Dépannez le bit TWAMP S est placé inexactement

Contenu

Introduction

Ce document décrit la mesure active Protocol et l'utilisation de synchroniser le bit (bit S) pour des mesures de retard. Il décrit le supportabilty du bit S dans la plate-forme IOS-XR.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Mesure active à sens unique Protocol (OWAMP)
- Mesure active bi-directionnelle Protocol (TWAMP)
- Routeurs à services d'agrégation de la gamme Cisco ASR 9000 (ASR9000)

Composants utilisés

Les informations dans ce document sont basées sur des périphériques de Cisco ASR9000 - release IOS-XR 5.3.4.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Problème : Le bit TWAMP S est placé inexactement

Vous pouvez employer TWAMP pour mesurer unidirectionnel et des performances d'aller-retour entre deux périphériques TWAMP-pris en charge. Quand vous testez l'accord de niveau de service basé sur TWAMP d'Internet Protocol (IP SLA) entre la sonde du tiers et les périphériques CRS/ASR9000 qui fonctionne sur IOS-XR 5.3.4, le serveur TWAMP place le bit S à faux. Par conséquent, le retard à sens unique n'est pas calculé par le périphérique de sonde.

Principe fondamental TWAMP

La mesure active à sens unique Protocol (OWAMP), spécifié dans RFC4656, fournit un protocole commun pour mesurer des mesures à sens unique entre les périphériques de réseau. OWAMP peut être utilisé bidirectionnel pour mesurer des mesures à sens unique dans les deux directions entre deux éléments de réseau. Cependant, il ne facilite pas des mesures aller-retour ou bi-directionnelles.

La mesure active bi-directionnelle Protocol (TWAMP) décrit dans RFC5357, est un procédé basé sur des standards et fortement efficace de supervision des performances qui développe sur la spécification active à sens unique de Protocol de mesure (OWAMP) définie dans RFC-4656 en plus de la mesure des performances des mesures aller-retour et bi-directionnelles pour les réseaux basés par IP. TWAMP est une méthode constructeur-agnostique pour mesurer exactement unidirectionnel et des performances d'aller-retour entre deux points finaux TWAMP-pris en charge.

Selon RFC4656 (mesure active à sens unique Protocol), le premier bit **S** doit être placé, si l'interlocuteur qui génère l'horodateur a une horloge qui est synchronisée à l'UTC par une source externe.

Par exemple, le bit S doit être placé, si :

- Le matériel de système de positionnement mondial (GPS) est utilisé pour indiquer qu'il a saisi la situation actuelle et le temps.
- Le Protocole NTP (Network Time Protocol) est utilisé pour indiquer qu'il est synchronisé à une source externe, qui inclut la source de la strate 0, etc.).
- Il n'y a aucune notion de synchronisation externe pour la source temporelle, le bit S ne devrait pas être placé.

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

Les entités TWAMP :

Le système TWAMP se compose de 4 entités logiques :

- serveur - gère un ou plusieurs sessions TWAMP et configure également des ports de par-session dans les points finaux
- session-réflecteur - reflète un paquet de mesure dès qu'il recevra un paquet de test TWAMP
- contrôle-client - initie le début et l'arrêt des sessions de test TWAMP

- session-expéditeur - instancie les paquets de test TWAMP envoyés au réflecteur de session

Les protocoles TWAMP :

Le protocole TWAMP inclut trois catégories distinctes d'échange de message inclut :

- Échange de configuration de connexion

Les messages établissent un à session entre le Contrôle-client et le serveur. D'abord les identités des pairs communiqués sont établies par l'intermédiaire d'un mécanisme de réponse de défi. Le serveur envoie un défi aléatoirement généré, auquel le Contrôle-client puis envoie une réponse en chiffrant le défi utilisant une clé dérivée du secret partagé. Une fois que les identités sont établies, l'étape suivante négocie une security mode qui binded pour les commandes de TWAMP-Control ultérieures aussi bien que les paquets de flot de TWAMP-test.

Note: Un serveur peut recevoir des demandes de connexion de plusieurs clients de contrôle.

