# MPTCP y descripción de la asistencia técnica

## Contenido



## Introducción

Este documento proporciona a una descripción de TCP de trayectoria múltiple (MPTCP), su impacto en el examen del flujo, y los Productos Cisco que están y no son afectados por él.

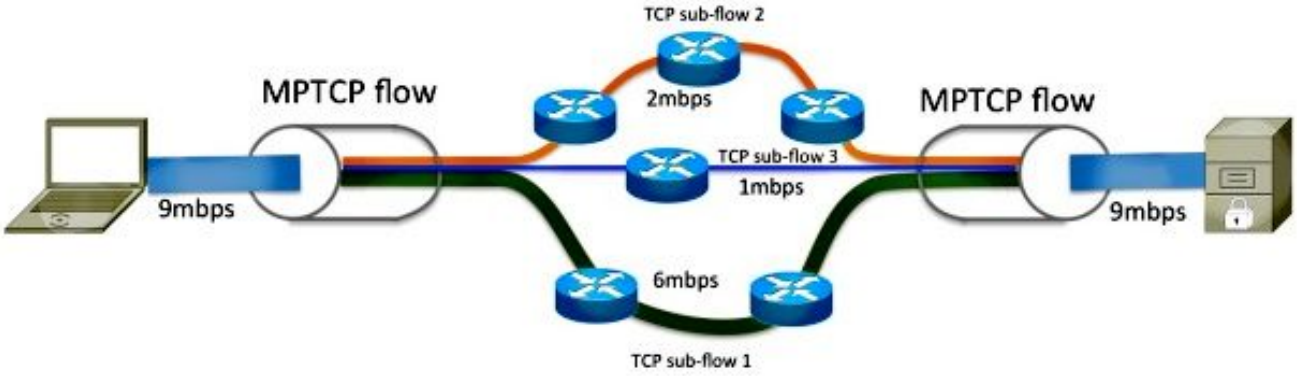
## Descripción MPTCP

### Antecedentes

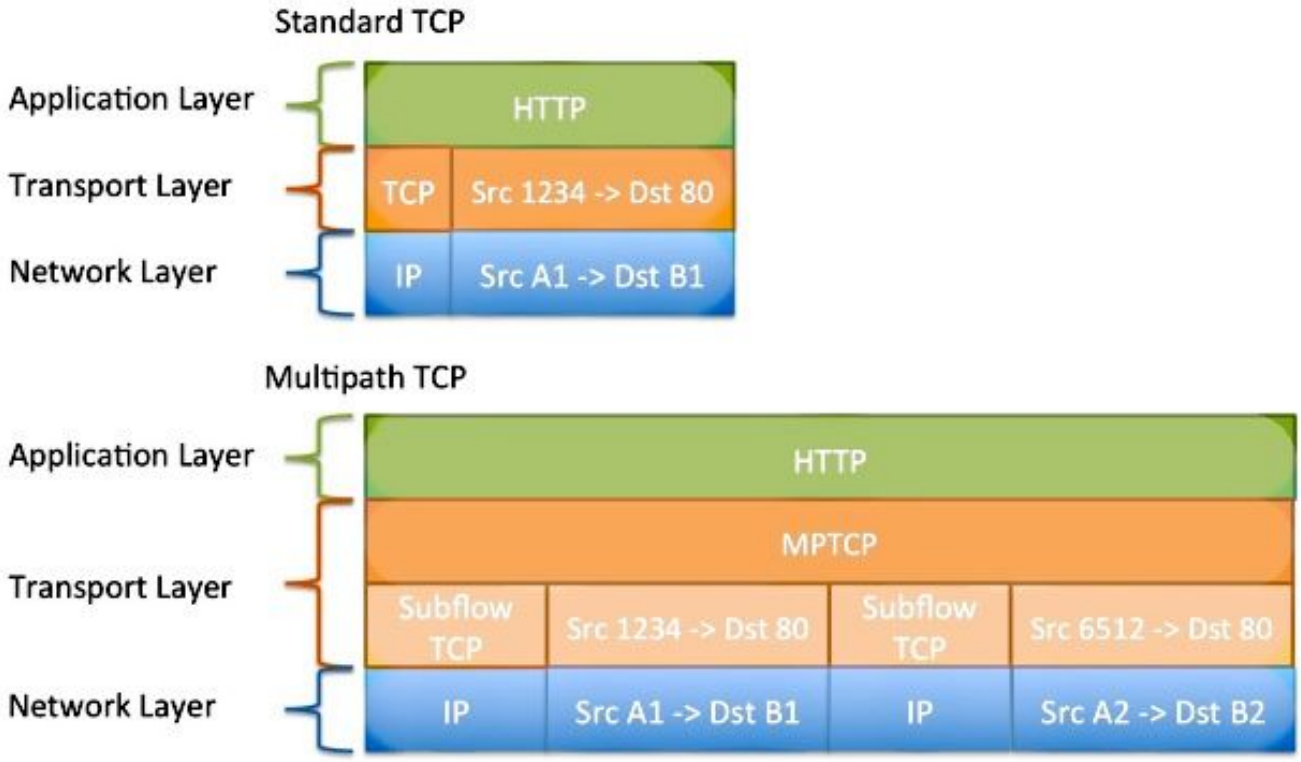
Los host conectados con Internet o dentro de un entorno del centro de datos son conectados a menudo por los trayectos múltiples. Sin embargo, cuando el TCP se utiliza para el transporte de datos, la comunicación se restringe a una trayectoria de red única. Es posible que algunas trayectorias entre los dos host están congestionadas, mientras que las trayectorias alternas están inutilizadas. Un uso más eficiente de los recursos de red es posible si estos trayectos múltiples se utilizan en paralelo. Además, el uso de las conexiones múltiples aumenta la experiencia del usuario, porque proporciona al más alto rendimiento y a la resistencia mejorada contra los desperfectos de la red.

