MPTCP和产品支持概述

目录

简介

本文档概述了多路径TCP(MPTCP)、其对流量检测的影响，以及受其影响和不受其影响的思科产品。

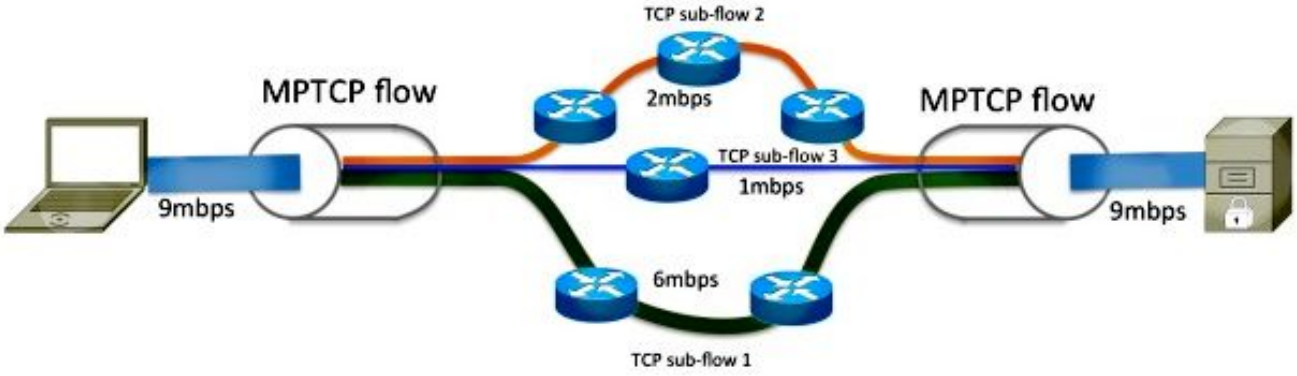
MPTCP概述

背景信息

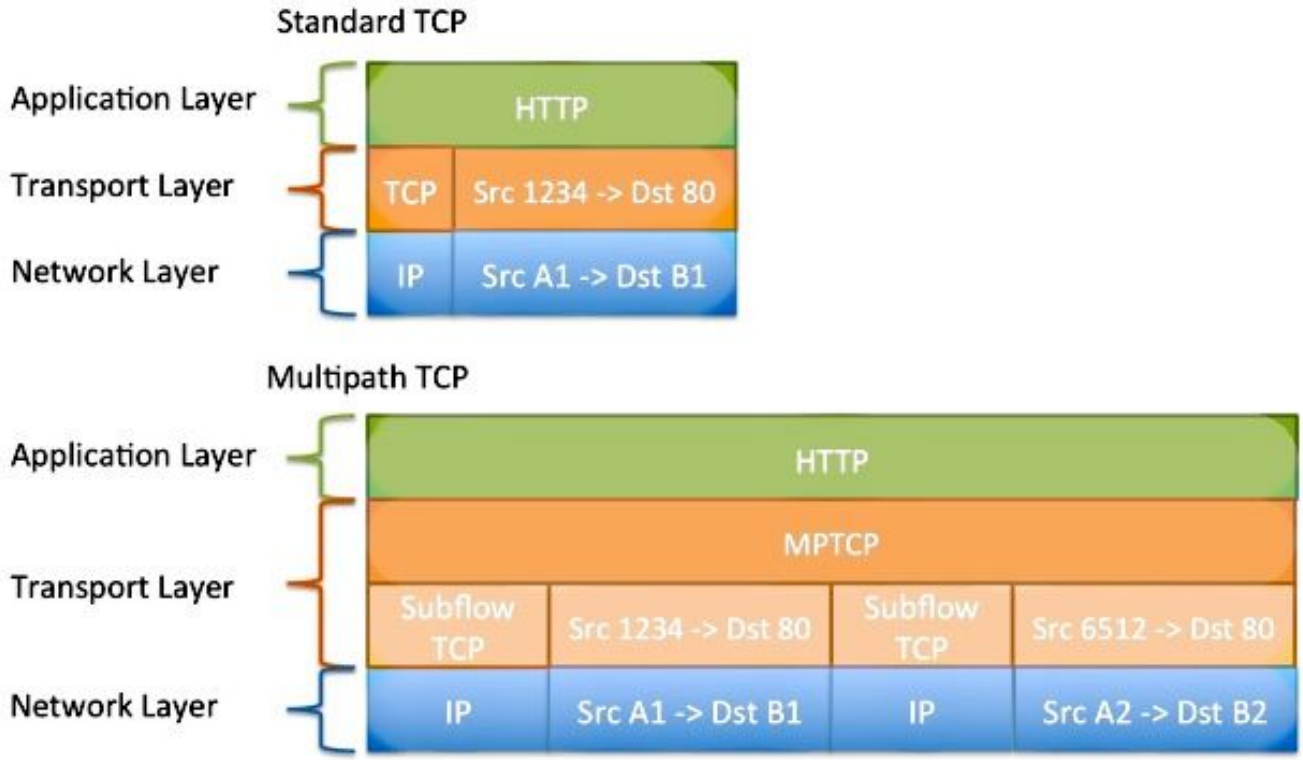
连接到互联网或数据中心环境中的主机通常通过多条路径连接。但是，当TCP用于数据传输时，通信仅限于单个网络路径。两台主机之间的某些路径可能拥塞，而备用路径则未充分利用。如果同时使用这些多条路径，则可以更有效地使用网络资源。此外，使用多个连接可增强用户体验，因为它提供更高的吞吐量和更强的网络故障恢复能力。

