Troubleshooting de TWAMP S bit is Set Incorrect (O bit S do TWAMP está configurado incorretamente)

Contents

Introduction

Este documento descreve o Ative Measurement Protocol e o uso do bit de sincronização (S bit) para medições de atraso. Ele descreve a capacidade de suporte do bit S na plataforma IOS-XR.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento básico destes tópicos:

- Protocolo de Medição Ativa Unidirecional (OWAMP)
- Protocolo de Medição Ativa Bidirecional (TWAMP - Two Way Ative Measurement Protocol)
- Roteadores de serviços de agregação Cisco ASR 9000 Series (ASR9000)

Componentes Utilizados

As informações neste documento são baseadas em Dispositivos Cisco ASR9000 - IOS-XR versão 5.3.4.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Problema: bit S TWAMP configurado incorretamente

Você pode usar o TWAMP para medir o desempenho unidirecional e de ida e volta entre dois dispositivos suportados pelo TWAMP. Quando você testa o Contrato de nível de serviço de protocolo Internet (IP SLA - Internet Protocol Service Level Agreement) baseado em TWAMP entre o testador de terceiros e os dispositivos CRS/ASR9000 que são executados no IOS-XR 5.3.4, o Servidor TWAMP define o bit S como Falso. Portanto, o atraso unidirecional não é calculado pelo dispositivo de sonda.

TWAMP Fundamental

O OWAMP (One-way Ative Measurement Protocol), especificado no RFC4656, fornece um protocolo comum para medir métricas unidirecionais entre dispositivos de rede. O OWAMP pode ser usado bidirecionalmente para medir métricas unidirecionais em ambas as direções entre dois elementos de rede. No entanto, não acomoda medições de ida e volta ou de mão dupla.

O Protocolo de Medição Ativa Bidirecional (TWAMP - Two-Way Ative Measurement Protocol), descrito no RFC5357, é um processo de monitoração de desempenho altamente eficiente e baseado em padrões que se expande sobre a especificação do Protocolo de Medição Ativa Unidirecional (OWAMP - One-Way Ative Measurement Protocol) definido no RFC-4656 com a adição da medição de desempenho de métricas de ida e volta para redes baseadas em IP. O TWAMP é um método independente de fornecedor para medir com precisão o desempenho unidirecional e de ida e volta entre dois endpoints suportados pelo TWAMP.

De acordo com o RFC4656 (One-Way Ative Measurement Protocol), o primeiro bit **S** deve ser definido, se a parte que gera o timestamp tiver um relógio que esteja sincronizado com o UTC através de uma fonte externa.

Por exemplo, o bit S deve ser definido, se:

