Descripción general de MPTCP y soporte de productos

Contenido

Introducción

Este documento proporciona una descripción general de TCP de ruta múltiple (MPTCP), su impacto en la inspección de flujo y los productos de Cisco que se ven afectados y no lo son.

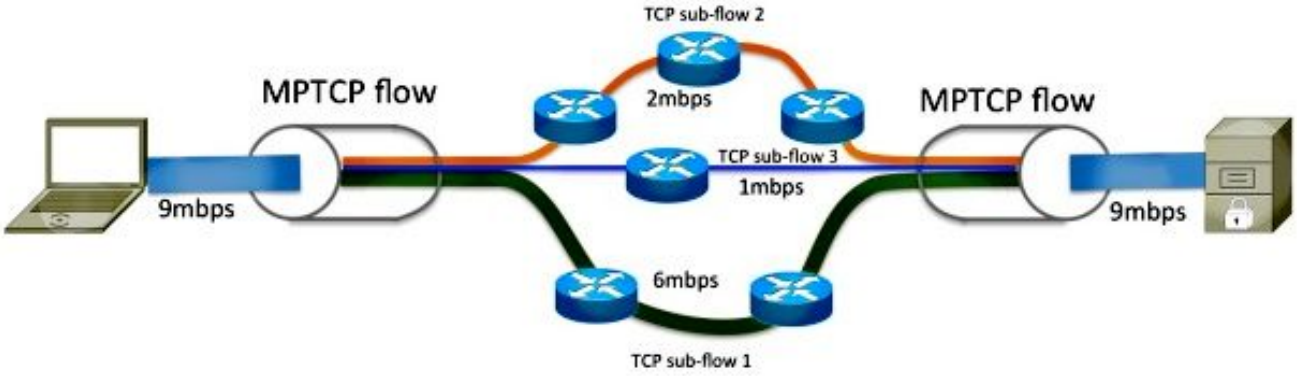
Descripción General de MPTCP

Antecedentes

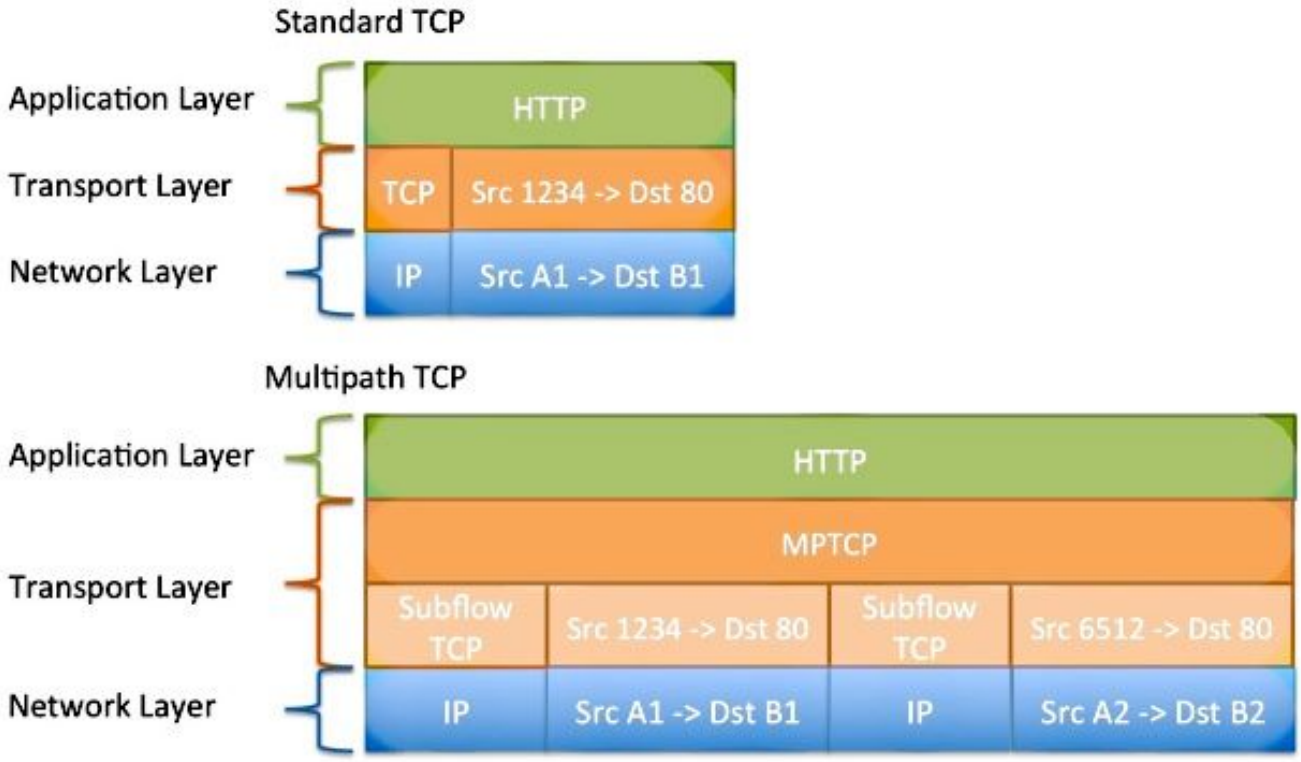
Los hosts conectados a Internet o dentro de un entorno de Data Center suelen estar conectados por varias rutas. Sin embargo, cuando se utiliza TCP para el transporte de datos, la comunicación se restringe a una única ruta de red. Es posible que algunas trayectorias entre los dos hosts estén congestionadas, mientras que las trayectorias alternativas están infrautilizadas. Es posible un uso más eficiente de los recursos de red si se utilizan simultáneamente estas varias rutas. Además, el uso de varias conexiones mejora la experiencia del usuario, ya que proporciona un mayor rendimiento y una resistencia mejorada frente a los fallos de la red.

