Configure and Verify Port-Channel on Firepower Appliances

Contents

Introduction

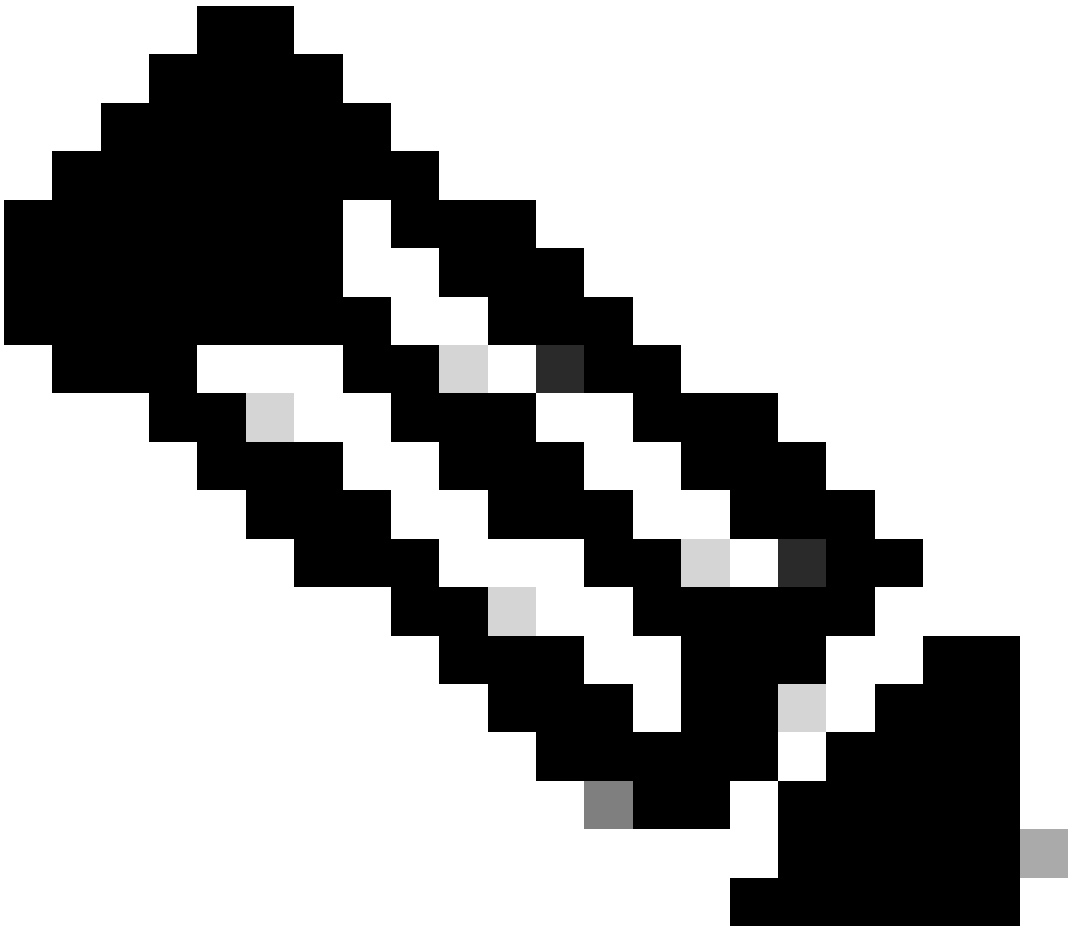
This document describes how to configure, verify, and troubleshoot the Port-Channel on Firepower Appliances.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Firepower Management Center (FMC)
- Firepower Chassis Manager (FCM)
- Firepower eXtensible Operating System (FXOS)
- Firepower Threat Defense (FTD)
- EtherChannel (EC)



Note: In this document, the terms EtherChannel and Port-Channel (PC) are used interchangeably.

Components Used

The information in this document is based on these software and hardware versions:

- 2 x FPR4120 on FXOS 2.2(2.17), FTD 6.2.0.2.51
- 1 x FPR4110 on FXOS 2.1(0.159), FTD 6.1.0.330
- 1 x FPR2110 on FTD 6.2.1 (build 341)
- 1 x FPR1150 on FTD 6.5.0
- WS-C3750X-24 on15.2(4)E5