MPTCP是对常规TCP的一组扩展，它使单个数据流能够分离并跨多个连接传输。请参阅[RFC6824:多路径操作的TCP扩展（带多个地址）](#)以了解详细信息。

如下图所示，MPTCP能够将9mbps流分离到发送方节点上的三个不同的子流中，这些子流随后汇聚回接收节点上的原始数据流。



进入MPTCP连接的数据与通过常规TCP连接的数据完全一样；传输的数据保证了按顺序传送。由于MPTCP调整网络堆栈并在传输层内运行，因此应用会透明地使用它。

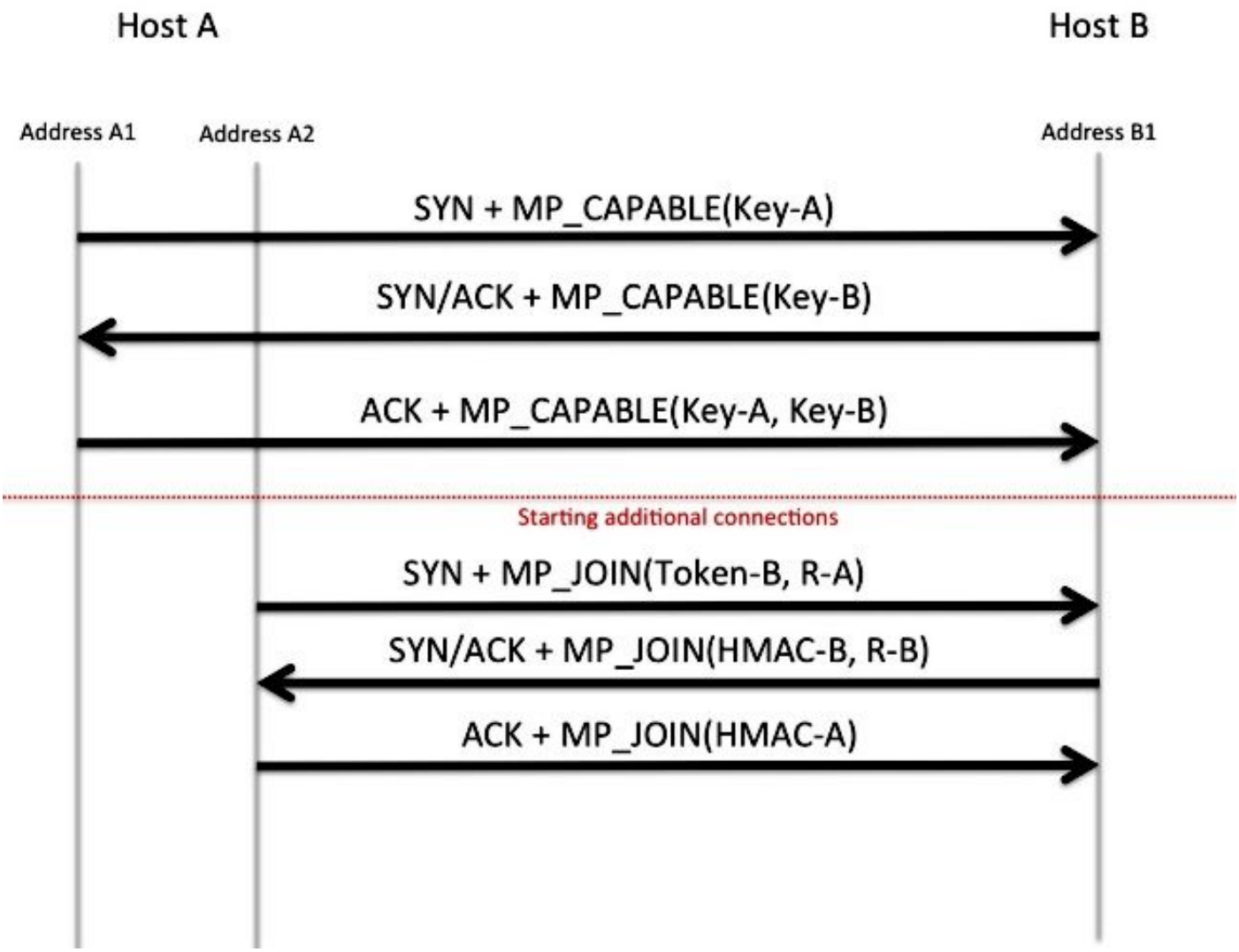


会话建立

MPTCP使用TCP选项来协商和协调多个子流上数据的分离和重组。**TCP选项30**由Internet编号指派机构(IANA)保留，供MPTCP专用。有关详细信息，请参阅传输控制协议(TCP)参数。