Aperçu des mécanismes de keepalive sur le Cisco IOS

Contenu

Introduction

Ce document décrit les divers mécanismes de keepalive sur le Cisco IOS®.

Informations générales

Des messages de keepalive sont envoyés par un périphérique de réseau par l'intermédiaire d'un examen médical ou d'un circuit virtuel afin d'informer toujours un autre périphérique de réseau ce le circuit entre eux des fonctions. Pour que le Keepalives fonctionne il y a deux facteurs essentiels :

- L'intervalle keepalive est la durée qui s'écoule entre chaque message keepalive envoyé par un périphérique réseau. C'est toujours configurable.
- La keepalive retries est le nombre de fois que le périphérique continue à envoyer à des paquets keepalive sans réponse avant que l'état soit changé à « vers le bas ». Pour quelques types de Keepalives c'est configurable, alors que pour d'autres il y a une valeur par défaut qui ne peut pas être changée.

Mécanismes de keepalive d'interface

Interfaces Ethernet

Sur des supports de diffusion tels qu'un Ethernet, le Keepalives est légèrement seul. Puisqu'il y a beaucoup de voisins possibles sur Ethernet, le keepalive n'est pas conçu pour déterminer si le chemin à un voisin quelconque sur le câble est disponible. Il est conçu uniquement pour vérifier que le système local a un accès en lecture et en écriture au câble Ethernet lui-même. Le routeur produit un paquet Ethernet avec lui-même comme adresse MAC source et de destination et un code de type Ethernet spécial de 0x9000. Le matériel Ethernet envoie ce paquet sur le câble Ethernet, puis reçoit immédiatement ce paquet. Cela permet de vérifier le matériel d'envoi et de réception sur la carte Ethernet et l'intégrité de base du câble.

Interfaces série

Les interfaces série peuvent avoir différents types d'encapsulations et chaque type d'encapsulation détermine le genre de Keepalives qui sera utilisé.

Sélectionnez la commande de **keepalive** dans le mode de configuration d'interface afin de placer la fréquence à laquelle un routeur envoie des paquets ECHOREQ à son pair :

- Afin de restaurer le système sur l'intervalle de message de veille par défaut de 10 secondes, sélectionnez la commande de **keepalive** avec l'**aucun** mot clé.
- Afin de désactiver le Keepalives, sélectionnez la commande de **débronchement de keepalive**.

  Remarque: **keepalive** La commande s'applique aux interfaces série qui utilisent la liaison de données de haut niveau Contol (HDLC) ou l'encapsulation PPP. Il ne s'applique pas aux interfaces série qui utilisent l'Encapsulation de relais de trames.

  Remarque: Pour des types d'encapsulation de PPP et HDLC, une keepalive de zéro désactive le Keepalives et est signalée dans la **commande show running-config** sortie comme **débronchement de keepalive**.

Keepalives HDLC

Un autre mécanisme réputé de keepalive est Keepalives séquentiel pour le HDLC. Les keepalives séquentiels sont envoyés entre deux routeurs et font l'objet d'un accusé de réception. Avec l'utilisation des numéros de séquence de dépister chaque keepalive, chaque périphérique peut confirmer si c'est pair HDLC recevait la keepalive qu'il a envoyée. Pour l'encapsulation HDLC, trois Keepalives ignorés cause l'interface d'être réduite.

Permettez à la commande d'**interface série de débogage** pour une connexion HDLC afin de permettre à l'utilisateur pour voir le Keepalives qui sont générés et envoyés :

```
Sample Output:
17:21:09.685: Serial0/0: HDLC myseq 0, mineseen 0*, yourseen 1, line up
```

Le Keepalives HDLC contient trois parties afin de le déterminer fonctionne :

- Le « myseq » qui est notre propre nombre de incrémentation.
- « Mineseen » qui est réellement un accusé de réception de l'autre côté (incrémenté) qui dit qu'ils s'attendent à un ce nombre de nous.
- « Yourseen » qui est notre accusé de réception à l'autre côté.

Remarque: Quand la différence en valeurs dans le myseq et mineseen des champs dépasse trois sur le Router2, la ligne descend et l'interface est remise à l'état initial.

Puisque le Keepalives HDLC est Keepalives de type ECHOREQ, la fréquence de keepalive est importante et il est recommandé que qu'ils apparient exactement des deux côtés. Si les temporisateurs sont hors de sync, le début de numéros de séquence à sortir de la commande. Par exemple, si vous placez un côté à 10 secondes et à l'autre à 25 secondes, il permettra toujours à l'interface pour rester tant que la différence dans la fréquence n'est pas suffisante pour faire être éteints les numéros de séquence par une différence de trois.

En tant qu'une illustration de la façon dont le Keepalives HDLC fonctionne, le routeur 1 et Router2 sont directement connectés par l'intermédiaire de Serial0/0 et de Serial2/0 respectivement. Afin d'illustrer comment le Keepalives défectueux HDCL est utilisé pour dépister les états d'interface, l'interface série 0/0 sera arrêtée sur le routeur 1.