- O hardware do sistema de posicionamento global (GPS) é usado para indicar que ele adquiriu a posição e o tempo atuais.
- O Network Time Protocol (NTP) é usado para indicar que ele está sincronizado com uma fonte externa, que inclui a fonte stratum 0, etc.).
- Não há noção de sincronização externa para a fonte de tempo, o bit S não deve ser definido.

```
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  |
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

As entidades TWAMP:

O sistema TWAMP consiste em 4 entidades lógicas:
· servidor - gerencia uma ou mais sessões TWAMP e também configura portas por sessão nos terminais
· refletor de sessão - reflete um pacote de medição assim que recebe um pacote de teste TWAMP
· cliente de controle - inicia o início e o fim das sessões de teste TWAMP

· session-sender - instancia os pacotes de teste TWAMP enviados ao refletor de sessão

Os protocolos TWAMP:

O protocolo TWAMP inclui três categorias distintas de troca de mensagens:

- Intercâmbio de configuração de conexão

As mensagens estabelecem uma conexão de sessão entre o cliente de controle e o servidor. Primeiro, as identidades dos colegas comunicados são estabelecidas por meio de um mecanismo de resposta a desafios. O servidor envia um desafio gerado aleatoriamente, para o qual o cliente de controle envia uma resposta criptografando o desafio usando uma chave derivada do segredo compartilhado. Uma vez estabelecidas as identidades, a próxima etapa negocia um modo de segurança que é vinculado para os comandos TWAMP-Control subsequentes, bem como os pacotes de fluxo TWAMP-Test.

> **Observação**: um servidor pode aceitar solicitações de conexão de vários clientes de controle.

- Intercâmbio de controle TWAMP

O protocolo TWAMP-Control é executado sobre TCP e é usado para instanciar e controlar sessões de medição. A sequência de comandos é a seguinte, mas ao contrário das trocas de configuração de conexão, os comandos TWAMP-Control podem ser enviados várias vezes. No entanto, as mensagens não podem ocorrer fora de sequência, embora vários comandos request-session possam ser enviados antes de um comando session-start.

  - Request-Session
  - Start-Session
  - Stop-Session

- Intercâmbio de fluxo de teste TWAMP

O TWAMP-Test é executado sobre UDP e troca pacotes TWAMP-Test entre Session-Sender e Session-Refletor. Esses pacotes incluem campos de carimbo de data/hora que contêm o instante de saída e ingresso do pacote. Além disso, cada pacote inclui uma estimativa de erro que indica o desvio de sincronização do remetente (sessão-remetente ou sessão-refletor) com uma fonte de tempo externa (por exemplo, GPS ou NTP). O pacote também inclui um número de sequência.

TWAMP-Control e TWAMP-test stream, têm três modos de segurança: não autenticado, autenticado e criptografado.

Troubleshoot

Algumas plataformas podem depender de uma determinada configuração ou implantação para fornecer carimbo de data/hora de hardware. Em particular, os roteadores da série Cisco ASR9000 precisam da sincronização do Precision Time Protocol (PTP) como fonte de tempo. Essa solução pode não estar disponível em todos os cenários de usuário. Para permitir o uso de outras fontes de registro de data e hora (fonte de registro de data e hora NTP, através de um daemon em execução no RouteProcessor (RP)), uma nova configuração de **ipsla hw-timestamp disable** é introduzida para ignorar os valores de registro de data e hora fornecidos por outras camadas

dependentes da plataforma e reverter para os registros de data e hora independentes da plataforma.

Se a sincronização de relógio NTP estiver habilitada e ativada, use o comando **hw-timestamp disable** na configuração SLA IP para desabilitar o carimbo de data/hora do hardware.

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

Notas de versão para Cisco ASR 9000 Series Aggregation Services Routers, a versão 6.0.1 apresenta um novo recurso de aprimoramento de precisão TWAMP.

O aprimoramento de precisão TWAMP fornece granularidade de microssegundos em medições TWAMP. Esse aprimoramento permite a coleta de carimbos de data/hora de entrada e saída o mais próximo possível do fio, para obter mais precisão.

Você pode atualizar o IOS XR Release para 6.1.X e superior para poder usar o recurso de Aprimoramento de Precisão TWAMP e verificar a realização do comportamento desejado.

Você pode executar estas etapas para solucionar o problema, bem como as capturas de pacotes

1. Configure valores mais altos para tempos limite para o servidor twamp e o respondente (por exemplo, 120s), para que as informações não expirem muito rapidamente antes da coleta.
2. Como a depuração precisa ser habilitada, certifique-se de configurar o dispositivo para enviar mensagens de log de depuração para o buffer de registro. O tamanho do buffer de registro precisa ser configurado grande o suficiente para impedir a transferência de mensagens de depuração durante o teste.
3. Certifique-se de que todos os pacotes trocados entre o dispositivo e a sonda sejam capturados (não apenas os pacotes de sonda UDP, mas também o TCP para o estabelecimento da sessão)
4. Colete os comandos listados dos dispositivos ASR9000 ou CRS, dependendo de onde os testes forem feitos:

Etapa 1. Antes de iniciar o teste a partir da sonda, colete:

- **terminal length 0**
- **show install ative sum**
- **admin show platform**
- **admin show hw-module fpd location all**
- **show run**
- **padrões ipsla twamp**

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

Etapa 2.Ative todas as depurações do Twamp no dispositivo e limpe o log.

1. iniciar a captura de pacotes
2. iniciar o teste da sonda

   Observação: isso não produzirá muitas saídas se for o único teste de twamp executado no teste.

Etapa 3.Colete esses comandos após o término do teste

- 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 initialization verbose

Solução: bit S nunca implementado no IOS-XR

De acordo com o RFC 4656, se não houver noção de sincronização externa para a origem de tempo, o bit não deve ser definido. Portanto, o bit S não é implementado na plataforma IOS-XR.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.