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

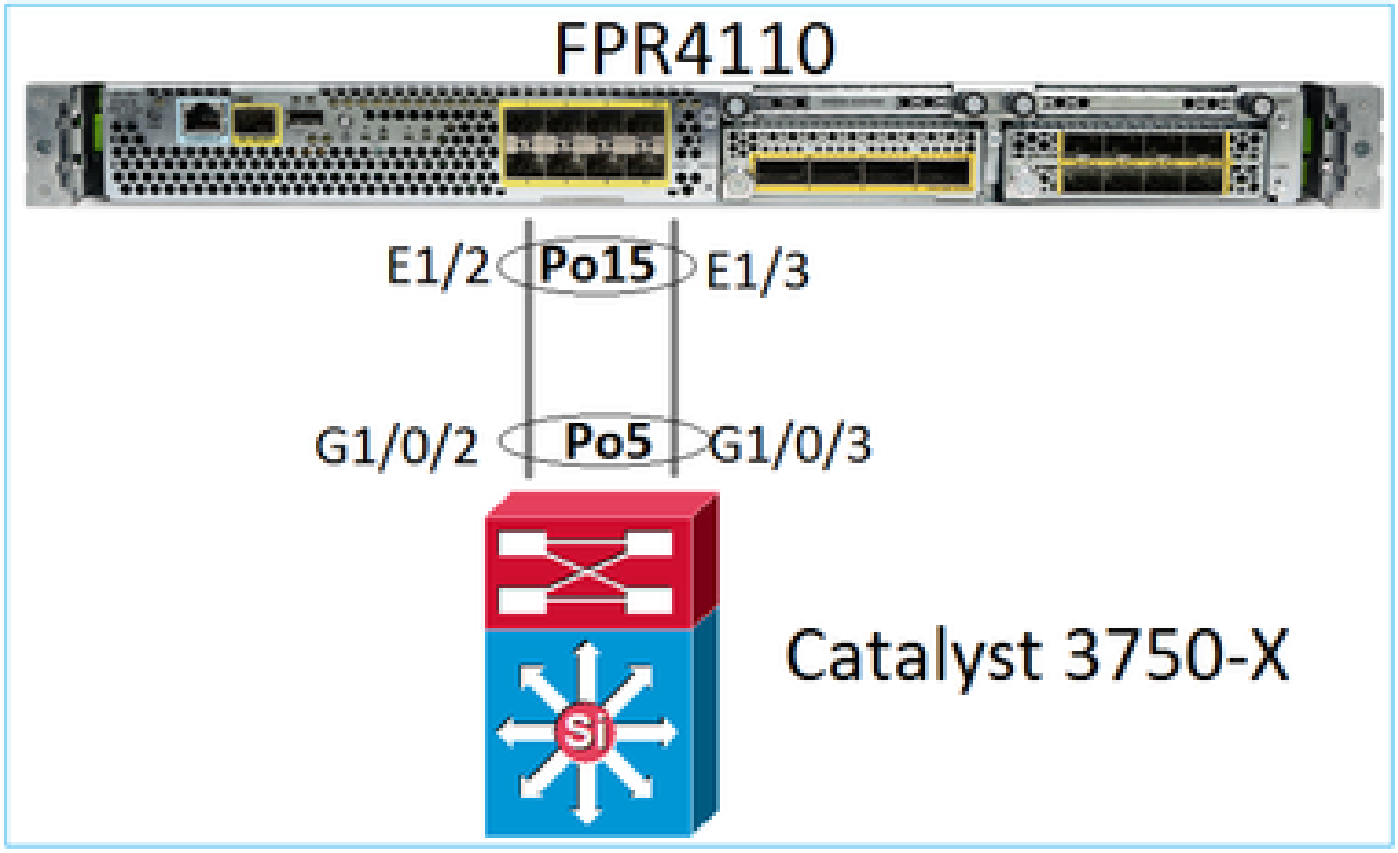
Background Information

This document describes the configuration, verification and troubleshoot of a Port-Channel on Firepower Appliances (FPR1xxx, FPR21xx, FPR41xx, FPR93xx). The document configuration examples are based on Firepower Threat Defense (FTD), but many concepts (for example, the verification and troubleshoot) are fully applicable to Adaptive Security Appliance (ASA) as well.

