Visão geral dos mecanismos de manutenção de atividade no Cisco IOS

Contents

Introduction

Este documento descreve os vários mecanismos de keepalive no Cisco IOS®.

Informações de Apoio

As mensagens de manutenção de atividade são enviadas por um dispositivo de rede através de um circuito físico ou virtual para informar a outro dispositivo de rede que o circuito entre eles ainda funciona. Para os keepalives funcionarem, há dois fatores essenciais:

- O intervalo de keepalive é o período de tempo entre cada mensagem de keepalive enviada por um dispositivo de rede. Isso é sempre configurável.
- As novas tentativas de keepalive são o número de vezes que o dispositivo continua a enviar pacotes de keepalive sem resposta antes que o estado seja alterado para "desativado". Para alguns tipos de manutenções de atividade, isso é configurável, enquanto para outros há um valor padrão que não pode ser alterado.

Mecanismos de manutenção de atividade da interface

Interfaces de Ethernet

Em meios de transmissão como uma Ethernet, os keepalives são um pouco exclusivos. Como há muitos vizinhos possíveis na Ethernet, o keepalive não foi projetado para determinar se o caminho para qualquer vizinho específico no fio está disponível. Ele foi projetado apenas para verificar se o sistema local tem acesso de leitura e gravação ao próprio fio Ethernet. O roteador produz um pacote Ethernet com ele mesmo como o endereço MAC de origem e de destino e um código do tipo Ethernet especial de 0x9000. O hardware Ethernet envia esse pacote para o fio Ethernet e recebe imediatamente esse pacote de volta. Isso verifica o hardware de envio e recebimento no adaptador Ethernet e a integridade básica do fio.

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

Interfaces seriais

As interfaces seriais podem ter diferentes tipos de encapsulamento e cada tipo de encapsulamento determina o tipo de manutenção de atividade que será usada.

Insira o comando **keepalive** no modo de configuração de interface para definir a frequência na qual um roteador envia pacotes ECHOREQ ao seu peer:

- Para restaurar o sistema para o intervalo de keepalive padrão de 10 segundos, insira o comando **keepalive** com a palavra-chave **no**.
- Para desativar keepalives, insira o comando **keepalive disable**.

Note: O **keepalive** aplica-se às interfaces seriais que usam HDLC (High-Level Data Link Control) ou encapsulamento PPP. Ele não se aplica às interfaces seriais que usam o encapsulamento Frame Relay.

Note: Para os tipos de encapsulamento PPP e HDLC, uma keepalive de zero desativa keepalives e é relatada na saída do comando **show running-config** como **keepalive disable**.

Keepalives HDLC

Outro mecanismo de keepalive conhecido é o serial keepalives para HDLC. Os keepalives seriais são enviados entre dois roteadores e os keepalives são confirmados. Com o uso de números de sequência para rastrear cada keepalive, cada dispositivo é capaz de confirmar se é o par HDLC que recebeu o keepalive que enviou. Para o encapsulamento HDLC, três keepalives ignorados fazem com que a interface seja desativada.

Ative o comando **debug serial interface** para uma conexão HDLC para permitir que o usuário veja keepalives gerados e enviados:

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

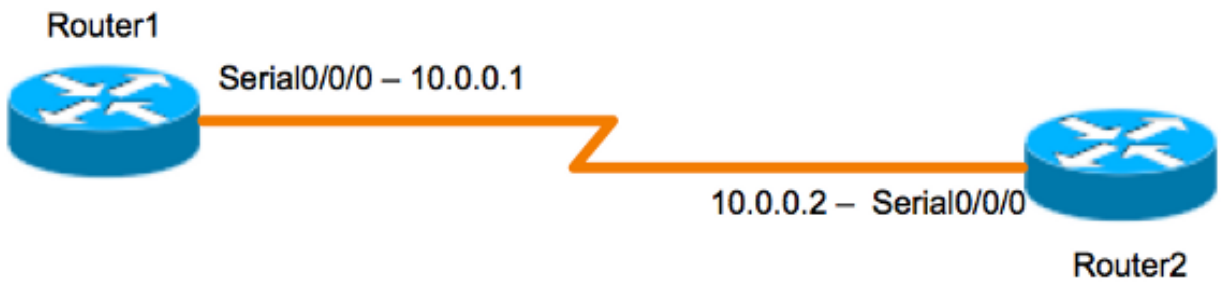
Os keepalives HDLC contêm três partes para determinar se funciona:

- O "myseq" que é o nosso próprio número crescente.
- A "mineseen", que é na verdade um reconhecimento do outro lado (incrementado) que diz que eles esperam esse número de nós.
- O "você viu" que é nosso reconhecimento para o outro lado.

Note: Quando a diferença nos valores nos campos myseq e mineseen excede três no Roteador 2, a linha fica inativa e a interface é redefinida.

Como os keepalives HDLC são keepalives do tipo ECHOREQ, a frequência de keepalive é importante e é recomendável que eles correspondam exatamente em ambos os lados. Se os temporizadores estiverem dessincronizados, os números de sequência começam a ficar fora de ordem. Por exemplo, se você definir um lado como 10 segundos e o outro como 25 segundos, ainda permitirá que a interface permaneça ativa enquanto a diferença na frequência não for suficiente para fazer com que os números de sequência fiquem desligados por uma diferença de três.