MPTCP es un conjunto de extensiones a TCP normal que permite separar un flujo de datos único y transportarlo a través de varias conexiones. Consulte RFC6824: Extensiones TCP para Operación de Trayectoria Múltiple con Direcciones Múltiples para obtener más información.

Como se muestra en este diagrama, MPTCP puede separar el flujo de 9 mbps en tres subflujos diferentes en el nodo del remitente, que luego se agrega de nuevo al flujo de datos original en el nodo receptor.



Los datos que ingresan a la conexión MPTCP actúan exactamente como lo hace a través de una conexión TCP regular; los datos transmitidos han garantizado una entrega en orden. Dado que MPTCP ajusta la pila de red y funciona dentro de la capa de transporte, la aplicación la utiliza de forma transparente.



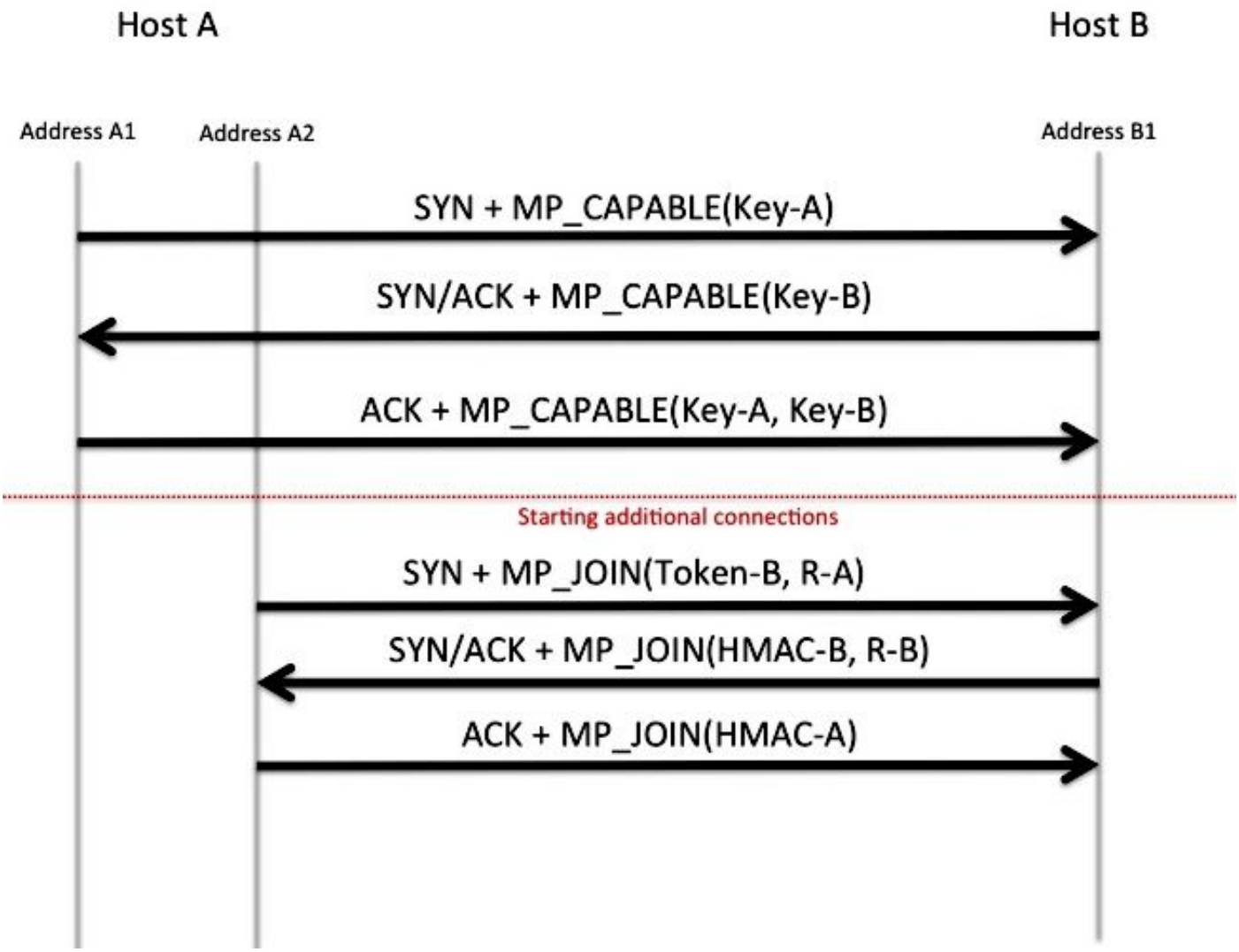
Establecimiento de sesión

MPTCP utiliza las opciones TCP para negociar y orquestar la separación y el reensamblado de datos sobre los subflujos múltiples. La **opción 30 de TCP** está reservada por la Autoridad de Números Asignados de Internet (IANA) para uso exclusivo de MPTCP. Consulte Parámetros de protocolo de control de transmisión (TCP) para obtener más información. En el establecimiento de una sesión TCP regular, se incluye una opción **MP_CAPABLE** en el paquete de sincronización inicial (SYN). Si el respondedor admite y elige negociar MPTCP, también responde con la opción **MP_CAPABLE** en el paquete SYN-confirm (ACK). Las claves intercambiadas dentro de este

intercambio de señales se utilizan en el futuro para autenticar la unión y la eliminación de otras sesiones TCP en este flujo MPTCP.

