

Resolución de problemas de configuración incorrecta del bit S de TWAMP

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Problema: el bit S de TWAMP está configurado incorrectamente](#)

[TWAMP fundamental](#)

[Las entidades de TWAMP:](#)

[Los protocolos de TWAMP:](#)

[Troubleshoot](#)

[Solución: bit S nunca implementado en IOS-XR](#)

Introducción

Este documento describe Active Measurement Protocol y el uso del bit de sincronización (bit S) para las mediciones de retardo. Describe la compatibilidad del bit S en la plataforma IOS-XR.

Prerequisites

Requirements

Cisco recomienda tener conocimientos básicos sobre estos temas:

- Protocolo de medición activa unidireccional (OWAMP)
- Protocolo de medición activa bidireccional (TWAMP)
- Routers de servicios de agregación Cisco ASR serie 9000 (ASR9000)

Componentes Utilizados

La información de este documento se basa en Dispositivos Cisco ASR9000 - IOS-XR versión 5.3.4.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). If your network is live, make sure that you understand the potential impact of any command.

Problema: el bit S de TWAMP está configurado incorrectamente

Puede utilizar TWAMP para medir el rendimiento unidireccional y de ida y vuelta entre dos dispositivos compatibles con TWAMP. Al probar el acuerdo de nivel de servicio del protocolo de Internet basado en TWAMP (IP SLA) entre la sonda de terceros y los dispositivos CRS/ASR9000 que se ejecutan en IOS-XR 5.3.4, el servidor TWAMP establece el bit S en False. Por lo tanto, el dispositivo de sondeo no calcula la demora unidireccional.

TWAMP fundamental

El protocolo de medición activa unidireccional (OWAMP), especificado en RFC4656, proporciona un protocolo común para medir métricas unidireccionales entre dispositivos de red. OWAMP se puede utilizar bidireccionalmente para medir métricas unidireccionales en ambas direcciones entre dos elementos de la red. Sin embargo, no admite mediciones de ida y vuelta o bidireccionales.

El protocolo de medición activa bidireccional (TWAMP) descrito en RFC5357 es un proceso de supervisión del rendimiento altamente eficaz y basado en estándares que amplía la especificación del protocolo de medición activa unidireccional (OWAMP) definida en RFC-4656 con la adición de la medición del rendimiento de las métricas de ida y vuelta y bidireccionales para redes basadas en IP. TWAMP es un método independiente del proveedor para medir con precisión el rendimiento unidireccional y de ida y vuelta entre dos terminales compatibles con TWAMP.

Según RFC4656 (One-Way Active Measurement Protocol), se debe establecer el primer bit **S**, si la parte que genera la marca de tiempo tiene un reloj que se sincroniza con UTC a través de una fuente externa.

Por ejemplo, se debe establecer el bit S, si:

- El hardware del Sistema de posicionamiento global (GPS) se utiliza para indicar que ha adquirido la posición y la hora actuales.
- El protocolo de tiempo de la red (NTP) se utiliza para indicar que está sincronizado con una fuente externa, que incluye una fuente de estrato 0, etc.).
- No existe ninguna noción de sincronización externa para la fuente de tiempo, el bit S no debe configurarse.

The Error Estimate specifies the estimate of the error and synchronization. It has the following format:

```

0                               1
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5
+-----+-----+-----+-----+
|S|Z|   Scale   | Multiplier |
+-----+-----+-----+-----+

```

Las entidades de TWAMP:

El sistema TWAMP consta de 4 entidades lógicas:

- servidor: gestiona una o más sesiones de TWAMP y también configura los puertos por sesión en los terminales

- reflector de sesión: refleja un paquete de medición en cuanto recibe un paquete de prueba TWAMP

- cliente de control: inicia el inicio y la detención de las sesiones de prueba de TWAMP

- session-sender: crea instancias de los paquetes de prueba TWAMP enviados al reflector de sesión

Los protocolos de TWAMP:

El protocolo TWAMP incluye tres categorías distintas de intercambio de mensajes:

- Intercambio de configuración de la conexión

Los mensajes establecen una conexión de sesión entre Control-Client y el Servidor. En primer lugar, las identidades de los pares comunicados se establecen a través de un mecanismo de respuesta de desafío. El servidor envía un desafío generado aleatoriamente, al que el cliente de control envía una respuesta cifrando el desafío mediante una clave derivada del secreto compartido. Una vez que se establecen las identidades, el siguiente paso negocia un modo de seguridad que está enlazado para los subsiguientes comandos TWAMP-Control, así como los paquetes de secuencia TWAMP-Test.

Nota: Un servidor puede aceptar solicitudes de conexión de varios clientes de control.