Configure

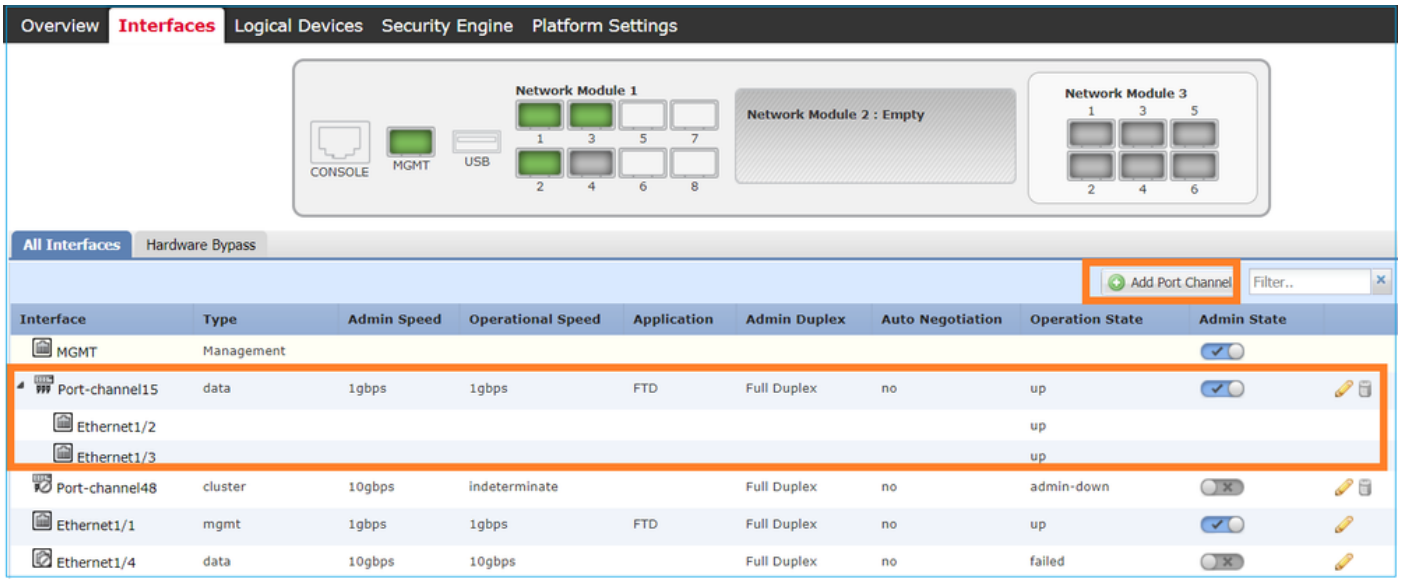
Port-Channel on FPR4100/FPR9300

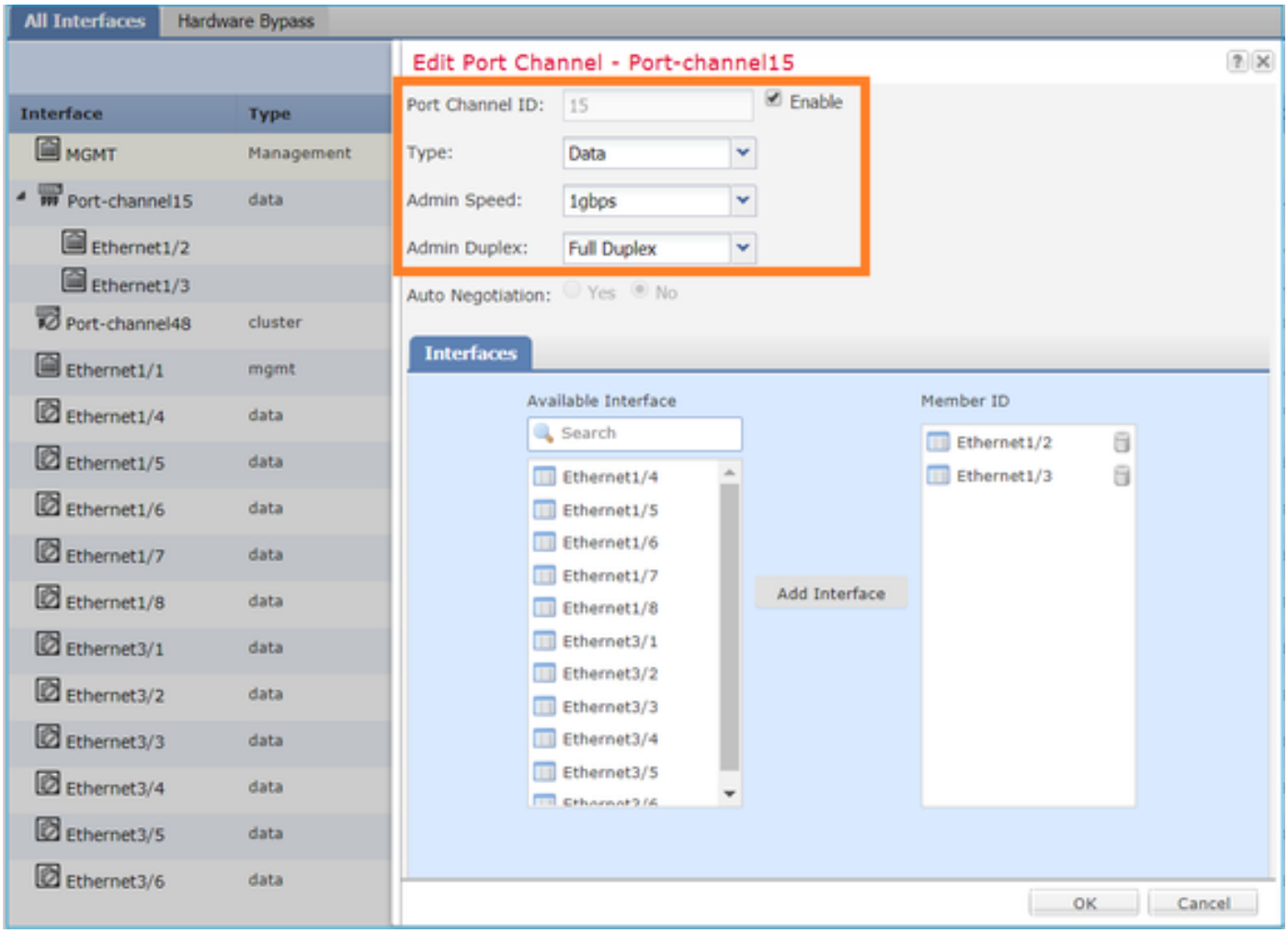
Network Diagram



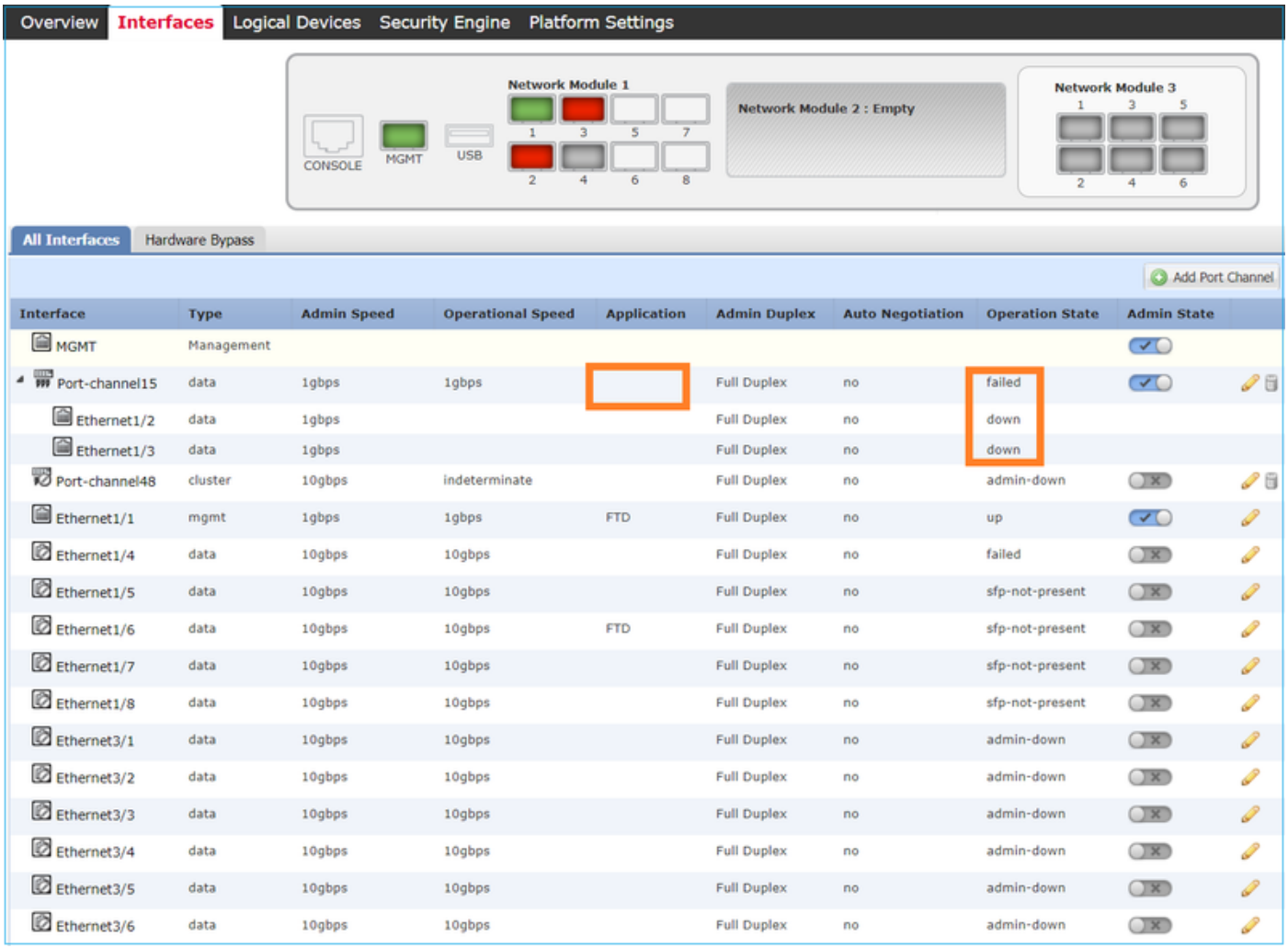
Configure a Port-Channel from FXOS User Interface (FPR4100/FPR9300)

FTD Port-Channel on Firepower Appliances is managed by the FXOS code. On FPR4100/FPR9300 the configuration is done from the Firepower Chassis Manager:

