

# 방화벽 클러스터 환경에서 LACP 포트 채널 오류 트러블슈팅

## 문제

FTD 어플라이언스의 Port-channel1에서 작동 상태가 Failed(실패)로 표시되었으며, 전송 또는 수신되는 LACP PDU는 없습니다. 디바이스는 FTD 클러스터에 속했으며 Port-channel1은 데이터 인터페이스로 사용되었으므로 포트 채널이 다운될 때 트래픽에 영향을 주었습니다.

관찰된 특정 증상은 다음과 같습니다.

- 파트너 시스템 ID를 0,0-0-0-0-0-0으로 표시하고 포트 번호가 0x0인 LACP 인접 디바이스 정보.
- 파트너 운영 키 및 포트 상태가 0x0으로 표시됩니다.
- 방화벽 새시에서 LACP 카운터가 증가하지 않습니다.
- "일시 중단(LACP PDU 없음)" 상태를 표시하는 인터페이스.
- 인접한 스위치에서는 LACP Sent 카운터만 증가합니다. LACP Recv 카운터는 증가하지 않습니다.

영향을 받는 디바이스의 LACP 네이버 출력에는 다음이 표시됩니다.

```
<#root>
```

```
device(fxos)#
```

```
show lacp neighbor
```

```
Flags: S - Device is sending Slow LACPDUs F - Device is sending Fast LACPDUs  
A - Device is in Active mode P - Device is in Passive mode
```

```
port-channel1 neighbors
```

```
Partner's information
```

Port	Partner System ID	Partner Port Number	Age	Partner Flags
Eth1/2				

```
0,0-0-0-0-0-0
```

0x0

```

          5022089      SP
          LACP Partner      Partner
          Port Priority      Oper Key      Partner
          0                0x0          Port State
Partner's information      0x0
          Partner          Partner
Port      System ID      Port Number      Age      Partner
Eth1/3

```

0,0-0-0-0-0-0

0x0

```

          4895677      SP
          LACP Partner      Partner
          Port Priority      Oper Key      Partner
          0                0x0          Port State

```

방화벽에서는 포트 채널 멤버에 대해 LACP Sent/Recv 카운터가 증가하지 않습니다.

<#root>

device#

connect fxos

device(fxos)#

show lacp counters

Port	LACPDUs		Marker		Marker Response		LACPDUs	
	Sent	Recv	Sent	Recv	Sent	Recv	Pkts	Err
port-channel1								
Ethernet1/4	11413	13114	0	0	0	0	0	0

<-- the LACP counters do not increase

포트 채널 인터페이스 및 하위 인터페이스는 다운/다운 상태입니다.

<#root>

#

show interface ip brief

Interface	IP-Address	OK?	Method	Status	Protocol
Internal-Contro10/0	unassigned	YES	unset	up	up
Internal-Data0/0	unassigned	YES	unset	up	up
Internal-Data0/1	unassigned	YES	unset	up	up
Internal-Data0/2	169.254.1.1	YES	unset	up	up
Internal-Data0/3	unassigned	YES	unset	up	up
Internal-Data0/4	unassigned	YES	unset	down	up
Port-channel1	unassigned	YES	unset		

down down

Port-channel1.90 192.0.2.15 YES CONFIG

down down

Port-channel1.102 192.0.2.130 YES CONFIG

down down

...

스위치측 로그에 따르면 스위치가 LACP를 전송했지만 파트너 LACP PDU를 수신하지 못했으며 포트가 일시 중단되었습니다.

<#root>

Apr 2 18:44:20.614: %LINEPROTO-5-UPDOWN: Line protocol on Interface TwentyFiveGigE2/0/25, changed state to down  
Apr 2 18:44:25.452: %ETC-5-L3DONTBNL2: Twe2/0/25

suspended

: LACP currently not enabled on the remote port.  
Apr 2 18:44:36.318: %ETC-5-L3DONTBNL2: Twe2/0/25

suspended

: LACP currently not enabled on the remote port.  
Apr 3 02:17:06.798: %LINK-5-UPDOWN: Interface TwentyFiveGigE2/0/25, changed state to down  
Apr 3 02:17:26.722: %LINK-5-UPDOWN: Interface TwentyFiveGigE2/0/25, changed state to up  
Apr 3 02:17:35.915: %ETC-5-L3DONTBNL2: Twe2/0/25 suspended: LACP currently not enabled on the remote port  
Apr 3 02:23:22.255: %LINK-5-UPDOWN: Interface TwentyFiveGigE2/0/25, changed state to down