Incorporación de subflujos adicionales

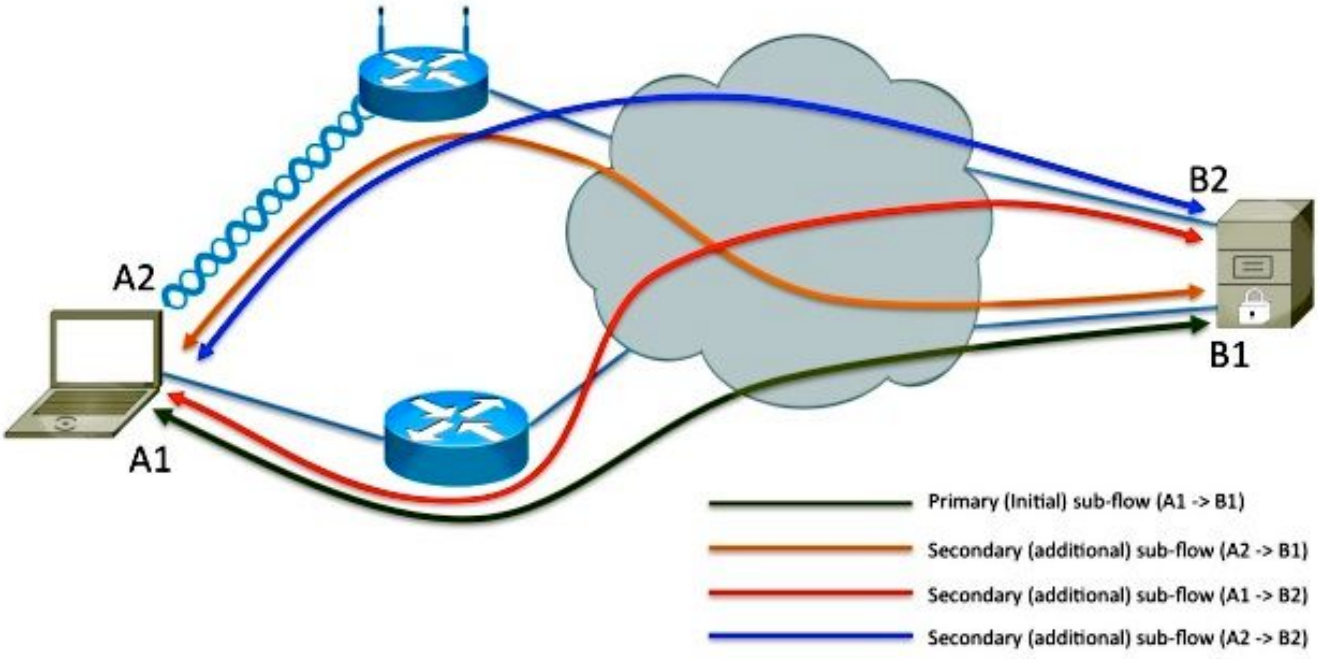
Cuando se considere necesario, **Host-A** podría iniciar subflujos adicionales originados en una interfaz o dirección diferente al **Host-B**. Al igual que con el subflujo inicial, las opciones TCP se utilizan para indicar el deseo de fusionar este subflujo con el otro subflujo. El **Host-B** utiliza las claves que se intercambian dentro del establecimiento inicial de subflujo (junto con un algoritmo de hashing) para confirmar que la solicitud de unión es efectivamente enviada por el **Host-A**. El subflujo secundario de 4 tuplas (IP de origen, IP de destino, puerto de origen y puerto de destino) es diferente del subflujo principal; este flujo puede tomar un trayecto diferente a través de la red.



Agregar dirección

Host-A tiene varias interfaces y es posible que **Host-B** tenga varias conexiones de red. **El Host B** aprende implícitamente sobre las direcciones A1 y A2 como resultado de los subflujos de **suministro del Host A** desde cada una de sus direcciones destinadas a B1. Es posible que **Host-B** anuncie su dirección adicional (B2) al **Host-A** para que otros subflujos se hagan a B2. Esto se completa a través de la **opción TCP 30**. Como se muestra en este diagrama, **Host-B** anuncia su dirección secundaria (B2) al **Host-A**, y se crean dos subflujos adicionales. Dado que MPTCP funciona sobre la capa de red de la pila de interconexión de sistema abierto (OSI), las direcciones IP anunciadas pueden ser IPv4, IPv6 o ambas. Es posible que algunos de los subflujos sean

transportados por IPv4 simultáneamente, ya que otros subflujos son transportados por IPv6.



Segmentación, múltiples rutas y reensamblado

El remitente debe segmentar y distribuir un flujo de datos que la aplicación ha dado a MPTCP entre los subflujos múltiples. A continuación, se debe volver a ensamblar en el flujo de datos único antes de que se devuelva a la aplicación.

MPTCP inspecciona el rendimiento y la latencia de cada subflujo y ajusta dinámicamente la distribución de los datos para obtener el máximo rendimiento agregado. Durante la transferencia de datos, la opción de encabezado TCP incluye información sobre los números de secuencia/reconocimiento MPTCP, el número de secuencia/reconocimiento de flujo secundario actual y una suma de comprobación.

Impacto en la inspección del flujo

Muchos dispositivos de seguridad podrían poner en cero o sustituir las opciones TCP desconocidas por un valor de opción sin opción (NOOP). Si el dispositivo de red hace esto al paquete TCP SYN en el subflujo inicial, el anuncio **MP_CAPABLE** se elimina. Como resultado, el servidor considera que el cliente no admite MPTCP y vuelve a la operación TCP normal.