- échange de TWAMP-control

Le protocole de TWAMP-Control exécute plus de le TCP et est utilisé pour instancier et contrôler des sessions de mesure. L'ordre des commandes est comme suit, mais différent, les échanges de configuration de connexion, les commandes de TWAMP-Control peuvent être envoyés de plusieurs périodes. Cependant, les messages ne peuvent pas se produire hors de l'ordre bien que de plusieurs commandes de demande-session puissent être envoyées avant une commande de session start.
  Demande-session de ◦
  Commencement-session de ◦
  Arrêt-session de ◦

- échange de flot de TWAMP-test

Le TWAMP-test exécute plus de l'UDP et permute des paquets de TWAMP-test entre le Session-expéditeur et le Session-réflecteur. Ces paquets incluent les champs d'horodateur qui contiennent l'instant de sortie et d'entrée de paquet. En outre, chaque paquet inclut une erreur-évaluation qui indique la distorsion de synchronisation de l'expéditeur (session-expéditeur ou session-réflecteur) avec une source temporelle externe (e.g.GPS ou NTP). Le paquet inclut également un numéro de séquence.

Le TWAMP-Control et le TWAMP-test coulent, ont trois securitys mode : unauthenticated, authentifié, et chiffré.

Dépannez

Quelques Plateformes peuvent se fonder sur une certaine configuration ou déploiement pour fournir le groupe date/heure de matériel. En particulier, les Routeurs de gamme Cisco ASR9000 ont besoin de la synchronisation de Time Protocol de précision (PTP) comme clock source. Cette solution peut ne pas être disponible dans tous les scénarios d'utilisateur. Pour permettre l'utilisation d'autres sources d'estampillage de temps (clock source de NTP, par une exécution de démon sur RouteProcessor (RP)) une nouvelle configuration de **débronchement de hw-horodateur d'ipsla** est introduite pour ignorer les valeurs de groupe date/heure fournies par d'autres couches

dépendantes de plate-forme et pour revenir aux groupes date/heure indépendants de plate-forme.

Si le sync d'horloge de NTP est activé et lancé, utilisez la commande de **débronchement de hw-horodateur** dans la configuration d'IP SLA de désactiver le groupe date/heure de matériel.

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

Les notes en version pour le Routeurs à services d'agrégation de la gamme Cisco ASR 9000, la version 6.0.1 introduit une nouvelle caractéristique d'amélioration de précision TWAMP.

L'amélioration de précision TWAMP fournit la finesse de microseconde dans des mesures TWAMP. Cette amélioration permet à la collecte de groupes date/heure d'entrée et de sortie aussi près que possible au fil, pour réaliser plus de précision.

Vous pouvez améliorer la release IOS XR à 6.1.X et en haut pouvoir utiliser la caractéristique d'amélioration de précision TWAMP et vérifier la réalisation du comportement désiré.

Vous pouvez exécuter ces étapes pour dépanner la question aussi bien que les captures de paquet

1. Configurez les valeurs supérieures pour des délais d'attente pour le serveur de twamp et le responder (par exemple 120s), ainsi les informations n'expirent pas trop rapidement avant collecte.
2. Puisque le débogage doit être activé, assurez pour configurer le périphérique pour envoyer des messages de log d'élimination des imperfections au tampon de journalisation. La taille du tampon de journalisation doit être assez grande configuré pour empêcher le rouleau plus de messages d'élimination des imperfections pendant le test.
3. Esure que tous les paquets permutés entre le périphérique et la sonde sont capturé (non seulement des paquets de sonde d'UDP, mais également le TCP pour l'établissement de session)
4. Collectez les commandes énumérées des dispositifs ASR9000 ou CRS, dépendez où les tests est faits :

Étape 1. Avant que vous commenciez le test à partir de la sonde, collectez :

- **terminal length 0**
- **somme de show install active**
- **show platform d'admin**
- **emplacement tout de show hw-module fpd d'admin**
- **affichez le passage**

- normes de twamp d'ipsla
- état de twamp d'ipsla de vshow
- show ntp status
- détail de show ntp associations

Étape 2.Enable que tout le Twamp met au point sur le périphérique et puis clair le log.

1. commencez la capture de paquet
2. commencez le test à partir de la sonde

   Note: Ceci ne produit pas trop de sorties si c'est le seul test de twamp qui exécute sur la sonde.

Étape 3.Collect ces commandes après test terminé

- show log
- affichez le détail de connexion de twamp d'ipsla
- affichez les demandes de connexion de twamp d'ipsla
- affichez la session de twamp d'ipsla
- twamp de suivi d'ipsla d'exposition tout bavard
- initialisation de twamp de suivi d'ipsla d'exposition bavarde

Solution : Bit S non jamais mis en application dans IOS-XR

Selon RFC 4656, s'il n'y a aucune notion de synchronisation externe pour la source temporelle, le bit ne devrait pas être placé. Par conséquent, le bit S n'est pas mis en application dans la plate-forme IOS-XR.