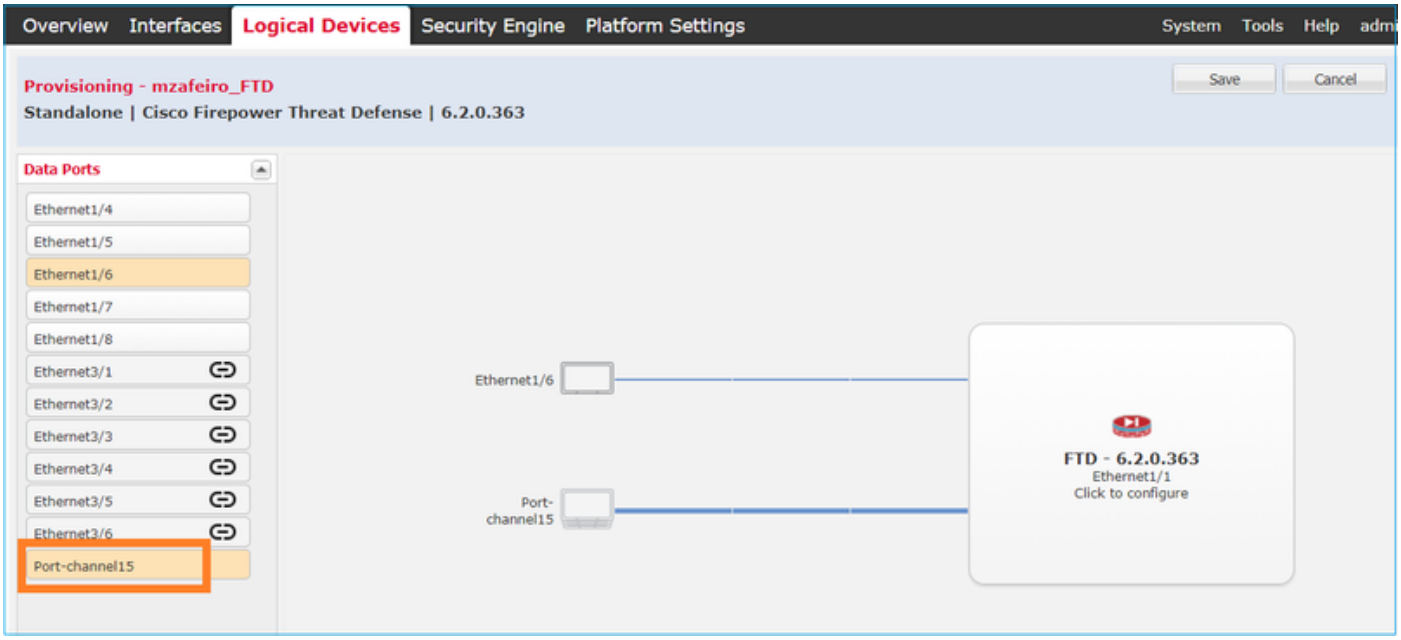




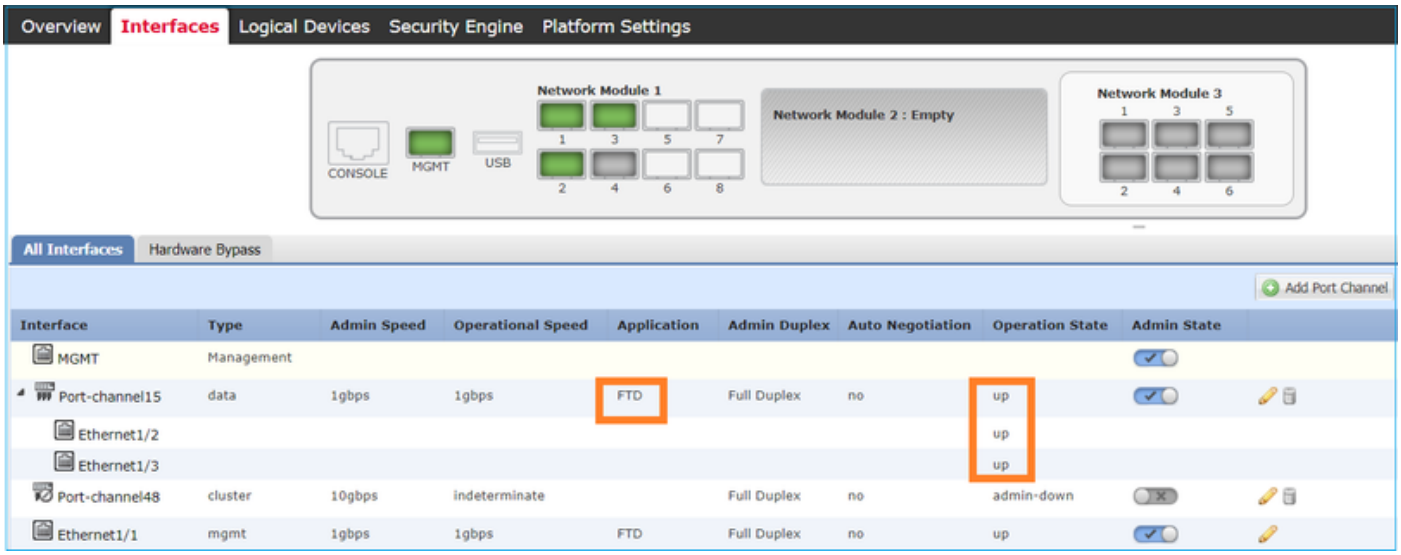
The Port-Channel is down (failed state) until it is assigned to a logical device:



To assign the Port-Channel to the logical device:



The result:



Main points

- Before FXOS 2.4.x release, the FPR4100/FPR9300 supports only LACP (no mode ON or PAGP). Since FXOS 2.4.1.101 mode ON is supported for data and data-sharing Etherchannels.
- Please ensure that the interface(s) which are to be added in the Port-Channel are not added already to the logical device. If they are, they do not show up in the interface when the Port-Channel is added.
- You cannot enable/disable individual Port-Channel members, but only the Port-Channel itself.
- You cannot delete a Port-Channel that is used by a Logical Device (for example, ASA or FTD). You must disassociate it first.
- The Port-Channel does not come up until you assign it to a logical device. If the EtherChannel is removed from the logical device or the logical device is deleted, the Port-Channel reverts to a Suspended state.
- Set the switch ports that connect to Active mode for the best compatibility.

