Panoramica dei meccanismi keepalive su Cisco IOS

Sommario

Introduzione

Questo documento descrive i vari meccanismi keepalive di Cisco IOS®.

Premesse

I messaggi keepalive vengono inviati da un dispositivo di rete tramite un circuito fisico o virtuale per comunicare a un altro dispositivo di rete che il circuito tra i due funziona ancora. Perché funzioni, i fattori essenziali sono due:

- L'intervallo keepalive è l'intervallo di tempo tra i messaggi keepalive inviati da un dispositivo di rete. Questa operazione è sempre configurabile.
- I tentativi keepalive corrispondono al numero di volte in cui il dispositivo continua a inviare pacchetti keepalive senza risposta prima che lo stato venga impostato su "down". Per alcuni tipi di pacchetti keepalive è possibile configurarlo, mentre per altri è disponibile un valore predefinito che non può essere modificato.

Meccanismi Keepalive interfaccia

Interfacce Ethernet

I pacchetti keepalive su supporti di broadcast quali Ethernet sono leggermente unici. Poiché esistono molti possibili router adiacenti sulla rete Ethernet, il comando keepalive non è progettato per determinare se è disponibile il percorso di uno specifico router adiacente sul cavo. È progettato solo per verificare che il sistema locale disponga di accesso in lettura e scrittura al cavo Ethernet stesso. Il router produce un pacchetto Ethernet con se stesso come indirizzo MAC di origine e di destinazione e un codice di tipo Ethernet speciale 0x9000. L'hardware Ethernet invia il pacchetto sul cavo Ethernet e quindi lo riceve nuovamente immediatamente. Questo controllo controlla l'hardware di invio e ricezione sulla scheda Ethernet e l'integrità di base del cavo.

Source MAC	Destination MAC	Protocol Type	Data	Layer-2 Padding
00-00-0C-04-EF-04	00-00-0C-04-EF-04	9000	0000 0100	0000 ... 0000

Interfacce seriali

Le interfacce seriali possono avere diversi tipi di incapsulamento e ciascun tipo di incapsulamento determina il tipo di pacchetti keepalive che verrà usato.

Per impostare la frequenza con cui un router invia i pacchetti ECHOREQ al proprio peer, immettere il comando **keepalive** in modalità di configurazione interfaccia:

- Per ripristinare il sistema all'intervallo keepalive predefinito di 10 secondi, immettere il comando **keepalive** con la parola chiave **no**.
- Per disabilitare l'opzione keepalive, immettere il comando **keepalive disable**.

Nota: OSPF (Open Shortest Path First) **keepalive** Questo comando viene applicato alle interfacce seriali che usano l'incapsulamento HDLC (High-Level Data Link Control) o PPP. Non è applicabile alle interfacce seriali che usano l'incapsulamento Frame Relay.

Nota: Per entrambi i tipi di incapsulamento PPP e HDLC, un keepalive pari a zero disabilita i keepalive e viene indicato nell'output del comando **show running-config** come **keepalive disable**.

Mantenimento HDLC

Un altro meccanismo keepalive conosciuto è il serial keepalive per HDLC. I pacchetti keepalive seriali vengono inviati avanti e indietro tra due router e vengono riconosciuti. Utilizzando numeri di sequenza per tenere traccia di ciascun keepalive, ciascun dispositivo è in grado di confermare se il peer HDLC ha ricevuto il keepalive inviato. Per l'incapsulamento HDLC, tre pacchetti keepalive ignorati causano la disabilitazione dell'interfaccia.

