Cisco IOS でのキープアライブ メカニズムの概要

内容

[概要](#)
[背景説明](#)
[インターフェイスのキープアライブ メカニズム](#)
[イーサネット インターフェイス](#)
[シリアル インターフェイス](#)
[HDLC キープアライブ](#)
[PPP キープアライブ](#)
[GRE トンネル インターフェイス](#)
[暗号化キープアライブ](#)
[IKE キープアライブ](#)
[NAT キープアライブ](#)

概要

このドキュメントでは、Cisco IOS® のさまざまなキープアライブ メカニズムについて説明します。

背景説明

1 つのネットワーク デバイスから物理回線または仮想回線を介してキープアライブ メッセージを送信することで、別のネットワーク デバイスとの間の回線が引き続き機能していることをそのデバイスに通知します。キープアライブが機能するには、2 つの重要な要素があります。

- キープアライブの間隔とは、ネットワーク デバイスから送られる各キープアライブ メッセージ間の時間を指します。これはいつでも設定できます。
- キープアライブのリトライとは、状態が「ダウン」に変更される前に、応答がなくてもデバイスがキープアライブ パケットを送信し続ける回数のことです。 これは、一部のタイプのキープアライブでは設定可能ですが、その他のタイプではデフォルト値を変更できません。

インターフェイスのキープアライブ メカニズム

イーサネット インターフェイス

イーサネットなどのブロードキャスト メディアでは、やや独特なキープアライブがあります。イ

ーサネット上では、想定される隣接ルータが多数あるため、回線上のある特定の隣接ルータへのパスが使用可能かどうかを判定する目的ではキープアライブは設計されていません。単に、ローカル システムにイーサネット ワイヤ自体への読み取り/書き込みアクセスがあることを確認するためにのみ設計されています。ルータは、自身を送信元と宛先のMACアドレスとし、特別なイーサネットタイプコード0x9000を持つイーサネットパケットを生成します。イーサネットハードウェアはこのパケットをイーサネットワイヤに送信し、すぐに再び受信します。これによって、イーサネット アダプタ上の送受信ハードウェアと、回線の状態をチェックします。

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

シリアル インターフェイス

シリアル インターフェイスではさまざまなタイプのカプセル化を設定でき、それぞれのタイプのカプセル化で、使用するキープアライブの種類が決まります。

ルータがピアに ECHOREQ パケットを送信する頻度を設定するには、インターフェイス設定モードで keepalive コマンドを入力します。

- システムを 10 秒のデフォルト キープアライブ インターバルに戻すには、keepalive コマンドを no キーワードとともに入力します。
- キープアライブをディセーブルにするには、keepalive disable コマンドを入力します。

注：「 keepalive コマンドは、ハイレベルデータリンクコントロール(HDLC)またはPPPカプセル化を使用するシリアルインターフェイスに適用されます。フレーム リレー カプセル化を使用するシリアル インターフェイスには適用されません。

注：PPP と HDLC のカプセル化タイプでは、キープアライブ 0 によってキープアライブがディセーブルになり、show running-config コマンド出力で keepalive disable としてそれが報告されます。

HDLC キープアライブ

普及している別のキープアライブ メカニズムとして、HDLC のシリアル キープアライブがあります。シリアル キープアライブは 2 台のルータ間で相互に送信され、確認応答されます。各キープアライブを追跡するためにシーケンス番号を使用することにより、各デバイスは、自分が送信したキープアライブを HDLC ピアが受信したかどうか確認できます。HDLC カプセル化の場合、無視されるキープアライブが 3 つあると、インターフェイスがダウン状態になります。

生成され送信されたキープアライブをユーザが確認できるようにするには、HDLC 接続に対する **debug serial interface コマンドをイネーブルにします。**

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

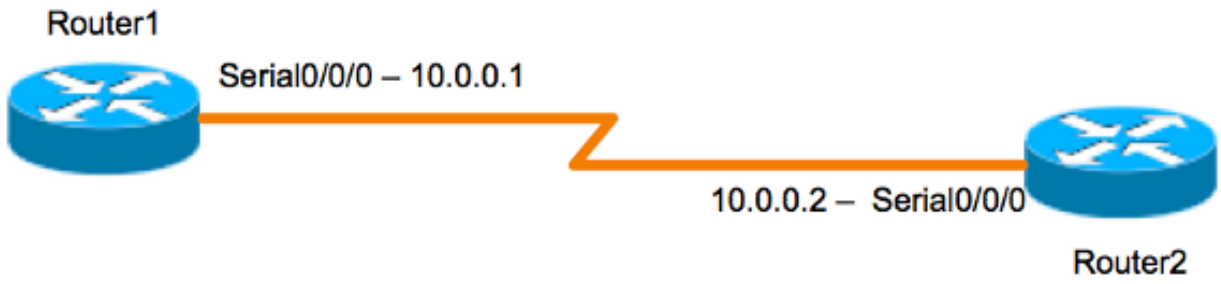
HDLC キープアライブが機能していることを判断できる 3 つの要素がこのキープアライブに含まれています。

- 「myseq」：こちら側の独自の、増加していく数値。
- 「mineseen」：こちら側にこの数値を期待すると相手側から通知してくる確認応答（増加していきます）。
- 「yourseen」：こちら側から相手側への確認応答。

