

Risoluzione dei problemi: il bit S di TWAMP non è impostato correttamente

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Problema: il bit S TWAMP non è impostato correttamente](#)

[TWAMP fondamentale](#)

[Le entità TWAMP:](#)

[I protocolli TWAMP:](#)

[Risoluzione dei problemi](#)

[Soluzione: S bit mai implementato in IOS-XR](#)

Introduzione

Questo documento descrive il protocollo Active Measurement e l'uso del bit di sincronizzazione (S bit) per le misurazioni ritardate. Descrive la supportabilità del bit S nella piattaforma IOS-XR.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza di base dei seguenti argomenti:

- Protocollo OWAMP (One-way Active Measurement Protocol)
- Protocollo TWAMP (Two Way Active Measurement Protocol)
- Cisco ASR serie 9000 Aggregation Services Router (ASR9000)

Componenti usati

Le informazioni di questo documento si basano Dispositivi Cisco ASR9000 - IOS-XR versione 5.3.4.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Problema: il bit S TWAMP non è impostato correttamente

È possibile utilizzare TWAMP per misurare le prestazioni unidirezionali e di andata e ritorno tra due dispositivi supportati da TWAMP. Quando si esegue il test del protocollo IP SLA (Internet Protocol Service Level Agreement) basato su TWAMP tra la sonda di terze parti e i dispositivi CRS/ASR9000 in esecuzione su IOS-XR 5.3.4, il server TWAMP imposta il bit S su False. Pertanto, il ritardo unidirezionale non viene calcolato dal dispositivo di tastatura.

TWAMP fondamentale

Il protocollo OWAMP (One-way Active Measurement Protocol), specificato nella RFC4656, fornisce un protocollo comune per misurare le metriche unidirezionali tra i dispositivi di rete. OWAMP può essere utilizzato bidirezionalmente per misurare le metriche unidirezionali in entrambe le direzioni tra due elementi di rete. Tuttavia, non supporta misurazioni di andata e ritorno o a due vie.

Il protocollo TWAMP (Two Way Active Measurement Protocol) descritto nella RFC5357 è un processo di monitoraggio delle prestazioni basato su standard e altamente efficace che si espande in base alla specifica OWAMP (One-Way Active Measurement Protocol) definita nella RFC-4656 con l'aggiunta della misurazione delle prestazioni delle metriche round-trip e two-way per le reti IP. TWAMP è un metodo indipendente dal fornitore che consente di misurare accuratamente le prestazioni unidirezionali e di andata e ritorno tra due endpoint supportati da TWAMP.

In base a RFC4656 (One-Way Active Measurement Protocol), il primo bit **S** deve essere impostato se la parte che genera il timestamp dispone di un orologio sincronizzato con UTC tramite un'origine esterna.

Ad esempio, il bit S deve essere impostato se:

- L'hardware GPS (Global Positioning System) viene utilizzato per indicare che ha acquisito la posizione e l'ora corrente.
- Il protocollo NTP (Network Time Protocol) viene utilizzato per indicare che è sincronizzato con un'origine esterna, che include l'origine di livello 0 e così via.
- Non esiste un concetto di sincronizzazione esterna per l'origine ora. Il bit S non deve essere impostato.

