Übersicht über Keepalive-Mechanismen in Cisco IOS

Inhalt

Einführung

Dieses Dokument beschreibt die verschiedenen Keepalive-Mechanismen auf Cisco IOS®.

Hintergrundinformationen

Keepalive-Nachrichten werden von einem Netzwerkgerät über eine physische oder virtuelle Leitung gesendet, um einem anderen Netzwerkgerät mitzuteilen, dass die Verbindung zwischen ihnen weiterhin funktioniert. Für Keepalives gibt es zwei wesentliche Faktoren:

- Das Keepalive-Intervall ist der Zeitraum zwischen den einzelnen Keepalive-Nachrichten, die von einem Netzwerkgerät gesendet werden. Dies ist immer konfigurierbar.
- Der Keepalive-Versuch ist die Anzahl der Versuche, die das Gerät weiterhin ohne Antwort Keepalive-Pakete sendet, bevor der Status auf "Down" (Herunterfahren) geändert wird. Für einige Keepalives ist dies konfigurierbar, für andere gibt es einen Standardwert, der nicht geändert werden kann.

Schnittstellenwahren-Mechanismen

Ethernet-Schnittstellen

Bei Sendemedien wie Ethernet sind Keepalives etwas einzigartig. Da das Ethernet viele mögliche Nachbarn enthält, ist der Keepalive nicht darauf ausgelegt, festzustellen, ob der Pfad zu einem bestimmten Nachbarn des Kabels verfügbar ist. Es ist nur so konzipiert, dass das lokale System über Lese- und Schreibzugriff auf das Ethernet-Kabel selbst verfügt. Der Router erstellt ein Ethernet-Paket mit sich selbst als Quell- und Ziel-MAC-Adresse und einem speziellen Ethernet-Typcode von 0x9000. Die Ethernet-Hardware sendet dieses Paket an das Ethernet-Kabel und empfängt dieses Paket dann sofort wieder zurück. Dadurch wird die Sende- und Empfangshardware des Ethernet-Adapters und die grundlegende Integrität des Kabels überprüft.

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

Serielle Schnittstellen

Serielle Schnittstellen können verschiedene Arten von Kapselungen aufweisen, und jeder Kapselungstyp bestimmt die Art der zu verwendenden Keepalives.

Geben Sie den **Keepalive-**Befehl im Schnittstellenkonfigurationsmodus ein, um die Häufigkeit festzulegen, mit der ein Router ECHOREQ-Pakete an seinen Peer sendet:

- Um das System auf das Standard-Keepalive-Intervall von 10 Sekunden zurückzusetzen, geben Sie den Befehl **keepalive** mit dem **no-**Schlüsselwort ein.
- Um Keepalives zu deaktivieren, geben Sie den Befehl **keepalive disable ein**.

Hinweis: Die **keepalive** -Befehl bezieht sich auf serielle Schnittstellen, die High-Level Data Link Control (HDLC) oder PPP-Kapselung verwenden. Sie gilt nicht für serielle Schnittstellen, die Frame-Relay-Kapselung verwenden.

Hinweis: Sowohl für PPP- als auch für HDLC-Kapselungstypen deaktiviert ein Keepalive von 0 Keepalives und wird in der Ausgabe des Befehls **show running-config** als **keepalive disable** gemeldet.

HDLC-Keepalives

Ein weiterer bekannter Keepalive-Mechanismus sind serielle Keepalives für HDLC. Serielle Keepalives werden zwischen zwei Routern hin und her gesendet, und die Keepalives werden bestätigt. Durch die Verwendung von Sequenznummern zur Verfolgung der Keepalive-Vorgänge kann jedes Gerät bestätigen, ob es den von ihm gesendeten Keepalive-Empfang empfangen hat. Bei der HDLC-Kapselung werden drei ignorierte Keepalives zum Herunterfahren der Schnittstelle führen.