Routeur 1

```
Router1#show interfaces serial 0/0/0
Serial0/0/0 is up, line protocol is up (connected)
Hardware is HD64570
Internet address is 10.0.0.1/8
MTU 1500 bytes, BW 64 Kbit, DLY 20000 usec, rely 255/255, load 1/255
Encapsulation HDLC, loopback not set, keepalive set (10 sec)
[output is omited]

17:21:09.685: Serial0/0: HDLC myseq 0, mineseen 0*, yourseen 1, line up
17:21:19.725: Serial0/0: HDLC myseq 1, mineseen 1*, yourseen 2, line up
17:21:29.753: Serial0/0: HDLC myseq 2, mineseen 2*, yourseen 3, line up
17:21:39.773: Serial0/0: HDLC myseq 3, mineseen 3*, yourseen 4, line up
17:21:49.805: Serial0/0: HDLC myseq 4, mineseen 4*, yourseen 5, line up
17:21:59.837: Serial0/0: HDLC myseq 5, mineseen 5*, yourseen 6, line up
17:22:09.865: Serial0/0: HDLC myseq 6, mineseen 6*, yourseen 7, line up
17:22:19.905: Serial0/0: HDLC myseq 7, mineseen 7*, yourseen 8, line up
17:22:29.945: Serial0/0: HDLC myseq 8, mineseen 8*, yourseen 9, line up
Router1 (config-if)#shut
17:22:39.965: Serial0/0: HDLC myseq 9, mineseen 9*, yourseen 10, line up
17:22:42.225: %LINK-5-CHANGED: Interface Serial0/0, changed state
to administratively down

17:22:43.245: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0,
changed state to down
```

Routeur 2

```
Router2#show interfaces serial 0/0/0
Serial0/0/0 is up, line protocol is up (connected)
Hardware is HD64570
Internet address is 10.0.0.2/8
MTU 1500 bytes, BW 64 Kbit, DLY 20000 usec, rely 255/255, load 1/255
Encapsulation HDLC, loopback not set, keepalive set (10 sec)
[output is omited]


17:21:04.929: Serial2/0: HDLC myseq 0, mineseen 0, yourseen 0, line up
17:21:14.941: Serial2/0: HDLC myseq 1, mineseen 1*, yourseen 1, line up
17:21:24.961: Serial2/0: HDLC myseq 2, mineseen 2*, yourseen 2, line up
17:21:34.981: Serial2/0: HDLC myseq 3, mineseen 3*, yourseen 3, line up
17:21:45.001: Serial2/0: HDLC myseq 4, mineseen 4*, yourseen 4, line up
17:21:55.021: Serial2/0: HDLC myseq 5, mineseen 5*, yourseen 5, line up
17:22:05.041: Serial2/0: HDLC myseq 6, mineseen 6*, yourseen 6, line up
```

```
17:22:15.061: Serial2/0: HDLC myseq 7, mineseen 7*, yourseen 7, line up
17:22:25.081: Serial2/0: HDLC myseq 8, mineseen 8*, yourseen 8, line up
17:22:35.101: Serial2/0: HDLC myseq 9, mineseen 9*, yourseen 9, line up
17:22:45.113: Serial2/0: HDLC myseq 10, mineseen 10*, yourseen 10, line up
17:22:55.133: Serial2/0: HDLC myseq 11, mineseen 10, yourseen 10, line up
17:23:05.153: HD(0): Reset from 0x203758
17:23:05.153: HD(0): Asserting DTR
17:23:05.153: HD(0): Asserting DTR and RTS
17:23:05.153: Serial2/0: HDLC myseq 12, mineseen 10, yourseen 10, line up
17:23:15.173: HD(0): Reset from 0x203758
17:23:15.173: HD(0): Asserting DTR
17:23:15.173: HD(0): Asserting DTR and RTS
17:23:15.173: Serial2/0: HDLC myseq 13, mineseen 10, yourseen 10, line down
17:23:16.201: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0,
changed state to down
Router2#
17:23:25.193: Serial2/0: HDLC myseq 14, mineseen 10, yourseen 10, line down
```

Keepalives de PPP

Le Keepalives de PPP est un peu différent du Keepalives HDLC. À la différence du HDLC, le Keepalives de PPP est plutôt des pings. Les deux côtés peuvent se cingler à leurs loisirs. Le mouvement négocié approprié est de répondre TOUJOURS à ce « ping ». Ainsi pour le Keepalives de PPP, la fréquence ou la valeur de temporisateur sont seulement localement appropriée et n'ont aucune incidence de l'autre côté. Même si un côté arrête le Keepalives, il RÉPONDRA toujours à ces requêtes d'écho du côté qui a un temporisateur de keepalive. Cependant, il n'initiera jamais aucune de ses propres moyens.

