排除防火墙集群环境中的LACP端口通道故障

问题

FTD设备上的Port-channel1显示运行状态为Failed，没有发送或接收LACP PDU。设备是FTD集群的一部分，Port-channel1用作数据接口，在端口通道关闭时导致流量影响。

观察到的具体症状包括：

- LACP邻居信息，其中合作伙伴系统ID显示为0,0-0-0-0-0，端口号为0x0。
- Partner Oper Key和Port State显示为0x0。
- 防火墙机箱上的LACP计数器未增加。
- 接口显示“暂停（无LACP PDU）”状态。
- 在邻接交换机上，只有LACP发送计数器增加。LACP Recv计数器不会增加。

受影响设备的LACP邻居输出显示：

<#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
           Partner                Partner                       Partner
Port       System ID              Port Number     Age           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
```

在防火墙上，端口通道成员的LACP发送/接收计数器不会增加：

```
<#root>

device#

connect fxos


device(fxos)#

show lacp counters


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

<-- the LACP counters do not increase
```

端口通道接口及其子接口处于down/down状态：

```
<#root>

#
```

show interface ip brief

```
Interface                  IP-Address      OK?           Method Status      Protocol
Internal-Control0/0        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

```
...
```

交换机端日志表明交换机正在传输LACP，但未接收合作伙伴LACP PDU，端口处于挂起状态：

<#root>

```
Apr  2 18:44:20.614: %LINEPROTO-5-UPDOWN: Line protocol on Interface TwentyFiveGigE2/0/25, changed stat
Apr  2 18:44:25.452: %ETC-5-L3DONTBNDL2: Twe2/0/25
```

suspended

```
: LACP currently not enabled on the remote port.
Apr  2 18:44:36.318: %ETC-5-L3DONTBNDL2: 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
```

环境

- 软件版本:FTD 7.6.2。其他软件版本（包括ASA）也可能会受到影响。
- FTD集群配置，数据接口使用端口通道。
- 连接到上游交换机基础设施的启用LACP的端口通道。

分辨率

解决方案涉及确定受影响的FTD设备因端口通道接口运行状况检查失败而离开集群。当禁用设备上的集群时，所有数据接口都设计为关闭，这会停止LACP PDU并导致交换机端挂起和流量影响。

执行的诊断步骤

步骤 1：从Cisco Firepower设备和上游交换机收集调试和支持捆绑包

从FXOS机箱收集多个故障排除存档、LACP调试文件、核心文件和TS（故障排除）文件进行分析。

步骤 2：验证交换机行为和LACP状态

交换机工程师确认交换机正在发送LACP PDU，但未从Firepower设备接收合作伙伴PDU。

步骤 3：分析LACP内部状态转换

分析显示，由于缺少伙伴PDU，接口进入暂停状态，LACP计数器不会增加。

提示：检查“show cluster history”命令输出和防火墙LINA系统日志以确定集群故障的原因。

在本示例中，设备由于数据接口故障而退出集群：

```
<#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
```

恢复程序

步骤 1：在受影响的FTD设备上重新启用集群

```
<#root>

#

cluster enable
```

此命令导致设备重新加入集群、启用数据接口、恢复LACP PDU并恢复Port-channel1功能。

步骤 2：检验LACP恢复

重新启用集群后，LACP PDU恢复，Port-channel1在防火墙和交换机端均恢复正常运行。

原因

根本原因是端口通道接口运行状况检查失败，导致FTD设备离开集群。在FTD设备上禁用集群时，所有数据接口都设计为管理性关闭，这会停止LACP PDU传输，并导致上游交换机挂起端口通道接口。

此行为是预期行为。

Cisco Bug ID CSCwo09449（仅限注册用户）已归档以增强产品的适用性。

相关内容

- 思科漏洞ID CSCwo09449 - FXOS:禁用集群时，过时的TX和RX LACP计数器和暂停的数据端口通道

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。