Cisco IOS의 Keepalive 메커니즘 개요

목차

소개

이 문서에서는 Cisco IOS®의 다양한 keepalive 메커니즘에 대해 설명합니다.

배경 정보

Keepalive 메시지는 다른 네트워크 디바이스에서 상호 회로가 여전히 작동하고 있음을 알리기 위해 물리적 또는 가상 회로를 통해 한 네트워크 디바이스에서 전송됩니다.업무 유지를 위해 두 가지 필수 요소가 있습니다.

- keepalive 간격은 네트워크 디바이스에서 전송하는 각 keepalive 메시지 간의 기간입니다.이는 항상 구성 가능합니다.
- keepalive retries는 상태가 "down"으로 변경되기 전에 디바이스가 응답 없이 keepalive 패킷을 계속 전송하는 횟수입니다. 일부 유형의 keepalive는 이 구성 가능하지만 다른 유형의 경우 변경할 수 없는 기본값이 있습니다.

인터페이스 Keepalive 메커니즘

이더넷 인터페이스

이더넷과 같은 브로드캐스트 미디어에서는 keepalive가 약간 고유합니다.이더넷에는 가능한 인접 디바이스가 많으므로, keepalive는 와이어의 특정 인접 디바이스에 대한 경로를 사용할 수 있는지 확인하기 위해 설계되지 않았습니다.로컬 시스템이 이더넷 와이어 자체에 대한 읽기 및 쓰기 액세스 권한을 가지고 있는지 확인하도록 설계되었습니다.라우터는 소스 및 목적지 MAC 주소 및 특수

이더넷 유형 코드 0x9000으로 자체 이더넷 패킷을 생성합니다. 이더넷 하드웨어는 이 패킷을 이더넷 와이어로 전송한 다음 즉시 이 패킷을 다시 수신합니다.이는 이더넷 어댑터의 전송 및 수신 하드웨어와 와이어의 기본 무결성을 확인합니다.

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

직렬 인터페이스

직렬 인터페이스에는 여러 유형의 캡슐화가 있을 수 있으며 각 캡슐화 유형에 따라 사용할 keepalive의 유형이 결정됩니다.

라우터가 해당 피어로 ECHOREQ 패킷을 전송하는 빈도를 설정하려면 인터페이스 컨피그레이션 모드에서 keepalive 명령을 입력합니다.

- 시스템을 기본 keepalive 간격인 10초로 복원하려면 **no** 키워드와 함께 keepalive 명령을 입력합니다.
- keepalive를 비활성화하려면 keepalive disable 명령**을** 입력합니다.

참고:더 **keepalive** 명령은 HDLC(High-Level Data Link Control) 또는 PPP 캡슐화를 사용하는 직렬 인터페이스에 적용됩니다.프레임 릴레이 캡슐화를 사용하는 직렬 인터페이스에는 적용되지 않습니다.

참고:PPP 및 HDLC 캡슐화 유형 모두에 대해 keepalive가 0이면 keepalive가 비활성화되고 show running**-config** 명령 출력에 keepalive disable**로 보고됩니다**.

HDLC keepalives

또 다른 잘 알려진 keepalive 메커니즘은 HDLC용 직렬 keepalives입니다.두 라우터 간에 시리얼 keepalive가 전송되고 keepalive가 확인됩니다.시퀀스 번호를 사용하여 각 keepalive를 추적하면 각 디바이스가 HDLC 피어가 전송한 keepalive를 받았는지 확인할 수 있습니다.HDLC 캡슐화의 경우 세 개의 무시된 keepalive로 인해 인터페이스가 다운되었습니다.

사용자가 생성 및 전송된 keepalive를 볼 수 있도록 HDLC 연결에 대해 debug **serial interface** 명령을 활성화합니다.

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

HDLC keepalives는 3개의 요소를 사용하여 작동 여부를 확인합니다.