MPTCP es un conjunto de las Extensiones al TCP regular que permite a un solo flujo de datos ser separado y ser llevado a través de las conexiones múltiples. Refiera al [RFC6824: Extensiones TCP para la operación de trayectoria múltiple con las múltiples direcciones](#) para más información.

Tal y como se muestra en de este diagrama, MPTCP puede separar el 9mbps fluye en tres diversos sub-flujos en el nodo emisor, que se agrega posteriormente nuevamente dentro del flujo de las informaciones originales en el nodo de recepción.




Los datos que ingresan la conexión MPTCP actúan exactamente como hacen a través de una conexión TCP regular; los datos transmitidos han garantizado una salida de la en-orden. Puesto que MPTCP ajusta la pila de la red y actúa dentro de la capa de transporte, es utilizado transparente por la aplicación.



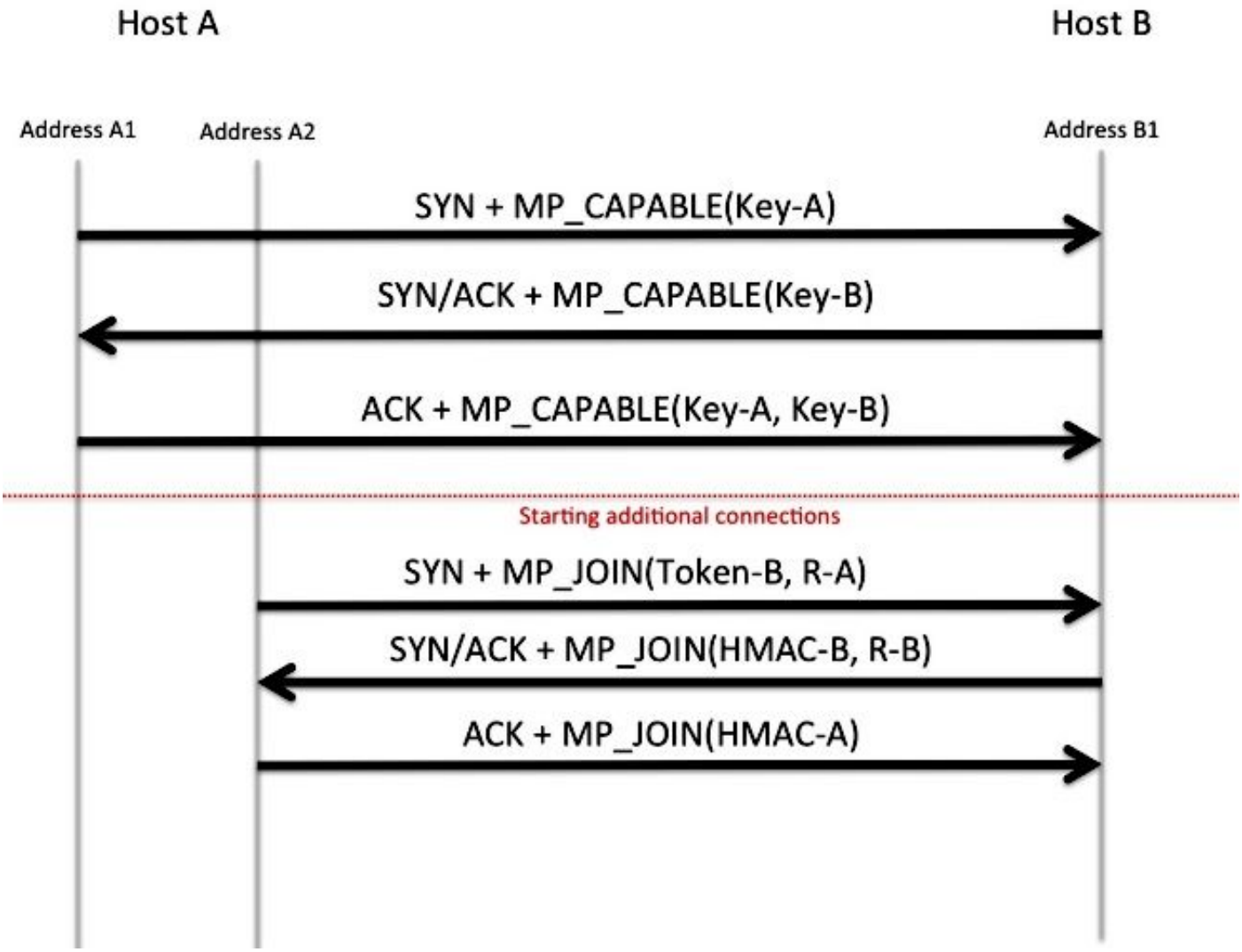

## Establecimiento de sesión

MPTCP utiliza las opciones TCP para negociar y orquestrar la separación y el nuevo ensamble de los datos sobre los sub-flujos múltiples. **La opción TCP 30** es reservada por el Internet Assigned Numbers Authority (IANA) para el uso exclusivo por MPTCP. Refiera a los parámetros del Transmission Control Protocol (TCP) para más información. En el establecimiento de una sesión TCP regular, una opción **MP_CAPABLE** se incluye en la inicial sincroniza el paquete (del SYN). Si las ayudas del respondedor y eligen negociar MPTCP, él también responden con la opción **MP_CAPABLE** en el paquete del SYN-reconocimiento (ACK). Las claves intercambiadas dentro

de este apretón de manos se utilizan en el futuro para autenticar unirse a y el retiro de otras sesiones TCP en este MPTCP fluye.