Switch Configuration

When you configure the switch, in order to avoid Port-Channel instabilities it is recommended to:

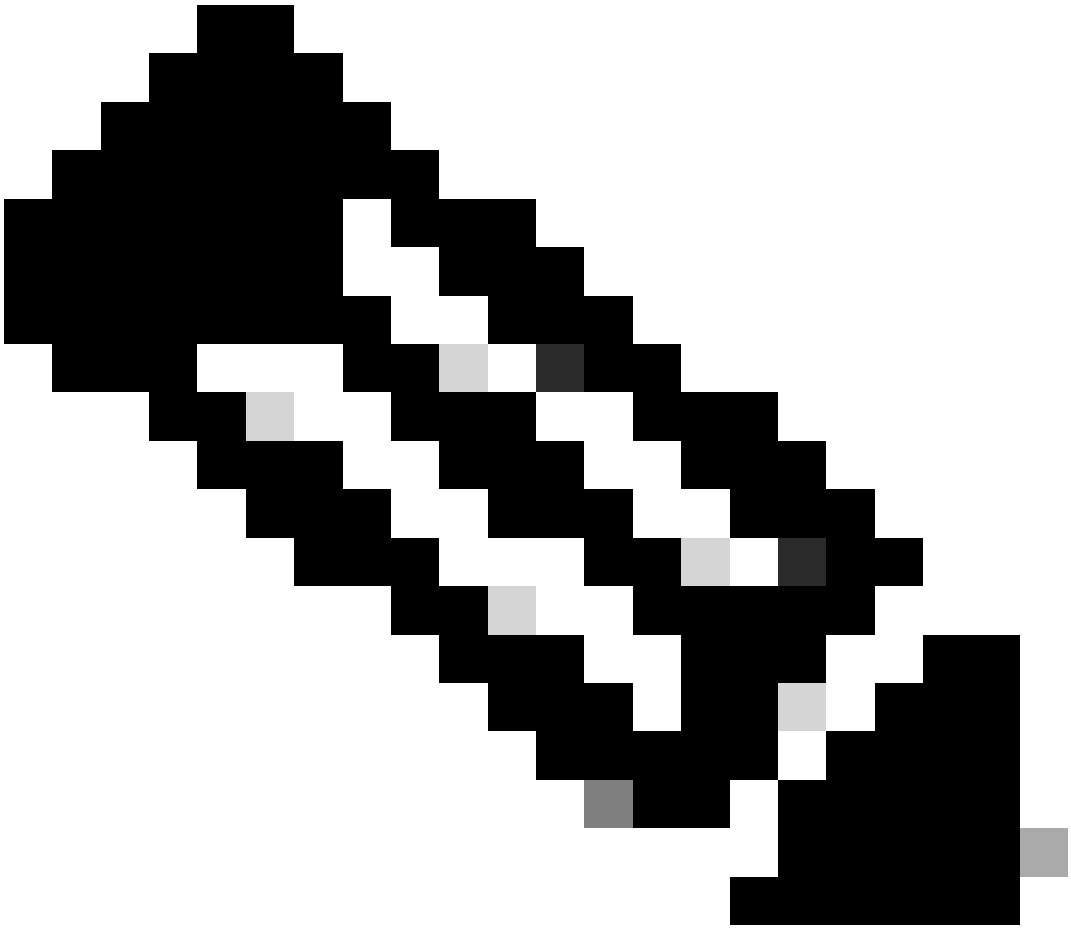
- Use the interface range command.
- Shutdown the Port-Channel interface members before you make changes that affect the Port-Channel operation (for example, if the Port-Channel mode is changed).

Example

<#root>

```
Switch(config)#
 interface range g1/0/2 - 3
Switch(config-if-range)#
shutdown
Switch(config-if-range)#
switchport trunk encapsulation dot1q
Switch(config-if-range)#
```

```
 switchport mode trunk
Switch(config-if-range)#
channel-group 5 mode active
Switch(config-if-range)#
no shutdown
```



Note: Always refer to the switch model Configuration Guide section for additional details.

Configure a Port-Channel from FXOS CLI (FPR4100/FPR9300)

Step 1. Verify the interfaces that are already assigned to the FTD logical device.

```
<#root>
FP4110-7-A#
```

```
scope ssa

FP4110-7-A /ssa #

show logical-device


Logical Device:
    Name       Description Slot ID    Mode       Oper State                Template Name
    ---------- ----------- ---------- ---------- ------------------------ -------------
    mzafeiro_FTD                          1          Standalone Ok                       ftd

FP4110-7-A /ssa #

scope logical-device mzafeiro_FTD

FP4110-7-A /ssa/logical-device #

show external-port-link


External-Port Link:
    Name            Port or Port Channel Name App Name   Description
    --------------- ------------------------- ---------- -----------
    Ethernet11_ftd  Ethernet1/1               ftd
    Ethernet16_ftd  Ethernet1/6               ftd
```

Step 2. Verify the chassis interfaces.

```
<#root>

FP4110-7-A#

scope eth-uplink

FP4110-7-A /eth-uplink #

scope fabric a

FP4110-7-A /eth-uplink/fabric #

show interface


Interface:
    Port Name       Port Type          Admin State Oper State       State Reason
    --------------- ------------------ ----------- ---------------- ------------
    Ethernet1/1     Mgmt               Enabled     Up
    Ethernet1/2     Data               Disabled    Admin Down       Administratively down
    Ethernet1/3     Data               Disabled    Admin Down       Administratively down
    Ethernet1/4     Data               Disabled    Failed           SFP checksum error
    Ethernet1/5     Data               Disabled    Sfp Not Present  Unknown
    Ethernet1/6     Data               Disabled    Sfp Not Present  Unknown
    Ethernet1/7     Data               Disabled    Sfp Not Present  Unknown
    Ethernet1/8     Data               Disabled    Sfp Not Present  Unknown
    Ethernet3/1     Data               Disabled    Admin Down       Administratively down
    Ethernet3/2     Data               Disabled    Admin Down       Administratively down
    Ethernet3/3     Data               Disabled    Admin Down       Administratively down
    Ethernet3/4     Data               Disabled    Admin Down       Administratively down
    Ethernet3/5     Data               Disabled    Admin Down       Administratively down
    Ethernet3/6     Data               Disabled    Admin Down       Administratively down
```

```
FP4110-7-A /eth-uplink/fabric #
show port-channel

Port Channel:
    Port Channel Id Name             Port Type          Admin State Oper State     State Reason
    --------------- ---------------- ------------------ ----------- --------------- ------------
    48              Port-channel48   Cluster            Disabled    Admin Down      Administratively dow
```

