TCP選項(包括**MPTCP選項30**)替換為NOOP選項（選項1）。 若要允許MPTCP選項，請使用以下設定：

1. 定義策略以允許**TCP選項30**（由MPTCP使用）通過裝置：

```
tcp-map my-mptcp
   tcp-options range 30 30 allow
```

2. 定義流量選擇：

```
class-map my-tcpnorm
   match any
```

3. 定義從流量到操作的對映：

```
policy-map my-policy-map
   class my-tcpnorm
       set connection advanced-options my-mptcp
```

4. 在機箱或每個介面上啟用它：

```
service-policy my-policy-map global
```

通訊協定檢查

ASA支援對多種協定進行檢查。檢查引擎可能對應用程式產生的影響各不相同。如果需要檢查，建議不要應用前面所述的TCP對映。

Cisco Firepower威脅防禦

TCP操作

由於FTD對IPS/IDS服務執行深入封包檢查，因此建議不要修改tcp對應以允許TCP選項通過。

Cisco IOS 防火牆

內容型存取控制(CBAC)

CBAC不會從TCP資料流中刪除TCP選項。MPTCP通過防火牆建立連線。

區域型防火牆(ZBFW)

Cisco IOS和IOS-XE ZBFW不會從TCP資料流中刪除TCP選項。MPTCP通過防火牆建立連線。

ACE

預設情況下，ACE裝置會從TCP連線中刪除TCP選項。MPTCP連線回退到常規TCP操作。

可以通過**tcp-options** 命令將ACE裝置配置為允許TCP選項，如Cisco ACE應用控制引擎Security Guide vA5(1.0)的配置ACE處理TCP選項部分所述。但是，並非總是建議這樣做，因為輔助子流可能均衡到不同的實際伺服器，因此連線失敗。

不受MPTCP影響的思科產品

通常，不檢查TCP流或第7層資訊的任何裝置也不會改變TCP選項，因此對MPTCP應該是透明的。這些裝置可能包括：

- Cisco 5000系列ASR(Starent)
- 廣域應用程式服務(WAAS)
- 電信級服務網路(CGN)(電信級服務引擎(CGSE)刀鋒(在電信級路由系統(CRS)-1)
- 所有乙太網路交換器產品
- 所有路由器產品(除非啟用防火牆或NAT功能；如需詳細資訊，請參閱檔案前面的受MPTCP影響的思科產品一節)