Abilitare il comando **debug serial interface** per una connessione HDLC in modo da consentire all'utente di visualizzare i pacchetti keepalive generati e inviati:

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

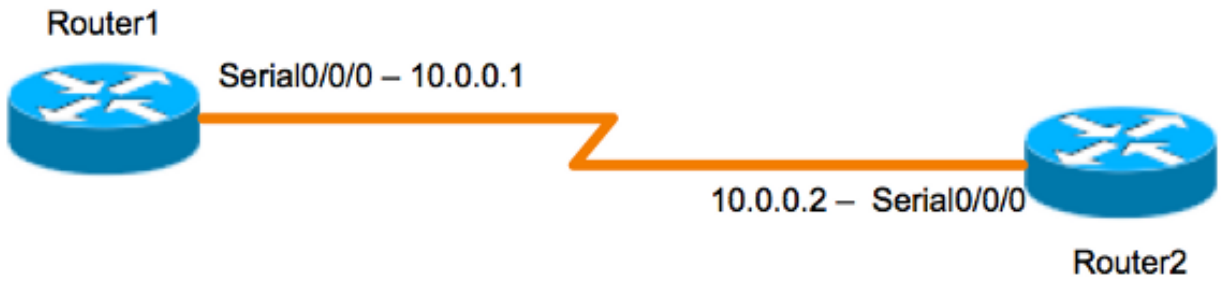
I pacchetti keepalive HDLC contengono tre elementi per determinarne il funzionamento:

- Il "myseq" che è il nostro numero crescente.
- I "mineseen" che in realtà è un riconoscimento dall'altra parte (incrementato) che dice che si aspettano questo numero da noi.
- Il "tuo visto" che è il nostro riconoscimento all'altra parte.

Nota: Quando la differenza tra i valori nei campi myseq e mineseen supera i tre sul router 2, la linea si interrompe e l'interfaccia viene reimpostata.

Poiché i keepalive HDLC sono keepalive di tipo ECHOREQ, la frequenza di keepalive è importante e si consiglia di associarli esattamente su entrambi i lati. Se i timer non sono sincronizzati, i numeri di sequenza iniziano a non funzionare. Ad esempio, se si imposta un lato su 10 secondi e l'altro su 25 secondi, l'interfaccia rimarrà attiva finché la differenza di frequenza non è sufficiente a provocare lo spegnimento dei numeri di sequenza di una differenza di tre.

A dimostrazione del funzionamento dei pacchetti keepalive HDLC, il router 1 e il router 2 sono collegati direttamente rispettivamente tramite Serial0/0 e Serial2/0. Per illustrare come i pacchetti keepalive HDCL guasti vengono usati per tenere traccia degli stati dell'interfaccia, la porta seriale 0/0 verrà chiusa sul router 1.



Router 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
```

Router 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
```

PPP keepalive

I pacchetti keepalive PPP sono leggermente diversi dai pacchetti keepalive HDLC. A differenza del protocollo HDLC, i pacchetti keepalive PPP sono più simili ai ping. Entrambe le parti possono comunicare a piacere. La mossa giusta da negoziare è di rispondere SEMPRE a questo "ping". Per i pacchetti keepalive PPP, la frequenza o il valore del timer sono solo rilevanti a livello locale e non hanno alcun impatto sull'altro lato del collegamento. Anche se un dispositivo disattiva l'invio dei pacchetti keepalive, risponderà comunque alle richieste echo provenienti dal dispositivo che dispone di un timer keepalive. Tuttavia, non inizierà mai niente di suo.

Abilitare il comando **debug ppp packet** per una connessione PPP in modo da consentire all'utente di visualizzare i pacchetti keepalive PPP inviati:

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

e risposte ricevute:

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

I pacchetti keepalive PPP contengono tre elementi:

- Numero ID: utilizzato per identificare a quale ECHOREQ risponde il peer.
- Tipo keepalive: ECHOREQ indica i pacchetti keepalive inviati dal dispositivo di origine, mentre ECHOREP indica le risposte inviate dal peer.
- Numeri magici: le notifiche includono i numeri magici del server e del client remoto. Il peer convalida il numero magico nel pacchetto di richiesta echo LCP e trasmette il pacchetto di risposta echo LCP corrispondente contenente il numero magico negoziato dal router.

