

# ファイアウォールクラスタ環境でのLACPポートチャンネル障害のトラブルシューティング

## お問い合わせ内容

FTDアプライアンスのport-channel1で動作ステータスがFailedと表示され、LACP PDUの送受信は行われていませんでした。デバイスはFTDクラスタの一部であり、Port-channel1はデータインターフェイスとして使用されているため、ポートチャンネルがダウンするとトラフィックに影響が及びます。

確認された具体的な症状は次のとおりです。

- ・ パートナーシステムID(PID)が0,0-0-0-0-0-0-0でポート番号が0x0のLACPネイバー情報。
- ・ パートナーのOperキーとポートの状態が0x0と表示される。
- ・ ファイアウォールシャーシのLACPカウンタが増加しない。
- ・ 「suspended (no LACP PDU)」ステータスを示すインターフェイス。
- ・ 隣接スイッチでは、LACP Sentカウンタのみが増加します。LACP Recvカウンタは増加しません。

該当するデバイスからのLACPネイバーの出力には次のように表示されます。

```
<#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		Partner
	Port Priority		Oper Key		Port State
	0		0x0		0x0
Partner's information					
	Partner		Partner		Partner
Port	System ID		Port Number	Age	Flags
Eth1/3					

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

0x0

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

ファイアウォールでは、ポートチャネルメンバに対するLACP Sent/Recvカウンタは増加しません。

<#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

ポートチャネルインターフェイスとそのサブインターフェイスがダウン/ダウンの状態になっている。

```
<#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
```

```
...
```

スイッチ側のログは、スイッチがLACPを送信しているものの、パートナーのLACP PDUを受信していないことを示しており、ポートは一時停止しています。

```
<#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-L3DONTBNDL2: Twe2/0/25 suspended: LACP currently not enabled on the remote
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-L3DONTBNDL2: Twe2/0/25 suspended: LACP currently not enabled on the remote
```

## 環境

- ソフトウェアバージョン：FTD 7.6.2ASAなど、その他のソフトウェアバージョンも影響を受ける可能性があります。
- ポートチャンネルを使用するデータインターフェイスを使用したFTDクラスタ設定。
- アップストリームスイッチインフラストラクチャに接続するLACP対応ポートチャンネル。

## 解決策

この問題の解決には、ポートチャンネルインターフェイスのヘルスチェックの失敗により、影響を受けたFTDユニットがクラスタから離脱したことを特定することが含まれていました。ユニットでクラスタリングを無効にすると、すべてのデータインターフェイスが意図的にシャットダウンされ、LACP PDUが停止してスイッチ側の一時停止とトラフィックへの影響が発生しました。

## 実行される診断手順

ステップ1: Cisco Firepowerデバイスとアップストリームスイッチの両方からデバッグバンドルとサポートバンドルを収集します

分析のために、複数のトラブルシューティングアーカイブ、LACPデバッグファイル、コアファイル、およびTS (トラブルシューティング) ファイルがFXOSシャーシから収集されました。

ステップ2: スwitchの動作とLACP状態を検証する

スイッチのエンジニアは、スイッチがLACP PDUを送信しているが、FirepowerデバイスからパートナーPDUを受信していないことを確認しました。

手順3:LACPの内部状態遷移を分析します。

分析により、パートナーPDUの欠落によりインターフェイスが中断状態に移行し、LACPカウンタが増加しないことが示されました。



ヒント:show cluster historyコマンドの出力とファイアウォールLINA syslogをチェックして、クラスタ障害の理由を特定します。

---

次の例では、データインターフェイスの障害により、デバイスがクラスタを終了しています。

```
<#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
```

## 回復手順

ステップ1:該当するFTDユニットでクラスタリングを再度有効にします

```
<#root>
```

```
#
```

```
cluster enable
```

このコマンドにより、ユニットはクラスタへの再参加、データインターフェイスの起動、LACP

PDUの再開、およびPort-channel1機能の復元を行いました。

## ステップ2:LACPリカバリの確認

クラスタリングを再度有効にすると、LACP PDUが再開され、ファイアウォール側とスイッチ側の両方でPort-channel1が通常の動作に戻ります。

## 原因

根本的な原因は、ポートチャンネルインターフェイスのヘルスチェックの障害であり、これによりFTDユニットがクラスタから離脱しました。FTDユニットでクラスタリングが無効になっている場合は、すべてのデータインターフェイスが管理上シャットダウンするように設計されているため、LACP PDUの送信が停止され、アップストリームスイッチでポートチャンネルインターフェイスが一時停止されます。

これは正常な動作です。

Cisco Bug ID CSCwo09449 ( 登録ユーザ専用 ) は、製品のサービスビリティを強化するために登録されました。

## 関連コンテンツ

- Cisco Bug ID [CSCwo09449](#) - FXOS : クラスタリングが無効な場合に、古いTXおよびRX LACPカウンタと中断されたデータポートチャンネル

## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。