## Únase a los Sub-flujos adicionales

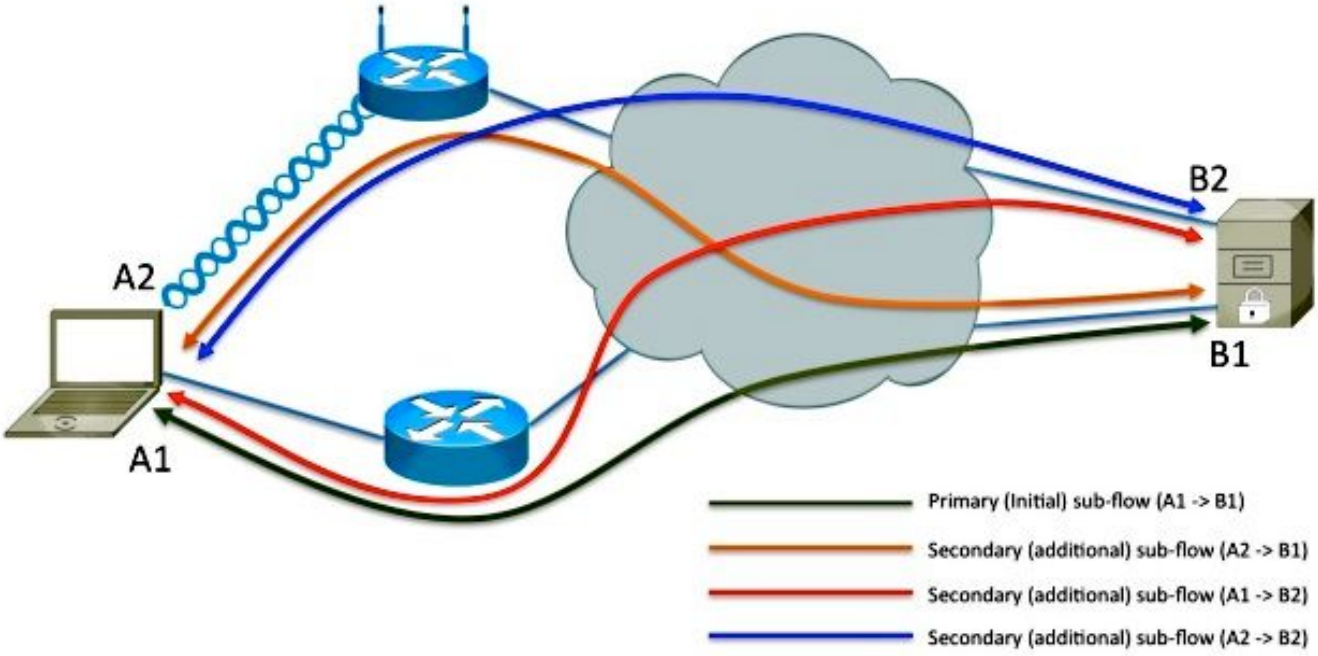
Cuando estaba juzgado necesario, el **host A** pudo iniciar los sub-flujos adicionales originarios de un diverso interfaz o direccionamiento al **host B**. Como con el sub-flujo inicial, las opciones TCP se utilizan para indicar el deseo de combinar este sub-flujo con el otro sub-flujo. Las claves que se intercambian dentro del establecimiento inicial del sub-flujo (junto con un algoritmo de troceo) son utilizadas por el **host B** para confirmar que la petición del unido es enviada de hecho por el **host A**. El sub-flujo secundario 4-tuple (IP de la fuente, IP del destino, puerto de origen, y puerto de destino) es diferente que el del sub-flujo primario; este flujo pudo tomar una diversa trayectoria a través de la red.




## Agregue el direccionamiento

**El host A** tiene interfaces múltiples, y es posible que el **host B** tiene conexiones de Red múltiple. **El host B** aprende sobre los direccionamientos A1 y A2 implícito como resultado de los sub-flujos de la compra de componentes del **host A de** cada uno de sus direccionamientos destinado al B1. Es posible que el **host B** hace publicidad de su dirección adicional (B2) al **host A** para hacer otros sub-flujos al B2. Esto se completa vía la **opción TCP 30**. Tal y como se muestra en de este diagrama, el **host B** hace publicidad de su dirección secundaria (B2) al **host A**, y se crean dos sub-flujos adicionales. Porque MPTCP actúa sobre la capa de red de la pila del interconexión de

sistema abierto (OSI), los IP Addresses des divulgación pueden ser IPv4, IPv6, o ambos. Es posible que algunos de los sub-flujos son transportados por IPv4 simultáneamente mientras que otros sub-flujos son transportados por el IPv6.




### Segmentación, de trayectoria múltiple, y nuevo ensamble

Una secuencia de datos dada a MPTCP por la aplicación se debe dividir en segmentos y distribuir a través de los sub-flujos múltiples por el remitente. Entonces debe ser vuelta a montar en la sola secuencia de datos antes de que se entregue de nuevo a la aplicación.

MPTCP examina el funcionamiento y el tiempo de espera de cada sub-flujo, y ajusta dinámicamente la distribución de datos para ganar la producción global más alta. Durante la Transferencia de datos, la opción del encabezado de TCP incluye la información sobre los números de la secuencia/del acuse de recibo MPTCP, la secuencia actual del sub-flujo/el número del acuse de recibo, y una suma de comprobación.

## Impacto en el examen del flujo

Muchos dispositivos de seguridad pudieron zero-out o substituir las opciones TCP desconocidas por un ningún valor de la opción (NOOP). Si el dispositivo de red hace esto paquete TCP Syn encendido al sub-flujo inicial, se quita el anuncio **MP_CAPABLE**. Como consecuencia, aparece al servidor que el cliente no utiliza MPTCP, e invierte a la operación normal TCP.