Step 3. Create the Port-Channel.

```
<#root>
bsns-4110-2-A#
scope eth-uplink
bsns-4110-2-A /eth-uplink #
scope fabric a
bsns-4110-2-A /eth-uplink/fabric #
create port-channel 15
bsns-4110-2-A /eth-uplink/fabric/port-channel* #
create member-port Ethernet1/5
bsns-4110-2-A /eth-uplink/fabric/port-channel/member-port* #
exit
bsns-4110-2-A /eth-uplink/fabric/port-channel* #
create member-port Ethernet1/6
bsns-4110-2-A /eth-uplink/fabric/port-channel/member-port* #
exit
bsns-4110-2-A /eth-uplink/fabric/port-channel* #
set port-type data
bsns-4110-2-A /eth-uplink/fabric/port-channel* #
set speed 1gbps
bsns-4110-2-A /eth-uplink/fabric/port-channel* #
enable
bsns-4110-2-A /eth-uplink/fabric/port-channel* #
commit-buffer
```

Step 4. Assign the interface to the FTD logical device:

```
<#root>
```

```
FP4110-7-A#
 scope ssa
FP4110-7-A /ssa #
scope logical-device mzafeiro_FTD
FP4110-7-A /ssa/logical-device #
create external-port-link PC15_ftd Port-channel15 ftd
FP4110-7-A /ssa/logical-device/external-port-link* #
commit-buffer
FP4110-7-A /ssa/logical-device/external-port-link #
```

Verification

```
<#root>
FP4110-7-A#
scope ssa
FP4110-7-A /ssa #
scope logical-device mzafeiro_FTD
FP4110-7-A /ssa/logical-device #
show external-port-link

External-Port Link:
    Name            Port or Port Channel Name App Name   Description
    --------------- ------------------------- ---------- -----------
    Ethernet11_ftd  Ethernet1/1               ftd
    Ethernet16_ftd  Ethernet1/6               ftd
    PC15_ftd        Port-channel15            ftd
```

```
<#root>
FP4110-7-A#
scope eth-uplink
FP4110-7-A /eth-uplink #
scope fabric a
FP4110-7-A /eth-uplink/fabric #
 show port-channel

Port Channel:
    Port Channel Id Name             Port Type          Admin State Oper State     State Reason
    --------------- ---------------- ------------------ ----------- ---------------- ------------
    15              Port-channel15   Data               Enabled     Up
```

```
    48              Port-channel48   Cluster           Disabled    Admin Down     Administratively down
```

<#root>

```
FP4110-7-A /eth-uplink/fabric #
```

enter port-channel 15

```
FP4110-7-A /eth-uplink/fabric/port-channel #
```

show member-port

```
Member Port:
    Port Name       Membership         Oper State       State Reason
    --------------- ------------------ ---------------- ------------
    Ethernet1/2     Up                 Up
    Ethernet1/3     Up                 Up
```

Delete the Port-Channel from FXOS CLI (FPR4100/FPR9300).

<#root>

```
FP4110-7-A#
```

scope eth-uplink

```
FP4110-7-A /eth-uplink #
```

scope fabric a

```
FP4110-7-A  /eth-uplink/fabric #
```

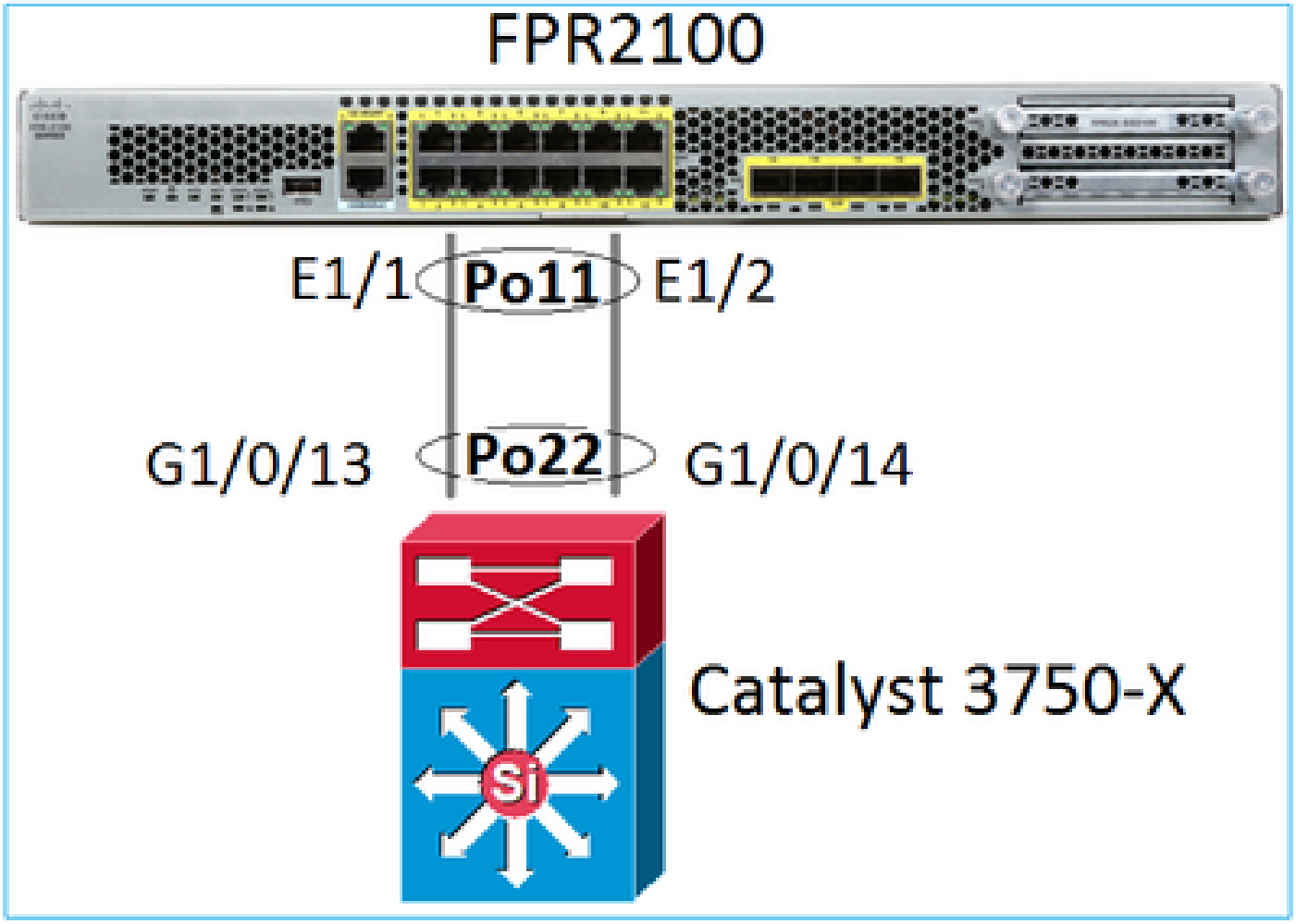
delete port-channel 15

```
FP4110-7-A /eth-uplink/fabric* #
```