Como uma ilustração de como os keepalives do HDLC funcionam, o Roteador 1 e o Roteador 2 são conectados diretamente via Serial0/0 e Serial2/0, respectivamente. Para ilustrar como keepalives HDCL com falha são usados para rastrear os estados da interface, Serial 0/0 será desligado no Roteador 1.



Roteador 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
```

Roteador 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 do PPP

Os keepalives PPP são um pouco diferentes dos keepalives HDLC. Ao contrário do HDLC, os keepalives PPP são mais parecidos com pings. Os dois lados podem fazer ping entre si quando quiserem. A mudança negociada apropriada é SEMPRE responder a esse "ping". Assim, para keepalives PPP, a frequência ou o valor do temporizador são relevantes apenas localmente e não têm impacto no outro lado. Mesmo que um lado desligue os keepalives, ele ainda RESPONDERÁ às solicitações de eco do lado que tem um temporizador keepalive. No entanto, nunca iniciará nenhum dos seus.

Ative o comando **debug ppp packet** para uma conexão PPP para permitir que o usuário veja os keepalives PPP enviados:

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

e respostas recebidas:

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

Os keepalives PPP contêm três partes:

- Número de ID - usado para identificar a qual ECHOREQ o peer responde.
- Tipo de manutenção de atividade - ECHOREQ são keepalives enviados pelo dispositivo de origem e ECHOREP são respostas enviadas pelo peer.
- Magic numbers - as notificações incluem os números mágicos do servidor e do cliente remoto. O peer valida o número mágico no pacote LCP Echo-Request e transmite o pacote LCP Echo-Reply correspondente que contém o número mágico negociado pelo roteador.

Para o encapsulamento PPP, cinco keepalives ignorados fazem com que a interface seja desativada

Interfaces de túnel GRE

O mecanismo de keepalive do túnel GRE é um pouco diferente do das interfaces Ethernet ou seriais. Ele permite que um lado origine e receba pacotes keepalive de e de um roteador remoto, mesmo que o roteador remoto não suporte keepalives GRE. Como o GRE é um mecanismo de tunelamento de pacotes para tunelamento de IP dentro do IP, um pacote de túnel IP GRE pode ser construído dentro de outro pacote de túnel IP GRE. Para keepalives GRE, o remetente preconstrói o pacote de resposta keepalive dentro do pacote de solicitação keepalive original para que a extremidade remota só precise fazer o desencapsulamento GRE padrão do cabeçalho IP GRE externo e depois encaminhar o pacote GRE IP interno. Esse mecanismo faz com que a resposta de keepalive encaminhe a interface física em vez da interface de túnel. Para obter mais detalhes sobre o funcionamento dos keepalives de túnel GRE, consulte Como os Keepalives GRE funcionam.

Cripto Keepalives

Keepalives IKE

Os keepalives Internet Key Exchange (IKE) são um mecanismo usado para determinar se um peer VPN está ativo e pode receber tráfego criptografado. Os keepalives de criptografia separados são necessários além dos keepalives de interface porque os peers de VPN geralmente nunca são conectados de volta a trás, portanto os keepalives de interface não fornecem informações suficientes sobre o estado do peer de VPN.

Nos dispositivos Cisco IOS, os keepalives IKE são ativados pelo uso de um método proprietário chamado Dead Peer Detection (DPD). Para permitir que o gateway envie DPDs ao peer, insira este comando no modo de configuração global:

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

Para desativar keepalives, use a forma "no" deste comando. Para obter mais informações sobre o que cada palavra-chave neste comando faz, consulte crypto isakmp keepalive. Para maior granularidade, os keepalives também podem ser configurados no perfil ISAKMP. Para obter mais detalhes, consulte Visão geral do perfil ISAKMP [Cisco IOS IPsec].

Keepalives de NAT

No caso de cenários em que um peer VPN está por trás de uma Network Address Translation (NAT), a NAT-Traversal é usada para criptografia. No entanto, durante os períodos ociosos, é possível que a entrada NAT no dispositivo de upstream tenha tempo limite. Isso pode causar problemas quando você ativa o túnel e o NAT não é bidirecional. Os keepalives NAT são ativados para manter o mapeamento NAT dinâmico ativo ativo durante uma conexão entre dois pares. Os keepalives NAT são pacotes UDP com um payload não criptografado de um byte. Embora a implementação atual de DPD seja semelhante à manutenção de atividade de NAT, há uma pequena diferença - o DPD é usado para detectar o status de peer enquanto os keepalives de NAT são enviados se a entidade de IPsec não enviou ou recebeu o pacote em um período especificado. O intervalo válido é entre 5 e 3600 segundos.

> **Tip**: Se os keepalives NAT estiverem ativados (através do comando **crypto isamkp nat keepalive**), os usuários devem assegurar que o valor ocioso seja menor que o tempo de expiração do mapeamento NAT de 20 segundos.

Para obter mais informações sobre este recurso, consulte Transparência NAT IPsec.