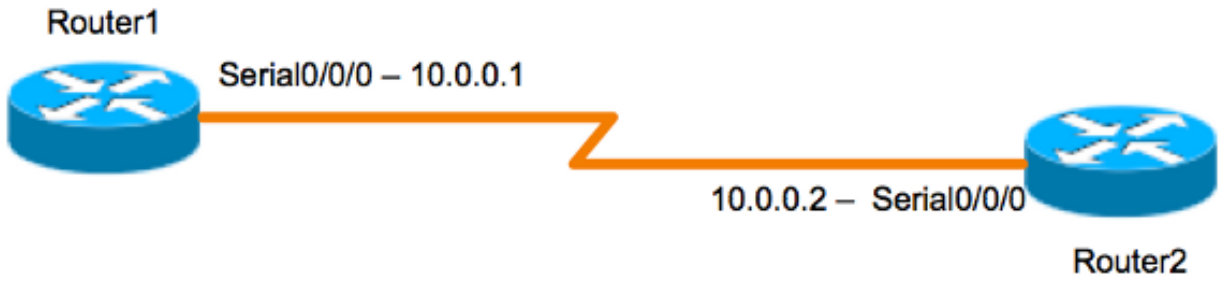
- 자체 증가된 번호인 "myseq"입니다.
- "mineseen"은 실제로 다른 쪽의 승인(증가됨)이며, 이는 그들이 우리로부터 이 번호를 기대한다고 말합니다.
- 반대편에 대한 우리의 승인인 "당신 본".

참고:myseq 및 mineseen 필드의 값 차이가 라우터 2에서 3을 초과하면 라인이 중단되고 인터

페이스가 재설정됩니다.

HDLC keepalive는 ECHOREQ 유형의 keepalive이므로 keepalive 빈도는 중요하며 양쪽에서 정확하게 일치하는 것이 좋습니다. 타이머가 동기화되지 않은 경우 시퀀스 번호가 순서가 잘못되기 시작합니다.예를 들어, 한 면을 10초로, 다른 면을 25초로 설정하면 빈도 차이가 충분하지 않아 시퀀스 번호가 3의 차이로 꺼지는 한 인터페이스가 계속 작동될 수 있습니다.

HDLC가 작동하는 방식에 대한 설명으로 라우터 1과 라우터 2는 각각 직렬0/0 및 직렬2/0을 통해 직접 연결됩니다.실패한 HDCL keepalive를 사용하여 인터페이스 상태를 추적하는 방법을 설명하기 위해 라우터 1에서 직렬 0/0이 종료됩니다.