Aktivieren Sie den Befehl **für die serielle Debugschnittstelle** für eine HDLC-Verbindung, damit der Benutzer Keepalives sehen kann, die generiert und gesendet werden:

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

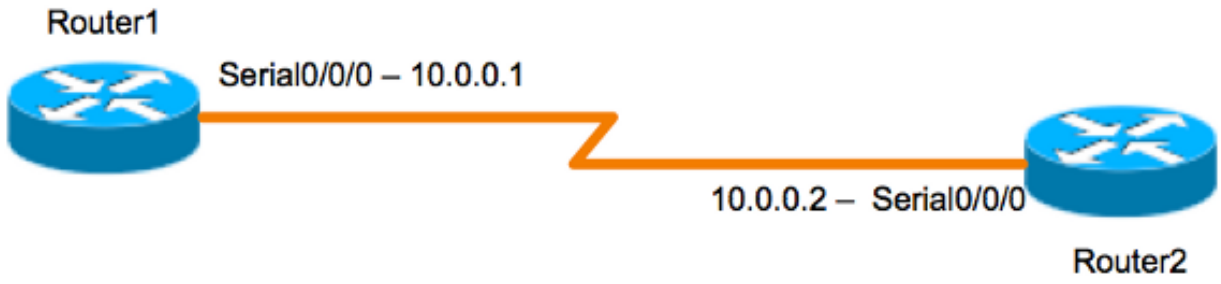
HDLC-Keepalives enthalten drei Teile, um festzustellen, ob sie funktionieren:

- Der "myseq" ist unsere eigene inkrementelle Zahl.
- Die "Bergleute", die eigentlich eine Anerkennung von der anderen Seite (erhöht), die sagt, sie erwarten diese Zahl von uns.
- Das "Ihre gesehen" ist unsere Anerkennung auf der anderen Seite.

Hinweis: Wenn die Differenz zwischen den Werten in den Feldern myseq und mineseen auf Router 2 drei überschreitet, wird die Leitung unterbrochen und die Schnittstelle zurückgesetzt.

Da es sich bei HDLC-Keepalives um Keepalives vom Typ ECHOREQ handelt, ist die Keepalive-Frequenz wichtig, und es wird empfohlen, dass sie genau auf beiden Seiten übereinstimmen. Wenn die Timer nicht synchronisiert sind, gehen die Sequenznummern aus der Reihenfolge. Wenn Sie beispielsweise eine Seite auf 10 Sekunden und die andere auf 25 Sekunden einstellen, bleibt die Schnittstelle so lange verfügbar, wie die Frequenzdifferenz nicht ausreicht, um die Sequenznummern um einen Unterschied von drei zu deaktivieren.

Zur Veranschaulichung der Funktionsweise von HDLC-Keepalives werden Router 1 und Router 2 direkt über Serial0/0 bzw. Serial2/0 verbunden. Um zu veranschaulichen, wie die Schnittstellenzustände mithilfe von ausgefallenen HDCL-Keepalives überwacht werden, wird die serielle 0/0 auf Router 1 deaktiviert.



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-Keepalives

PPP-Keepalives unterscheiden sich etwas von HDLC-Keepalives. Im Gegensatz zu HDLC sind PPP-Keepalives eher Pings. Beide Seiten können sich frei pingen. Der richtige ausgehandelte Schritt ist, IMMER auf diesen "Ping" zu antworten. Für PPP-Keepalives sind die Frequenz oder der Timer-Wert also nur lokal relevant und haben keine Auswirkungen auf die andere Seite. Selbst wenn eine Seite die Keepalives ausschaltet, reagiert sie weiterhin auf die Echo-Anfragen von der Seite, die über einen Keepalive-Timer verfügen. Sie wird jedoch niemals selbst eine Initiative einleiten.

Aktivieren Sie den Befehl **debug ppp packet** für eine PPP-Verbindung, damit der Benutzer die gesendeten PPP-Keepalives sehen kann:

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

und eingegangenen Antworten:

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

PPP-Keepalives enthalten drei Teile:

- ID-Nummer - wird verwendet, um herauszufinden, auf welche ECHOREQ der Peer reagiert.
- Keepalive-Typ - ECHOREQ sind Keepalives, die vom ursprünglichen Gerät gesendet werden, und ECHOREP sind Antworten, die vom Peer gesendet werden.
- Magische Zahlen: Die Benachrichtigungen enthalten die magischen Nummern des Servers und des Remote-Clients. Der Peer validiert die magische Nummer im LCP-Echo-Request-Paket und überträgt das entsprechende LCP-Echo-Reply-Paket, das die vom Router ausgehandelte magische Nummer enthält.