注：Router 2 で myseq フィールドと mineseen フィールドの値の差が 3 を超えると、回線がダウンし、インターフェイスがリセットされます。

HDLC キープアライブは ECHOREQ タイプのキープアライブであるため、キープアライブ頻度は重要であり、両側で正確に一致していることが推奨されます。 タイマーが同期されていない場合、シーケンス番号の順序が狂い始めます。たとえば、一方を 10 秒に、もう一方を 25 秒に設定した場合、シーケンス番号が 3 つずれるほど頻度の差が大きくならない限り、インターフェイスは立ち上がった状態を保つことができます。

HDLC キープアライブがどのように機能するかを示す図にあるように、Router 1 と Router 2 がそれぞれ Serial0/0 と Serial2/0 を介して直接接続されています。失敗した HDCL キープアライブを使ってインターフェイスの状態を追跡する方法を示すために、Router 1 で Serial 0/0 がシャットダウンされるとします。



ルータ 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
```

ルータ 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 キープアライブ

PPP キープアライブは HDLC キープアライブとは少し異なります。PPP キープアライブは、HDLC ではなく ping に似ています。両側で、都合の良いときに相互に ping を実行できます。動作が正しくネゴシエートされると、この「ping」に常に応答します。 したがって、PPP キープアライブでは、頻度やタイマー値はローカルにのみ意味を持ち、相手側には影響しません。一方の側でキープアライブをオフにしても、キープアライブ タイマーが機能している側からのエコー要求に引き続き応答します。ただし、自分の側からは何も開始しません。

送信される PPP キープアライブをユーザが確認できるようにするには、PPP 接続に対する **debug ppp packet コマンドをイネーブルにします。**

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

受信される応答：

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

PPP キープアライブには次の 3 つの部分が含まれています。

- ID 番号 - ピアがどの ECHOREQ に応答するかを識別するために使用されます。
- キープアライブ タイプ - ECHOREQ は発信側デバイスから送られたキープアライブ、ECHOREP はピアから送信された応答です。
- マジック ナンバー - 通知には、サーバとリモート クライアントの両方のマジック ナンバーが含まれています。ピアは LCP Echo-Request パケット内のマジック ナンバーを検証し、ルータによってネゴシエートされたマジック ナンバーを含む LCP Echo-Reply パケットを送信します。

PPP カプセル化の場合、5 つのキープアライブが無視されると、インターフェイスがダウン状態になります。

GRE トンネル インターフェイス

GRE トンネルのキープアライブ メカニズムは、イーサネット インターフェイスやシリアル インターフェイスの場合とやや異なります。リモート ルータが GRE キープアライブをサポートしていない場合でも、こちら側とリモート ルータとの間でキープアライブ パケットを発信および受信することができます。GRE は IP 内で IP をトンネリングするパケット トンネリング メカニズムなので、別の GRE IP トンネル パケットの内部に GRE IP トンネル パケットを構築できます。GRE キープアライブでは、送信側が元のキープアライブ要求パケット内にキープアライブ応答パケットを事前に作成します。したがって、リモート エンドは外部 GRE IP ヘッダーの標準 GRE カプセル化解除を行い、内部 IP GRE パケットを転送するだけです。このメカニズムにより、キープアライブの応答はトンネル インターフェイスではなく物理インターフェイスに転送されます。GRE トンネル キープアライブの動作方法の詳細については、「GRE キープアライブの動作方法」を参照してください。

暗号化キープアライブ

IKE キープアライブ

Internet Key Exchange（IKE）キープアライブは、VPN ピアが起動していて暗号化トラフィックを受信できる状態にあること判別するために使われるメカニズムです。VPN ピアは通常、バックツーバックで接続されず、インターフェイス キープアライブは VPN ピアの状態について十分な情報を提供しないため、インターフェイスのキープアライブに加えて別の暗号化キープアライブが必要です。

Cisco IOS デバイスでは、Dead Peer Detection（DPD）という独自の方式を使用して IKE キープアライブがイネーブルになります。 ゲートウェイがピアに DPD を送信できるようにするには、グローバル設定モードで次のコマンドを入力します。

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

キープアライブをディセーブルにするには、このコマンドの "no" 形式を使用します。このコマンドの各キーワードの詳細については、「ISAKMP 暗号化キープアライブ」を参照してください。さらに、ISAKMP プロファイルでキープアライブをより細かく設定することもできます。詳細については、「ISAKMP プロファイルの概要 [Cisco IOS IPsec]」を参照してください。

NAT キープアライブ

一方の VPN ピアがネットワーク アドレス変換（NAT）の背後にあるシナリオの場合、暗号化のために NAT トラバーサルが使用されます。ただし、アイドル時間中に、アップストリーム デバイスの NAT エントリがタイムアウトする可能性があります。これが原因で、トンネルを起動する際に NAT が双方向にならないという問題が生じる可能性があります。2 つのピア間の接続時にダイナミック NAT マッピングをアライブに保つために、NAT キープアライブがイネーブルにされます。NAT キープアライブは、1 バイトの非暗号化ペイロードを持つ UDP パケットです。現在の DPD 実装は NAT キープアライブに似ていますが、わずかな違いがあります。DPD はピアのステータスを検出するために使用されます。これに対して NAT キープアライブは、指定された期間に IPSec エンティティがパケットを送信/受信しない場合に送信されます。有効な範囲は 5 ~ 3600 秒です。

> **ヒント：（crypto isamkp nat keepalive コマンドを使用して）NAT キープアライブをイネーブルにする場合、ユーザは、アイドル値を NAT マッピング有効期間（20 秒）より小さくする必要があります。**

この機能の詳細については、「IPSec の NAT 透過性」を参照してください。