Troubleshoot LACP Port-Channel Failure in Firewall Cluster Environment

Contents

Issue

Port-channel1 on an FTD appliance showed an operational status as Failed, with no LACP PDUs being sent or received. The device was part of an FTD cluster and Port-channel1 was used as a data interface, resulting in traffic impact when the port-channel went down.

The specific symptoms observed included:

- LACP neighbor information showing Partner System ID as 0,0-0-0-0-0-0 with Port Number 0x0.
- Partner Oper Key and Port State showing as 0x0.
- LACP counters not incrementing on the firewall chassis.
- Interfaces showing "suspended (no LACP PDU)" status.
- On the adjacent switch, only the LACP Sent counters increase. The LACP Recv counters do not increase.

The LACP neighbor output from the affected device showed:

<#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
```

On the firewall, the LACP Sent/Recv counters do not increase for the port-channel members:

```
<#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
```

The port-channel interface and its subinterfaces are in down/down state:

```
<#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


...
```

Switch-side logs indicated the switch was transmitting LACP but not receiving partner LACP PDUs, with ports being suspended:

<#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
```

Environment

- Software version: FTD 7.6.2. Other software versions, including ASA, can be also affected.
- FTD cluster configuration with data interfaces using a Port-channel.
- LACP-enabled port-channel connecting to upstream switch infrastructure.

Resolution

The resolution involved identifying that the affected FTD unit had left the cluster due to a Port-channel interface health-check failure. When clustering was disabled on the unit, all data interfaces were shut down by design, which stopped LACP PDUs and caused switch-side suspension and traffic impact.

Diagnostic Steps Performed

Step 1: Collect debug and support bundles from both Cisco Firepower device and upstream switch.

Multiple troubleshooting archives, LACP debug files, core files, and TS (troubleshooting) files were collected from the FXOS chassis for analysis.

Step 2: Validate switch behavior and LACP state.

Switch engineer confirmed the switch was sending LACP PDUs but not receiving partner PDUs from the Firepower device.

Step 3: Analyze LACP internal state transitions.

Analysis showed interfaces moved into a suspended state due to missing partner PDUs, with LACP counters not incrementing.

Tip: Check the '**show cluster history**' command output and the firewall LINA syslogs to determine the reason of the cluster failure.

In this example, the device quit the cluster due to data interface failure:

<#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
```

Recovery Procedure

Step 1: Re-enable clustering on the affected FTD unit:

<#root>

#

cluster enable

This command caused the unit to rejoin the cluster, bring data interfaces up, resume LACP PDUs, and restore Port-channel1 functionality.

Step 2: Verify LACP recovery:

After re-enabling clustering, LACP PDUs resumed and Port-channel1 returned to normal operation on both the firewall and switch sides.

Cause

The root cause was a Port-channel interface health-check failure that caused the FTD unit to leave the cluster. When clustering is disabled on an FTD unit, all data interfaces are administratively shut down by design, which stops LACP PDU transmission and causes the upstream switch to suspend the port-channel interfaces.

This behavior is expected.

Cisco bug ID CSCwo09449 was filed to enhance the serviceability of the product.

Related Content

- Cisco bug ID CSCwo09449 - FXOS: stale TX and RX LACP counters and suspended data port-channels when clustering is disabled