Si se preserva la opción y MPTCP puede establecer los sub-flujos múltiples, el análisis en línea del paquete por los dispositivos de red no pudo funcionar confiablemente. Esto es porque solamente las porciones del flujo de datos se transportan a cada sub-flujo. El efecto del examen del protocolo sobre MPTCP pudo variar nada a la interrupción completa del servicio. El efecto varía basado en lo que y se examinan cuántos datos. El análisis del paquete pudo incluir el gateway de capa de aplicación del Firewall (ALG o fixup), el Network Address Translation (NAT) ALG, visibilidad de la aplicación y el control (AVC), Reconocimiento de aplicaciones basadas en la red (NBAR) o los servicios de la detección de intrusos (IDS/IPS). Si la Inspección de la aplicación se requiere en su entorno, se recomienda que el borrar de la **opción TCP 30** está activado.

Si el flujo no puede ser examinado debido al cifrado o si el protocolo es desconocido, después el dispositivo en línea no debe tener ningún impacto en el MPTCP fluye.

# Productos Cisco afectados por MPTCP

Estos Productos son afectados por MPTCP:

- Dispositivo de seguridad adaptante (ASA)
- Defensa de la amenaza de Cisco FirePOWER
- Sistema de prevención de intrusiones (IPS)
- Cisco IOS XE y IOS®
- Motor del control de la aplicación (ACE)

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

## ASA

### Operaciones TCP

Por abandono, el Firewall de Cisco ASA substituye las opciones TCP sin apoyo, que incluyen la **opción 30 MPTCP**, por la opción NOOP (opción 1). Para permitir la opción MPTCP, utilice esta configuración:

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

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

2. Defina la selección del tráfico:

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

3. Defina una correspondencia del tráfico a la acción:

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

4. Actívela en el cuadro o el por-interfaz:

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

### Examen del protocolo

El ASA utiliza el examen de muchos protocolos. El efecto que el motor del examen pudo tener en la aplicación varía. Se recomienda que, si se requiere el examen, la TCP-correspondencia descrita previamente no es aplicada.

## Defensa de la amenaza de Cisco FirePOWER

### Operaciones TCP

Mientras que el FTD se realiza el examen profundo del paquete para IPS/IDS lo mantiene no se recomienda modificar la TCP-correspondencia para permitir la opción TCP a través.

### Cisco IOS Firewall

#### Control de acceso basado en el contexto (CBAC)

CBAC no quita las opciones TCP de la secuencia TCP. MPTCP construye una conexión con el Firewall.

#### Firewall Zona-basado (ZBFW)

El Cisco IOS e IOS-XE ZBFW no quita las opciones TCP de la secuencia TCP. MPTCP construye una conexión con el Firewall.

### ACE

Por abandono, el dispositivo de ACE elimina las opciones TCP de las conexiones TCP. La conexión MPTCP recurre a las operaciones regulares TCP.

El dispositivo de ACE se pudo configurar para permitir las opciones TCP vía el comando de las TCP-**opciones**, según lo descrito en configurar cómo ACE maneja la sección de las opciones TCP de la guía de la Seguridad vA5(1.0), motor del control de la aplicación de Cisco ACE. Sin embargo, esto no se recomienda siempre, porque los sub-flujos secundarios se pudieron equilibrar a diversos servidores reales, y el unir a falla.

## Productos Cisco no afectados por MPTCP

Generalmente, cualquier dispositivo que no examine los flujos TCP o la información Layer-7 también no altera las opciones TCP, y como consecuencia debe ser transparente a MPTCP. Estos dispositivos pudieron incluir:

- Cisco 5000 Series ASR (Starent)
- Wide Area Application Services (WAAS)
- Portador-grado NAT (CGN) (el Portador-grado mantiene la cuchilla del motor (CGSE) en el sistema de ruteo del portador (CRS)-1)
- Todos los Productos del conmutador de los Ethernetes
- Todos los Productos del router (a menos que se activa el Firewall o la funcionalidad de NAT; vea los Productos Cisco afectados por la sección MPTCP anterior en el documento para más detalles)