在建立常规TCP会话时，初始同**步(SYN)**数据包中会包含MP_CAPABLE选项。如果响应方支持并选择协商MPTCP，它还会使用SYN-acknowledge(ACK)数据包中的**MP_CAPABLE**选项做出响应。在此握手中交换的密钥将来用于验证其他TCP会话加入和删除到此MPTCP流中的身份。

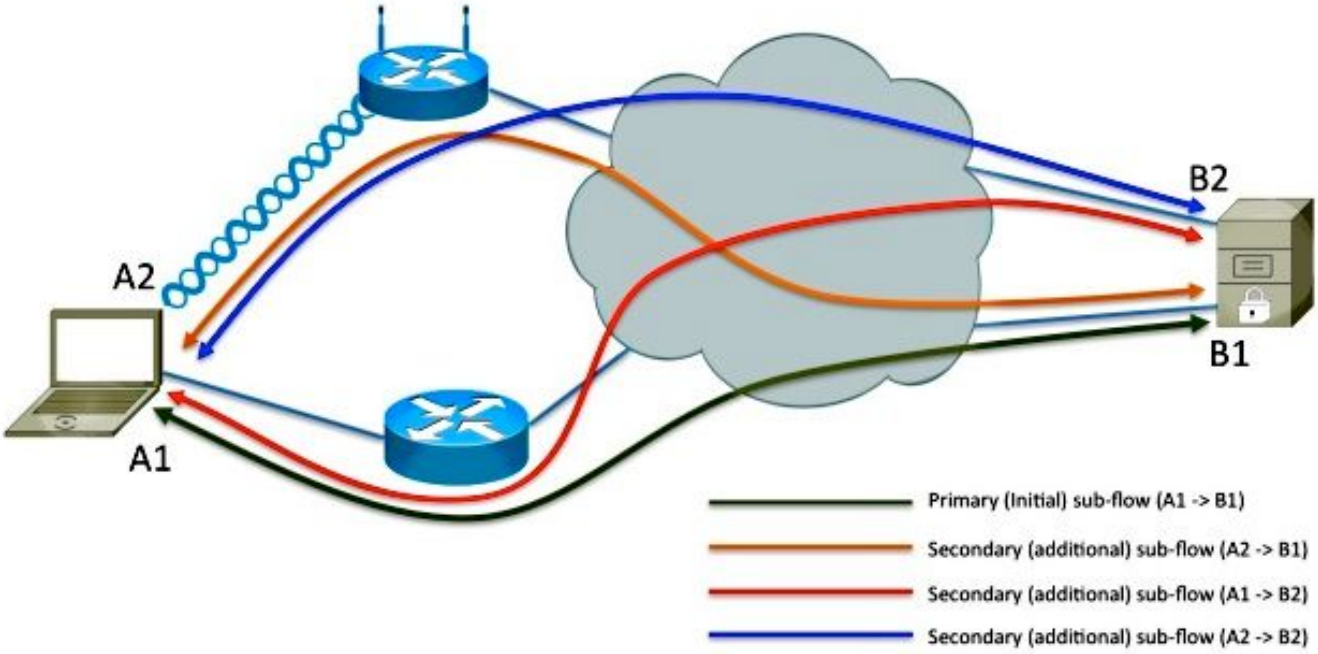
加入其他子流

如果认为必要，**主机A**可能会启动来自不同接口或地址到主机B的其**他子流**。与初始子流一样，使用TCP选项来表示希望将此子流与其他子流合并。主机B使用在初始子流建立内交换的密钥（以及散列算法），**以确**认加入请求确实由主机A**发送**。辅助子流4元组（源IP、目的IP、源端口和目的端口）与主子流不同；此流可能在网络中采用不同的路径。