Per l'incapsulamento PPP, cinque pacchetti keepalive ignorati causano la disattivazione dell'interfaccia

Interfacce tunnel GRE

Il meccanismo keepalive del tunnel GRE è leggermente diverso rispetto alle interfacce Ethernet o seriali. Offre la possibilità a un lato di originare e ricevere pacchetti keepalive da e verso un router remoto anche se il router remoto non supporta i pacchetti keepalive GRE. Poiché GRE è un meccanismo di tunneling dei pacchetti per il tunneling IP all'interno dell'IP, è possibile creare un pacchetto del tunnel GRE IP all'interno di un altro pacchetto del tunnel GRE IP. Per i pacchetti keepalive GRE, il mittente pre-crea il pacchetto di risposta keepalive all'interno del pacchetto di richiesta keepalive originale, in modo che l'estremità remota debba solo eseguire la decapsulamento GRE standard dell'intestazione IP GRE esterna e inoltrare il pacchetto GRE IP interno. Questo meccanismo fa sì che la risposta keepalive venga inoltrata sull'interfaccia fisica anziché sull'interfaccia del tunnel. Per ulteriori informazioni sul funzionamento dei pacchetti keepalive del tunnel GRE, vedere Funzionamento dei pacchetti keepalive del GRE.

Crypto Keepalives

IKE keepalive

I pacchetti keepalive IKE (Internet Key Exchange) sono un meccanismo utilizzato per determinare se un peer VPN è attivo e in grado di ricevere traffico crittografato. I pacchetti keepalive di crittografia separati sono richiesti in aggiunta ai pacchetti keepalive dell'interfaccia, perché i peer VPN in genere non sono mai connessi all'indietro, quindi i pacchetti keepalive dell'interfaccia non forniscono informazioni sufficienti sullo stato del peer VPN.

Sui dispositivi Cisco IOS, i pacchetti keepalive IKE sono abilitati dall'uso di un metodo proprietario chiamato Dead Peer Detection (DPD). Per consentire al gateway di inviare DPD al peer, immettere questo comando in modalità di configurazione globale:

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

Per disabilitare l'opzione keepalive, usare la forma "no" di questo comando. Per ulteriori informazioni sull'azione di ciascuna parola chiave del comando, vedere crypto isakmp keepalive. Per una maggiore granularità, i pacchetti keepalive possono essere configurati anche nel profilo ISAKMP. Per ulteriori informazioni, vedere Cenni preliminari sul profilo ISAKMP [Cisco IOS IPsec].

NAT Keepalives

In caso di scenari in cui un peer VPN si trova dietro un Network Address Translation (NAT), per la crittografia viene utilizzato NAT-Traversal. Tuttavia, durante i periodi di inattività, è possibile che la voce NAT nel dispositivo a monte si blocchi. Ciò può causare problemi quando si richiama il tunnel e NAT non è bidirezionale. I pacchetti keepalive NAT vengono abilitati per mantenere attiva la mappatura NAT dinamica durante una connessione tra due peer. I pacchetti keepalive NAT sono pacchetti UDP con un payload non crittografato di un byte. Sebbene l'implementazione DPD corrente sia simile ai pacchetti keepalive NAT, esiste una leggera differenza - la DPD viene utilizzata per rilevare lo stato del peer mentre i pacchetti keepalive NAT vengono inviati se l'entità IPsec non ha inviato o ricevuto il pacchetto in un periodo di tempo specificato. L'intervallo valido è compreso tra 5 e 3600 secondi.

> **Suggerimento**: Se i pacchetti keepalive NAT sono abilitati (tramite il comando **crypto isamkp nat** keepalive), gli utenti devono verificare che il valore di inattività sia inferiore al tempo di scadenza del mapping NAT di 20 secondi.

Per ulteriori informazioni su questa funzionalità, vedere Trasparenza NAT IPSec.