Si se conserva la opción y MPTCP puede establecer varios subflujos, es posible que el análisis de paquetes en línea por los dispositivos de red no funcione de forma fiable. Esto se debe a que sólo se trasladan partes del flujo de datos a cada subflujo. El efecto de la inspección de protocolo en MPTCP puede variar de nada a la interrupción completa del servicio. El efecto varía en función de qué datos se inspeccionan y de la cantidad de datos que se inspeccionan. El análisis de paquetes puede incluir firewall Application Layer Gateway (ALG o fixup), traducción de direcciones de red (NAT) ALG, visibilidad y control de aplicaciones (AVC), reconocimiento de aplicaciones basadas en red (NBAR) o servicios de detección de intrusiones (IDS/IPS). Si se requiere la inspección de la aplicación en su entorno, se recomienda que la limpieza de la **opción TCP 30** esté habilitada.

Si el flujo no se puede inspeccionar debido al cifrado o si el protocolo es desconocido, entonces el

dispositivo en línea no debería tener impacto en el flujo MPTCP.

Productos de Cisco afectados por MPTCP

MPTCP afecta a estos productos:

- Dispositivo de seguridad adaptable (ASA)
- Defensa frente a amenazas Cisco Firepower
- Sistema de prevención de intrusiones (IPS)
- Cisco IOS-XE e IOS®
- Application Control Engine (ACE)

Cada producto se describe en detalle en las secciones posteriores de este documento.

ASA

Operaciones TCP

De forma predeterminada, el firewall Cisco ASA reemplaza las opciones TCP no admitidas, que incluyen la **opción MPTCP 30**, por la opción NOOP (opción 1). Para permitir la opción MPTCP, utilice esta configuración:

1. Defina la política para permitir la **opción TCP 30** (utilizada por MPTCP) a través del dispositivo:

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

2. Defina la selección de tráfico:

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

3. Definir un mapa del tráfico a la acción:

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

4. Actívelo en la caja o por interfaz:

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

Inspección de protocolo

El ASA admite la inspección de muchos protocolos. El efecto que el motor de inspección puede tener en la aplicación varía. Se recomienda que, si se requiere inspección, NO se aplique el mapa TCP descrito anteriormente.

Defensa frente a amenazas Cisco Firepower

Operaciones TCP

Dado que el FTD realiza una inspección profunda de paquetes para los servicios IPS/IDS, no se recomienda modificar el tcp-map para permitir que pase la opción TCP.

Cisco IOS Firewall

Control de acceso basado en contexto (CBAC)

CBAC no quita las opciones TCP de la secuencia TCP. MPTCP crea una conexión a través del firewall.

Firewall basado en zonas (ZBFW)

Cisco IOS y IOS-XE ZBFW no quitan las opciones TCP de la secuencia TCP. MPTCP crea una conexión a través del firewall.

ACE

De forma predeterminada, el dispositivo ACE elimina las opciones TCP de las conexiones TCP. La conexión MPTCP vuelve a las operaciones TCP normales.

El dispositivo ACE se puede configurar para permitir las opciones TCP a través del comando **tcp-options**, como se describe en la sección Configuración de cómo la ACE maneja las opciones TCP de la Guía de Seguridad vA5(1.0), Cisco ACE Application Control Engine. Sin embargo, esto no siempre se recomienda, ya que los subflujos secundarios pueden equilibrarse a diferentes servidores reales y la unión falla.

Productos de Cisco no afectados por MPTCP

Por lo general, cualquier dispositivo que no inspeccione los flujos TCP o la información de Capa 7 tampoco modifica las opciones TCP y, como resultado, debe ser transparente para MPTCP. Estos dispositivos pueden incluir:

- ASR de Cisco serie 5000 (Starent)
- Wide Area Application Services (WAAS)
- NAT de nivel de operador (CGN) (blade de motor de servicios de nivel de operador (CGSE) en el sistema de routing de operador (CRS)-1)
- Todos los productos de switch Ethernet
- Todos los productos del router (a menos que se active la funcionalidad de firewall o NAT; consulte la sección Productos de Cisco Afectados por MPTCP anteriormente en el documento para obtener más detalles)