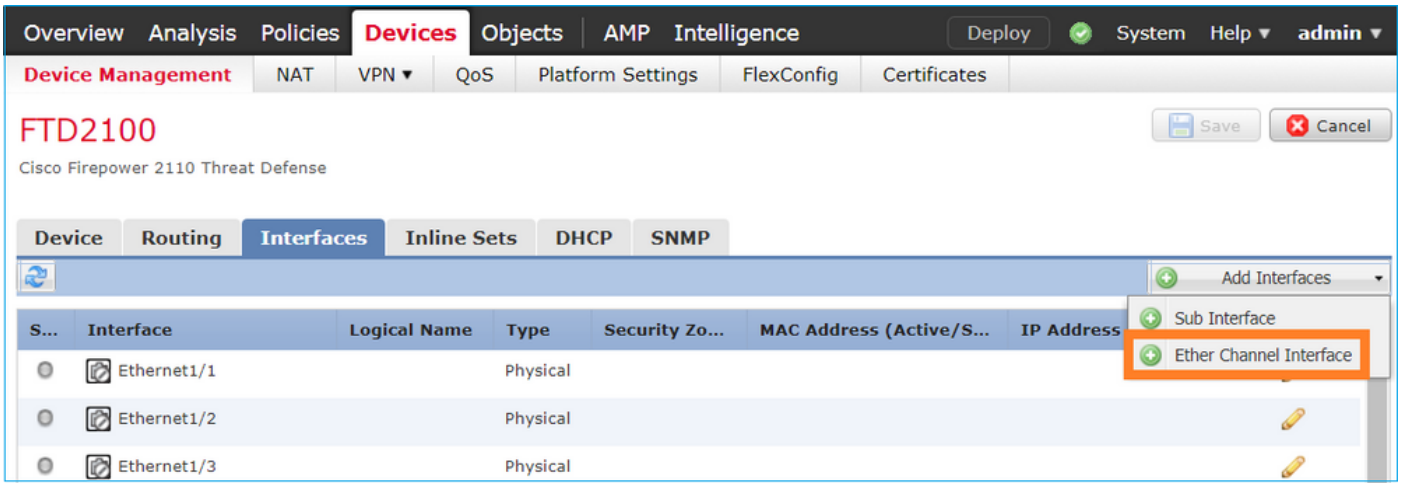
commit-buffer

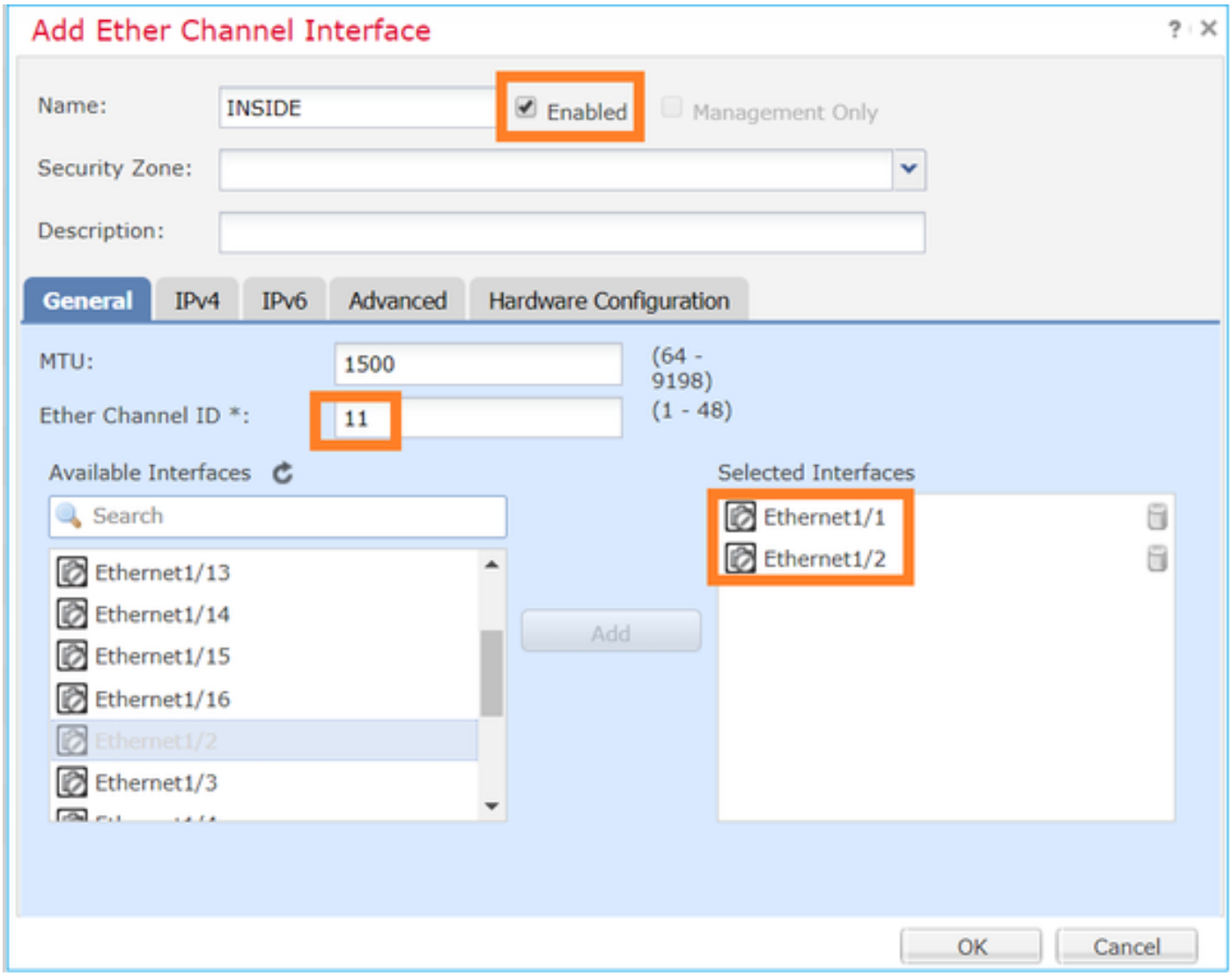
Port-Channel on FPR21xx/FPR1xxx

Network Diagram

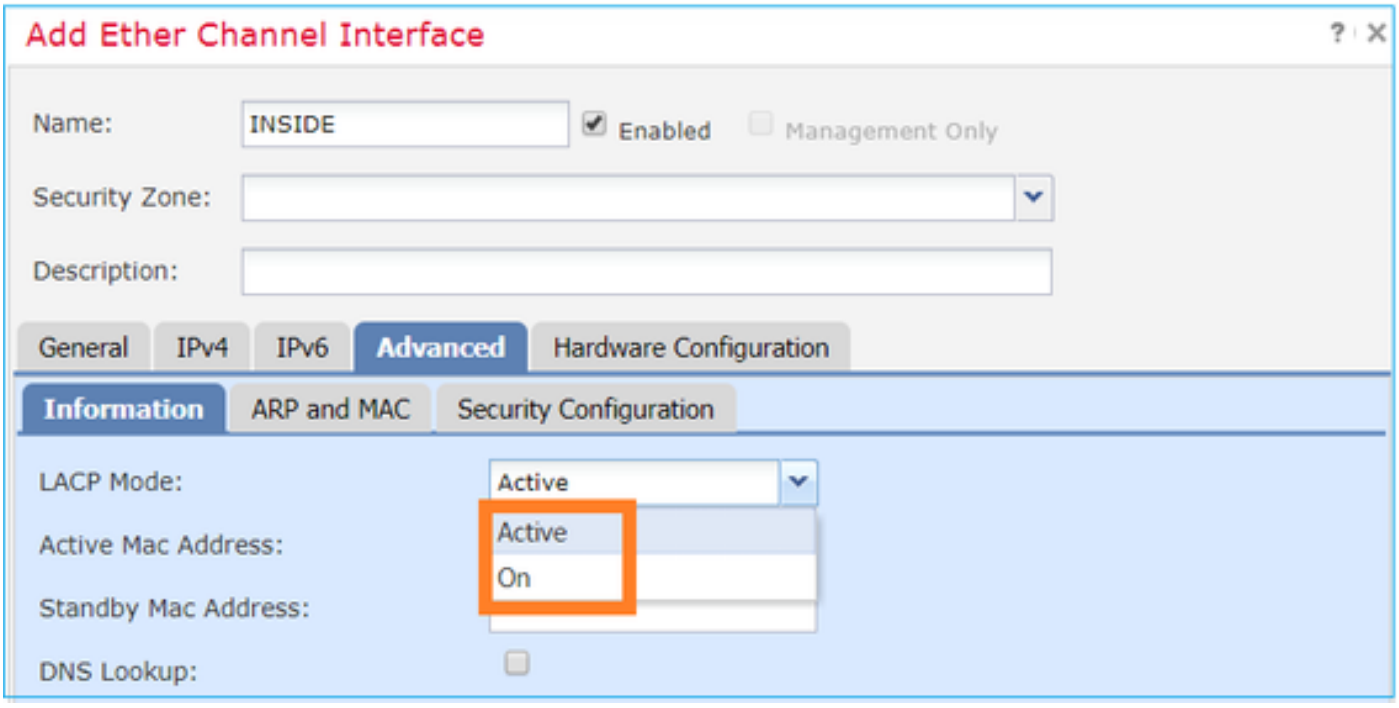