Bei der PPP-Kapselung werden fünf ignorierte Keepalives zum Herunterfahren der Schnittstelle führen.

GRE-Tunnelschnittstellen

Der GRE-Tunnel-Keepalive-Mechanismus unterscheidet sich geringfügig von Ethernet- oder seriellen Schnittstellen. Dadurch kann eine Seite Keepalive-Pakete an einen Remote-Router senden und von diesem empfangen, selbst wenn der Remote-Router keine GRE-Keepalives unterstützt. Da GRE ein Pakettunnelmechanismus für das Tunneling von IP innerhalb von IP ist, kann ein GRE-IP-Tunnelpaket in einem anderen GRE-IP-Tunnelpaket erstellt werden. Bei GRE-Keepalives erstellt der Sender das Keepalive-Antwortpaket im ursprünglichen Keepalive-Anforderungspaket vorab, sodass das Remote-Ende nur die standardmäßige GRE-Entkapselung des äußeren GRE-IP-Headers durchführen und anschließend das innere IP-GRE-Paket weiterleiten muss. Dieser Mechanismus bewirkt, dass die Keepalive-Reaktion die physische Schnittstelle und nicht die Tunnelschnittstelle weiterleitet. Weitere Informationen zum Arbeiten von GRE-Tunnel-Keepalives finden Sie unter Funktionsweise von GRE-Keepalives.

Krypto-Keepalives

IKE-Keepalives

IKE-Keepalives (Internet Key Exchange) (IKE-Keepalives) dienen dazu, festzustellen, ob ein VPN-Peer aktiv ist und verschlüsselten Datenverkehr empfangen kann. Zusätzlich zu den Schnittstellenkepaliven sind separate Krypto-Keepalives erforderlich, da VPN-Peers in der Regel nie wieder zurück verbunden sind. Schnittstellenkeepalives liefern daher nicht genügend Informationen über den Zustand des VPN-Peers.

Auf Cisco IOS-Geräten werden IKE-Keepalives durch die Verwendung einer proprietären Methode namens Dead Peer Detection (DPD) aktiviert. Geben Sie den folgenden Befehl im globalen Konfigurationsmodus ein, damit das Gateway DPDs an den Peer senden kann:

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

Um Keepalives zu deaktivieren, verwenden Sie die Form "no" dieses Befehls. Weitere Informationen darüber, was jedes Schlüsselwort in diesem Befehl tut, finden Sie unter crypto isakmp keepalive. Für mehr Detailgenauigkeit können die Keepalives auch unter dem ISAKMP-Profil konfiguriert werden. Weitere Informationen finden Sie unter ISAKMP Profile Overview [Cisco

IOS IPsec].

NAT-Keepalives

In Szenarien, in denen ein VPN-Peer hinter einer Network Address Translation (NAT) steht, wird NAT-Traversal für die Verschlüsselung verwendet. Während Leerlaufzeiten ist es jedoch möglich, dass der NAT-Eintrag auf dem Upstream-Gerät das Timeout erreicht. Dies kann Probleme verursachen, wenn Sie den Tunnel öffnen, und NAT ist nicht bidirektional. NAT-Keepalives werden aktiviert, um die dynamische NAT-Zuordnung während einer Verbindung zwischen zwei Peers aufrecht zu erhalten. NAT-Keepalives sind UDP-Pakete mit einer unverschlüsselten Nutzlast von einem Byte. Obwohl die aktuelle DPD-Implementierung mit NAT-Keepalives vergleichbar ist, gibt es einen geringfügigen Unterschied: Mit DPD wird der Peer-Status erkannt, während NAT-Keepalives gesendet werden, wenn die IPsec-Einheit das Paket nicht zu einem bestimmten Zeitpunkt gesendet oder empfangen hat. Der gültige Bereich liegt zwischen 5 und 3600 Sekunden.

> **Tipp**: Wenn NAT-Keepalives aktiviert sind (über den Befehl **crypto isamkp nat-Keepalive**), sollten Benutzer sicherstellen, dass der Wert im Leerlauf kürzer ist als die Ablaufzeit der NAT-Zuordnung von 20 Sekunden.

Weitere Informationen zu dieser Funktion finden Sie unter IPsec NAT Transparency.