添加地址

主机A有多个接口，并且主机B**可能有**多个网络连接。**主机B从发往B1的每个地址中获取子流，从而隐式获取地址A1和A2。主机B可能向主机A通告其附加地址(B2)，以便向B2发送其他子流。这通过TCP选项3完成0**.如下图所**示，主机**B将其辅助地址(B2)通告给主机A，并创建两个附加子流。由于MPTCP在开放式系统互联(OSI)堆栈的网络层上运行，因此通告的IP地址可以是IPv4、IPv6或两者。某些子流可能由IPv4同时传输，而其他子流则由IPv6传输。



分段、多路径和重组

应用给MPTCP的数据流必须由发送方在多个子流之间分段和分配。然后，必须将其重新组装到单个数据流中，然后再将其传回应用。

MPTCP检查每个子流的性能和延迟，并动态调整数据分布以获得最高的聚合吞吐量。在数据传输过程中，TCP报头选项包括有关MPTCP序列/确认号、当前子流序列/确认号和校验和的信息。

对流量检测的影响

许多安全设备可能会使用No Option(NOOP)值零出或替换未知TCP选项。如果网络设备对初始子流上的TCP SYN数据包执行此操作，则**MP_CAPABLE通**告将被删除。因此，对服务器来说，客户端不支持MPTCP，并恢复为正常的TCP操作。

如果保留了该选项，并且MPTCP能够建立多个子流，则网络设备的串行数据包分析可能无法可靠运行。这是因为只有部分数据流被传输到每个子流。协议检查对MPTCP的影响可能从无到完全中断服务。其影响因检测的数据和数量而异。数据包分析可能包括防火墙应用层网关（ALG或修正）、网络地址转换(NAT)ALG、应用可视性与可控性(AVC)、基于网络的应用识别(NBAR)或入侵检测服务(IDS/IPS)。 如果您的环境中需要应用检查，建议启用清**除TCP选项**30。

如果由于加密而无法检查流或协议未知，则内联设备对MPTCP流应不会产生影响。

受MPTCP影响的思科产品

以下产品受MPTCP影响：

- 自适应安全设备(ASA)
- 思科Firepower威胁防御
- 入侵防御系统 (IPS)
- Cisco IOS-XE和IOS®

- 应用程序控制引擎 (ACE)

本文档的后续部分将详细介绍每种产品。

ASA

TCP操作

默认情况下，Cisco ASA防火墙将不受支持的TCP选项(包括**MPTCP选项30)**替换为NOOP选项（选项1）。 要允许MPTCP选项，请使用以下配置：

1. 定义策略以允许TCP选**项30(**由MPTCP使用)通过设备：

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

2. 定义流量选择：

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

3. 定义从流量到操作的映射：

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

4. 在设备或每个接口上激活它：

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

协议检查

ASA支持检查许多协议。检查引擎可能对应用的影响会有所不同。如果需要检查，建议不应用之前描述的TCP映射。

思科Firepower威胁防御

TCP操作

当FTD对IPS/IDS服务执行深度数据包检测时，建议不要修改tcp-map以允许TCP选项通过。

Cisco IOS 防火墙

基于情景的访问控制(CBAC)

CBAC不会从TCP数据流中删除TCP选项。MPTCP通过防火墙建立连接。

基于区域的防火墙(ZBFW)

Cisco IOS和IOS-XE ZBFW不会从TCP数据流中删除TCP选项。MPTCP通过防火墙建立连接。

ACE

默认情况下，ACE设备从TCP连接中删除TCP选项。MPTCP连接回退到常规TCP操作。

ACE设备可以配置为通过**tcp-options**命令允许TCP选项，如Cisco ACE应用控制引擎安全指南vA5(1.0)的配置ACE如何处理TCP选项部分所述。但是，并不总是建议这样做，因为辅助子流可能会平衡到不同的实际服务器，而且连接失败。

不受MPTCP影响的思科产品

通常，任何不检查TCP流或第7层信息的设备也不会更改TCP选项，因此应对MPTCP透明。这些设备可能包括：

- Cisco 5000系列ASR(Starent)
- 广域应用服务（WAAS）
- 运营商级NAT(CGN)(运营商级路由系统(CRS)-1中的运营商级服务引擎(CGSE)刀片)
- 所有以太网交换机产品
- 所有路由器产品(除非启用防火墙或NAT功能；有关更多详细信息，请参阅文档前面的“受MPTCP影响的思科产品”部分)