Permettez à la commande de **paquet de debug ppp** pour une connexion PPP afin de permettre à l'utilisateur pour voir le Keepalives de PPP qui sont envoyés :

```
17:00:11.412: Se0/0/0 LCP-FS: I ECHOREQ [Open] id 32 len 12 magic 0x4234E325
```

et réponses qui sont reçues :

```
17:00:11.412: Se0/0/0 LCP-FS: O ECHOREP [Open] id 32 len 12 magic 0x42345A4D
```

Le Keepalives de PPP contient trois parties :

- Numéro d'ID - utilisé pour identifier au lequel ECHOREQ le pair répond.
- Type de keepalive - ECHOREQ sont Keepalives envoyé par le périphérique d'origine et ECHOREP sont des réponses envoyées par le pair.
- Nombres magiques - les notifications incluent les nombres magiques du serveur et du client distant. Le pair valide le nombre magique dans le paquet de demande d'écho LCP, et transmet le paquet de réponse d'écho correspondant LCP qui contient le nombre magique négocié par le routeur.

Pour l'encapsulation PPP, cinq Keepalives ignorés cause l'interface d'être réduite

Interfaces de tunnel GRE

Le mécanisme keepalive de tunnel GRE diffère légèrement de celui des interfaces Ethernet ou série. Il permet à une extrémité d'envoyer et de recevoir des paquets keepalives vers et en provenance d'un routeur distant même si ce dernier ne prend pas en charge les keepalives GRE. Puisque GRE est un mécanisme de transmission tunnel de paquet pour la transmission tunnel IP à l'intérieur d'IP, un paquet de tunnel IP GRE peut être construit à l'intérieur d'un autre paquet de

tunnel IP GRE. Pour les keepalives GRE, l'expéditeur préconstruit le paquet de réponse keepalive à l'intérieur du paquet de requête keepalive initial de sorte que l'extrémité distante ait uniquement besoin d'effectuer une désencapsulation GRE standard de l'en-tête IP GRE externe puis de transférer le paquet IP GRE interne. Ce mécanisme fait en sorte que la réponse keepalive transfère l'interface physique plutôt que l'interface du tunnel. Pour plus de détails sur le fonctionnement du Keepalives de tunnel GRE, voyez comment le Keepalives GRE fonctionne.

Crypto Keepalives

Keepalives d'IKE

Le Keepalives d'Échange de clés Internet (IKE) est un mécanisme utilisé pour déterminer si un homologue VPN peut haut et recevoir le trafic chiffré. Le crypto Keepalives distinct est exigé en plus des keepalives d'interface parce que des homologues VPN généralement ne sont jamais connectés de nouveau au dos, ainsi les keepalives d'interface ne fournissent pas assez d'informations au sujet de l'état de l'homologue VPN.

Sur des périphériques de Cisco IOS, le Keepalives d'IKE est activé en employant une méthode de propriété industrielle appelée Dead Peer Detection (DPD). Afin de permettre à la passerelle pour envoyer DPDs au pair, sélectionnez cette commande en mode de configuration globale :

crypto isakmp keepalive *seconds [retry-seconds]* [**periodic** | **on-demand**]

Afin de désactiver le Keepalives, utilisez « non » la forme de cette commande. Pour plus d'informations sur ce que chaque mot clé dans cette commande fait, voir le crypto isakmp keepalive. Pour plus de finesse, le Keepalives peut également être configuré sous le profil d'ISAKMP. Pour plus de détails, voir l'aperçu de profil d'ISAKMP [Cisco IOS IPsec].

Keepalives NAT

En cas de scénarios où un homologue VPN est derrière un Traduction d'adresses de réseau (NAT), le NAT-Traversal est utilisé pour le cryptage. Cependant, au cours des périodes de veille il est possible que l'entrée NAT sur le périphérique en amont pourrait chronométrer. Ceci peut poser des problèmes quand vous apportez le tunnel et NAT n'est pas bidirectionnel. Le Keepalives NAT est activé afin de maintenir le mappage NAT dynamique actif pendant une connexion entre deux pairs. Le Keepalives NAT est des paquets UDP avec une charge utile décryptée d'un octet. Bien que l'implémentation du courant DPD soit semblable au Keepalives NAT, il y a une légère différence - DPD est utilisé pour détecter l'état de pair tandis que le Keepalives NAT est envoyé si l'entité d'IPsec n'envoyait pas ou recevait le paquet à une période spécifiée. La plage valide a lieu entre 5 à 3600 secondes.

> **Conseil** : Si le Keepalives NAT est activé (par la commande **nat de keepalive de crypto isamkp**), les utilisateurs devraient s'assurer que la valeur de veille est plus courte que le temps d'expiration NAT de mappage de 20 secondes.

Pour plus d'informations sur cette caractéristique, voir la transparence NAT d'IPsec.