라우터 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
```

라우터 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 keepalive는 HDLC keepalive와 약간 다릅니다.HDLC와 달리 PPP keepalive는 ping과 유사합니다.양측 모두 한가할 때 서로 ping할 수 있다.적절한 협상 조치는 항상 이 "ping"에 응답하는 것입니다. 따라서 PPP keepalives의 경우 빈도 또는 타이머 값은 로컬에서만 관련이 있으며 다른 측에는 영향을 주지 않습니다.한쪽이 keepalive를 끄더라도 keepalive 타이머가 있는 측으로부터의 에코 요청에 계속 응답합니다.그러나, 그것은 그 자신의 어떤 것도 시작하지 않을 것입니다.

PPP 연결에 **debug ppp packet** 명령을 활성화하여 사용자가 전송된 PPP keepalive를 볼 수 있도록 합니다.

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

수신한 응답도 다음과 같습니다.

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

PPP keepalive는 세 가지 부분으로 구성됩니다.

- ID 번호 - 피어가 응답하는 ECHOREQ를 식별하는 데 사용됩니다.
- Keepalive type(keepalive 유형) - ECHOREQ는 원래 디바이스에서 전송하는 keepalive이며 ECHOREP는 피어에서 보낸 응답입니다.
- 매직 번호 - 알림에는 서버와 원격 클라이언트 모두의 매직 번호가 포함됩니다.피어는 LCP Echo-Request 패킷에서 매직 번호를 검증하고 라우터에서 협상한 매직 번호가 포함된 해당 LCP Echo-Reply 패킷을 전송합니다.

PPP 캡슐화의 경우 5개의 무시된 keepalives로 인해 인터페이스가 다운되었습니다.

GRE 터널 인터페이스

GRE 터널 keepalive 메커니즘은 이더넷 또는 직렬 인터페이스와 약간 다릅니다.원격 라우터가 GRE keepalives를 지원하지 않는 경우에도 한 측에서 원격 라우터에서 keepalive 패킷을 시작하고 받을 수 있습니다.GRE는 IP 내부 터널링을 위한 패킷 터널링 메커니즘이므로 다른 GRE IP 터널 패킷 내에 GRE IP 터널 패킷을 빌드할 수 있습니다.GRE keepalive의 경우 발신자는 원래 keepalive 요청 패킷 내에 keepalive 응답 패킷을 미리 구축하여 원격 엔드가 외부 GRE IP 헤더의 표준 GRE 역캡슐화를 수행한 다음 내부 IP GRE 패킷을 전달하기만 하면 됩니다.이 메커니즘으로 인해 keepalive 응답이 터널 인터페이스 대신 물리적 인터페이스를 포워딩합니다.GRE 터널 적용부 작업에 대한 자세한 내용은 GRE Keepalives 작동 방법을 참조하십시오.

암호화 keepalives

IKE keepalives

IKE(Internet Key Exchange) keepalive는 VPN 피어가 작동 중이고 암호화된 트래픽을 수신할 수 있는지 확인하는 데 사용되는 메커니즘입니다.VPN 피어는 일반적으로 다시 연결되지 않으므로 인터페이스 keepalive 외에 별도의 암호화 keepalive가 필요합니다. 따라서 인터페이스 keepalive는 VPN 피어의 상태에 대한 충분한 정보를 제공하지 않습니다.

Cisco IOS 디바이스에서 IKE keepalive는 DPD(Dead Peer Detection)라는 독점 방법을 사용하여 활성화됩니다. 게이트웨이가 DPD를 피어로 전송하도록 허용하려면 글로벌 컨피그레이션 모드에서 다음 명령을 입력합니다.

crypto isakmp keepalive *seconds [retry-seconds]* [**periodic** | **on-demand**]
keepalive를 비활성화하려면 이 명령의 "no" 형식을 사용합니다.이 명령의 각 키워드가 수행하는 작업에 대한 자세한 내용은 crypto isakmp keepalive를 참조하십시오.더 세분화하려면 ISAKMP 프로필 아래에서 keepalive를 구성할 수도 있습니다.자세한 내용은 ISAKMP 프로필 개요 [Cisco IOS IPsec]를 참조하십시오.

NAT keepalives

하나의 VPN 피어가 NAT(Network Address Translation) 뒤에 있는 시나리오의 경우 NAT-Traversal이 암호화에 사용됩니다.그러나 유휴 기간 동안 업스트림 디바이스의 NAT 항목이 시간 초과될 수 있습니다.이 경우 터널을 가동하고 NAT가 양방향적이지 않을 때 문제가 발생할 수 있습니다.두 피어 간의 연결 중에 동적 NAT 매핑을 활성 상태로 유지하기 위해 NAT keepalive가 활성화됩니다.NAT keepalive는 1바이트의 암호화되지 않은 페이로드를 가진 UDP 패킷입니다.현재 DPD 구현은 NAT keepalives와 비슷하지만 약간의 차이가 있습니다. DPD는 피어 상태를 탐지하는 데 사용되고, IPsec 엔티티가 지정된 기간 동안 패킷을 보내거나 받지 않은 경우 NAT keepalives가 전송됩니다.유효한 범위는 5~3600초입니다.

> **팁:**NAT keepalives가 활성화된 경우(**crypto isamkp nat keepalive** 명령을 통해) 사용자는 유휴 값이 NAT 매핑 만료 시간인 20초보다 짧은지 확인해야 합니다.

이 기능에 대한 자세한 내용은 IPsec NAT 투명도를 참조하십시오.