Apr 3 02:23:43.886: %LINK-5-UPDOWN: Interface TwentyFiveGigE2/0/25, changed state to up  
Apr 3 02:23:53.808: %ETC-5-L3DONTBNL2: Twe2/0/25 suspended: LACP currently not enabled on the remote

## 환경

- 소프트웨어 버전: FTD 7.6.2. ASA를 비롯한 다른 소프트웨어 버전도 영향을 받을 수 있습니다.
- 포트 채널을 사용하는 데이터 인터페이스를 사용하는 FTD 클러스터 컨피그레이션.
- LACP 지원 포트 채널을 업스트림 스위치 인프라에 연결합니다.

## 해결

포트 채널 인터페이스 상태 확인 실패로 인해 영향을 받는 FTD 유닛이 클러스터를 떠났음을 식별하는 데 문제가 있습니다. 장치에서 클러스터링이 비활성화되면 모든 데이터 인터페이스가 설계에 의해 종료되었으며, 이로 인해 LACP PDU가 중단되고 스위치측 중단 및 트래픽에 영향이 발생했습니다.

### 진단 단계 수행

1단계: Cisco Firepower 디바이스 및 업스트림 스위치에서 디버그 및 지원 번들 수집

여러 트러블슈팅 아카이브, LACP 디버그 파일, 핵심 파일, TS(트러블슈팅) 파일이 분석을 위해 FXOS 쉘에서 수집되었습니다.

2단계: 스위치 동작 및 LACP 상태 검증

스위치 엔지니어가 스위치가 LACP PDU를 전송하는 것을 확인했지만 Firepower 디바이스에서 패트너 PDU를 수신하지 못했습니다.

### 3단계: LACP 내부 상태 전환 분석

분석 결과, 파트너 PDU가 누락되어 인터페이스가 일시 중단 상태로 전환되었으며 LACP 카운터가 증가하지 않는 것으로 나타났습니다.



팁: 'show cluster history' 명령 출력과 방화벽 LINA syslogs를 확인하여 클러스터 실패의 원인을 확인합니다.

이 예에서 디바이스는 데이터 인터페이스 장애로 인해 클러스터를 종료했습니다.

```
<#root>
```

```
#
```

```
show cluster history
```

```
CONTROL_NODE          CONTROL_NODE          Event: Control node unit-1-1 is quitting
                        due to interface health check
                        failure on Port-channel1,
                        1 times. Rejoin will be attempted
                        after 5 min.

20:44:31 CEST Apr 2 2026
CONTROL_NODE          DISABLED              Client progression done
```

### 복구 절차

1단계: 영향을 받는 FTD 유닛에서 클러스터링 다시 활성화

```
<#root>
```

```
#
```

```
cluster enable
```

이 명령을 사용하면 유닛이 클러스터에 다시 가입하고, 데이터 인터페이스를 가동하고, LACP PDU를 재개하고, Port-channel1 기능을 복원할 수 있습니다.

2단계: LACP 복구 확인

클러스터링을 다시 활성화한 후 LACP PDU가 다시 시작되고 Port-channel1이 방화벽과 스위치 양 쪽에서 정상 작동으로 돌아왔습니다.

## 원인

근본 원인은 포트 채널 인터페이스 상태 검사 실패로 인해 FTD 유닛이 클러스터를 벗어났기 때문입니다. FTD 유닛에서 클러스터링이 비활성화되면 모든 데이터 인터페이스가 관리상 종료되므로 LACP PDU 전송이 중지되고 업스트림 스위치가 포트 채널 인터페이스를 일시 중단합니다.

이러한 동작이 필요합니다.

Cisco 버그 ID CSCwo09449은 제품의 서비스 가용성을 향상시키도록 등록되었습니다.

## 관련 콘텐츠

- Cisco 버그 ID [CSCwo09449](#) - FXOS: 클러스터링이 비활성화될 때 부실 TX 및 RX LACP 카운터 및 일시 중단된 데이터 포트 채널

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.