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 |
+-----+-----+-----+-----+

```

Le entità TWAMP:

Il sistema TWAMP è costituito da 4 entità logiche:

- server - gestisce una o più sessioni TWAMP e configura le porte per sessione negli endpoint
- riflettore di sessione - riflette un pacchetto di misurazione non appena riceve un pacchetto di prova TWAMP
- control-client - avvia e arresta le sessioni di test TWAMP

- session-sender - crea un'istanza dei pacchetti di prova TWAMP inviati al riflettore di sessione

I protocolli TWAMP:

Il protocollo TWAMP include tre diverse categorie di scambio di messaggi:

- Scambio configurazione connessione

I messaggi stabiliscono una connessione tra il client di controllo e il server. In primo luogo le identità dei peer comunicati vengono stabilite tramite un meccanismo di risposta alle richieste. Il server invia una richiesta di verifica generata casualmente, alla quale Control-Client invia una risposta crittografando la richiesta utilizzando una chiave derivata dal segreto condiviso. Una volta stabilite le identità, il passaggio successivo negozia una modalità di sicurezza che viene associata per i successivi comandi TWAMP-Control e per i pacchetti di flusso TWAMP-Test.

Nota: un server può accettare richieste di connessione da più client di controllo.

- scambio controllo TWAMP

Il protocollo TWAMP-Control viene eseguito su TCP e viene utilizzato per creare istanze e controllare sessioni di misurazione. La sequenza dei comandi è la seguente, ma a differenza degli scambi di configurazione della connessione, i comandi TWAMP-Control possono essere inviati più volte. Tuttavia, i messaggi non possono avere una sequenza diversa sebbene sia possibile inviare più comandi request-session prima di un comando session-start.

Richiesta-Session
Start-Session
STOP-Session

- scambio di flussi di test TWAMP

Il test TWAMP viene eseguito su UDP e scambia pacchetti di test TWAMP tra il mittente della sessione e il riflettore della sessione. Questi pacchetti includono campi di data e ora che contengono l'istante di uscita e di entrata del pacchetto. Inoltre, ciascun pacchetto include una stima dell'errore che indica l'inclinazione della sincronizzazione del mittente (mittente della sessione o riflettore di sessione) con una fonte temporale esterna (ad esempio, GPS o NTP). Il pacchetto include anche un numero di sequenza.

Controllo TWAMP e flusso di test TWAMP dispongono di tre modalità di protezione: non autenticato, autenticato e crittografato.

Risoluzione dei problemi

Per fornire l'indicatore orario dell'hardware, alcune piattaforme possono fare affidamento su una determinata configurazione o distribuzione. In particolare, i router Cisco ASR serie 9000 devono essere sincronizzati con Precision Time Protocol (PTP) come origine dell'orologio. Questa soluzione potrebbe non essere disponibile in tutti gli scenari utente. Per consentire l'uso di altre fonti di timestamp (sorgente dell'orologio NTP, attraverso un daemon in esecuzione su RouteProcessor (RP)), viene introdotta una nuova configurazione di **ipsla hw-timestamp disable** per ignorare i valori di timestamp forniti da altri livelli dipendenti dalla piattaforma e tornare ai timestamp indipendenti dalla piattaforma.

Se la sincronizzazione dell'orologio NTP è abilitata e attivata, usare il comando **hw-timestamp disable** nella configurazione dello SLA IP per disabilitare il timestamp dell'hardware.

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

[Note sulla versione per Cisco ASR serie 9000 Aggregation Services Router, versione 6.0.1.](#) introduce una nuova funzionalità di miglioramento della precisione TWAMP.

Il miglioramento dell'accuratezza TWAMP fornisce granularità al microsecondo nelle misurazioni TWAMP. Questo miglioramento consente la raccolta di timestamp in entrata e in uscita il più vicino possibile al filo, per ottenere una maggiore precisione.

È possibile aggiornare IOS XR release alla versione 6.1.X e successive per poter utilizzare la funzionalità TWAMP Accuracy Enhancement e verificare il raggiungimento del comportamento desiderato.

È possibile eseguire queste operazioni per risolvere il problema e per acquisire i pacchetti

1. Configurare valori più alti per i timeout per il server di timestamp e il risponditore (ad esempio, 120s), in modo che le informazioni non scadano troppo rapidamente prima della raccolta.
2. Poiché è necessario attivare il debug, configurare il dispositivo in modo che invii messaggi di registro di debug al buffer di registrazione. La dimensione del buffer di registrazione deve essere configurata in modo da impedire il rollover dei messaggi di debug durante il test.
3. Accertarsi che tutti i pacchetti scambiati tra il dispositivo e la sonda siano stati acquisiti (non solo i pacchetti di sonda UDP, ma anche il TCP per la definizione della sessione)
4. Raccogliere i comandi elencati dai dispositivi ASR9000 o CRS, a seconda del punto in cui vengono eseguiti i test:

Passaggio 1. Prima di iniziare il test dal probe, raccogliere:

- **lunghezza terminale 0**
- **show install active sum**
- **admin show platform**
- **admin show hw-module fpd location all**
- **show run**
- **standard ipsla twamp**
- **stato vshow ipsla twamp**
- **mostra stato ntp**
- **mostra dettagli associazioni ntp**

Passaggio 2. Abilitare tutti i debug di Twamp sul dispositivo e cancellare il registro.

1. avviare l'acquisizione dei pacchetti
2. avvia il test dalla sonda

Nota: questa operazione non produce troppi output se è l'unico test a torsione eseguito sulla sonda.

Passaggio 3. Raccogliere questi comandi dopo il completamento del test

- **show log**
- **mostra dettagli connessione twamp ipsla**
- **mostra richieste di connessione twamp ipsla**
- **mostra sessione twamp ipsla**
- **show ipsla trace twamp all verbose**
- **visualizzazione dettagliata dell'inizializzazione del twamp della traccia ipsla**

Soluzione: S bit mai implementato in IOS-XR

In base alla RFC 4656, se non è prevista la sincronizzazione esterna per l'origine ora, il bit non deve essere impostato. Pertanto, il bit S non è implementato nella piattaforma IOS-XR.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).