- intercambio de control TWAMP

El protocolo TWAMP-Control se ejecuta sobre TCP y se utiliza para instanciar y controlar sesiones de medición. La secuencia de comandos es la siguiente, pero a diferencia de los intercambios de configuración de conexión, los comandos TWAMP-Control se pueden enviar varias veces. Sin embargo, los mensajes no pueden aparecer fuera de secuencia, aunque se pueden enviar varios comandos request-session antes de un comando session-start.

- Request-Session
- Inicio de sesión
- Stop-Session

- intercambio de secuencia de prueba de TWAMP

La prueba TWAMP se ejecuta sobre UDP e intercambia paquetes de prueba TWAMP entre el remitente y el reflector de sesión. Estos paquetes incluyen campos de marca de tiempo que contienen el instante de la salida y el ingreso del paquete. Además, cada paquete incluye una estimación de error que indica el sesgo de sincronización del remitente (sesión-remitente o sesión-reflector) con una fuente de tiempo externa (por ejemplo, GPS o NTP). El paquete también incluye un número de secuencia.

El control de TWAMP y el flujo de prueba de TWAMP tienen tres modos de seguridad: sin autenticar, autenticado y cifrado.

Troubleshoot

Algunas plataformas pueden depender de una configuración o implementación determinada para proporcionar la marca de tiempo del hardware. En concreto, los routers de la serie ASR9000 de Cisco necesitan la sincronización del protocolo de tiempo de precisión (PTP) como fuente de reloj. Es posible que esta solución no esté disponible en todos los escenarios de usuario. Para permitir el uso de otras fuentes de marca de tiempo (fuente de reloj NTP, a través de un demonio que se ejecuta en RouteProcessor (RP)), se introduce una nueva configuración de **ipsla hw-**

timestamp disable para ignorar los valores de marca de tiempo proporcionados por otras capas dependientes de la plataforma y volver a las marcas de tiempo independientes de la plataforma.

Si la sincronización del reloj NTP está habilitada y activada, utilice el comando **hw-timestamp disable** en la configuración de IP SLA para inhabilitar la marca de tiempo del hardware.

```
ipsla
  hw-timestamp disable
  responder
    twamp
      timeout 100
    !
  !
  server twamp
    timer inactivity 100
```

[Notas de la versión para los routers de servicios de agregación de la serie ASR 9000 de Cisco, versión 6.0.1](#) introduce una nueva función de mejora de la precisión de TWAMP.

La mejora de la precisión de TWAMP proporciona granularidad en microsegundos en las mediciones de TWAMP. Esta mejora permite la recopilación de sellos de hora de entrada y salida lo más cerca posible del cable, para lograr una mayor precisión.

Puede actualizar la versión de IOS XR a 6.1.X y posterior para poder utilizar la función TWAMP Accuracy Enhancement y verificar el logro del comportamiento deseado.

Puede realizar estos pasos para resolver el problema, así como las capturas de paquetes

1. Configure valores más altos para los tiempos de espera para el servidor twamp y el respondedor (por ejemplo, 120s), para que la información no caduque demasiado rápido antes de la recopilación.
2. Dado que la depuración debe estar habilitada, asegúrese de configurar el dispositivo para enviar mensajes de registro de depuración al búfer de registro. El tamaño del buffer de registro debe configurarse lo suficientemente grande como para evitar la reversión de los mensajes de depuración durante la prueba.
3. Asegúrese de que se capturan todos los paquetes intercambiados entre el dispositivo y la sonda (no sólo paquetes de sonda UDP, sino también TCP para el establecimiento de sesión)
4. La recopilación de los comandos enumerados de los dispositivos ASR9000 o CRS depende del lugar en el que se realicen las pruebas:

Paso 1. Antes de iniciar la prueba desde la sonda, recopile:

- **terminal length 0**
- **show install active sum**
- **admin show platform**
- **admin show hw-module fpd location all**
- **'show run'**

- **ipsla twamp standards**
- **vshow ipsla twamp status**
- **show ntp status**
- **show ntp associations detail**

Paso 2.Habilite todos los debugs de Twamp en el dispositivo y luego borre el registro.

1. iniciar la captura de paquetes
2. iniciar la prueba desde la sonda

Nota: Esto no produce demasiadas salidas si es la única prueba de twamp que se ejecuta en la sonda.

Paso 3.Recopile estos comandos después de finalizar la prueba

- **show log**
- **show ipsla twamp connection detail**
- **show ipsla twamp connection requests**
- **show ipsla twamp session**
- **show ipsla trace twamp all verbose**
- **show ipsla trace twamp initialize verbose**

Solución: bit S nunca implementado en IOS-XR

Según RFC 4656, si no hay ninguna noción de sincronización externa para la fuente de tiempo, el bit S no debe configurarse. Por lo tanto, el bit S no se implementa en la plataforma IOS-XR.

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).