The FTD Port-Channel on FPR21xx/FPR1xxx appliances is managed by the FXOS code, but the configuration is done from the FMC since the FTD and FXOS code is integrated in one software bundle:

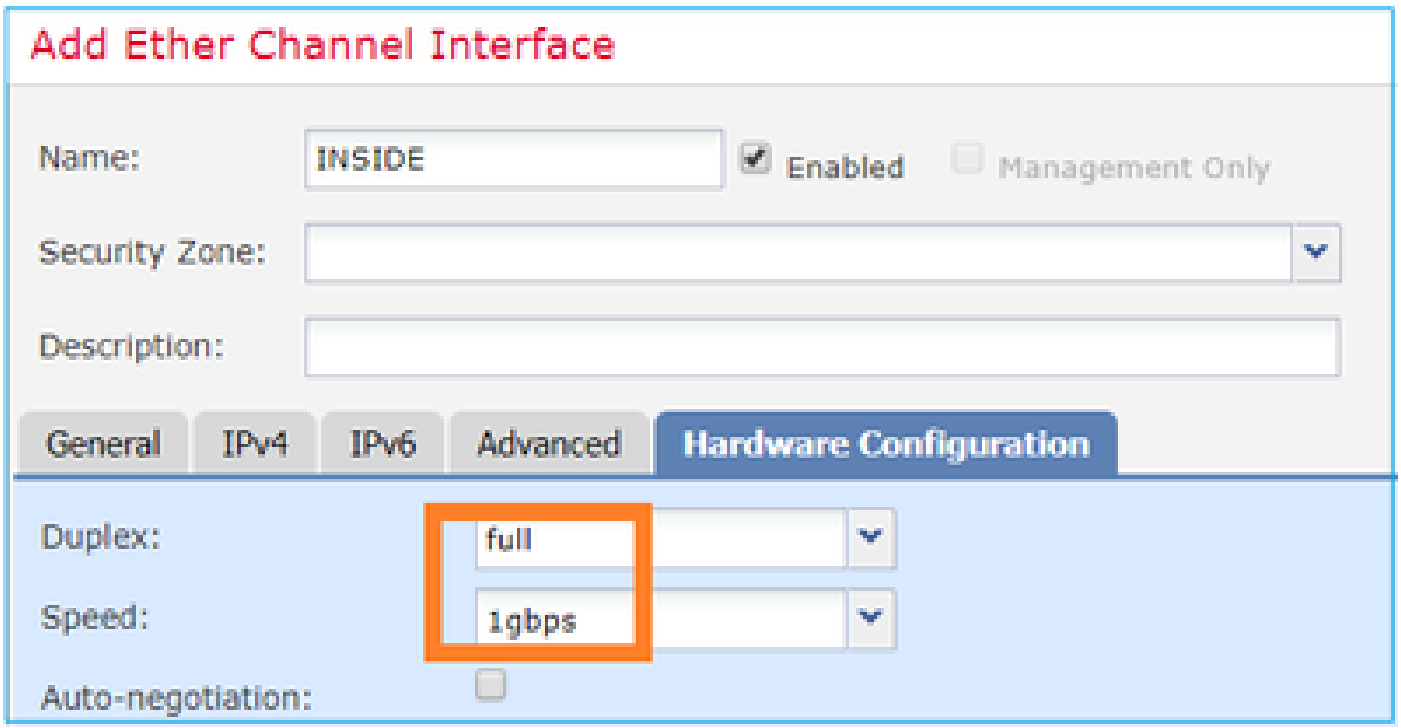


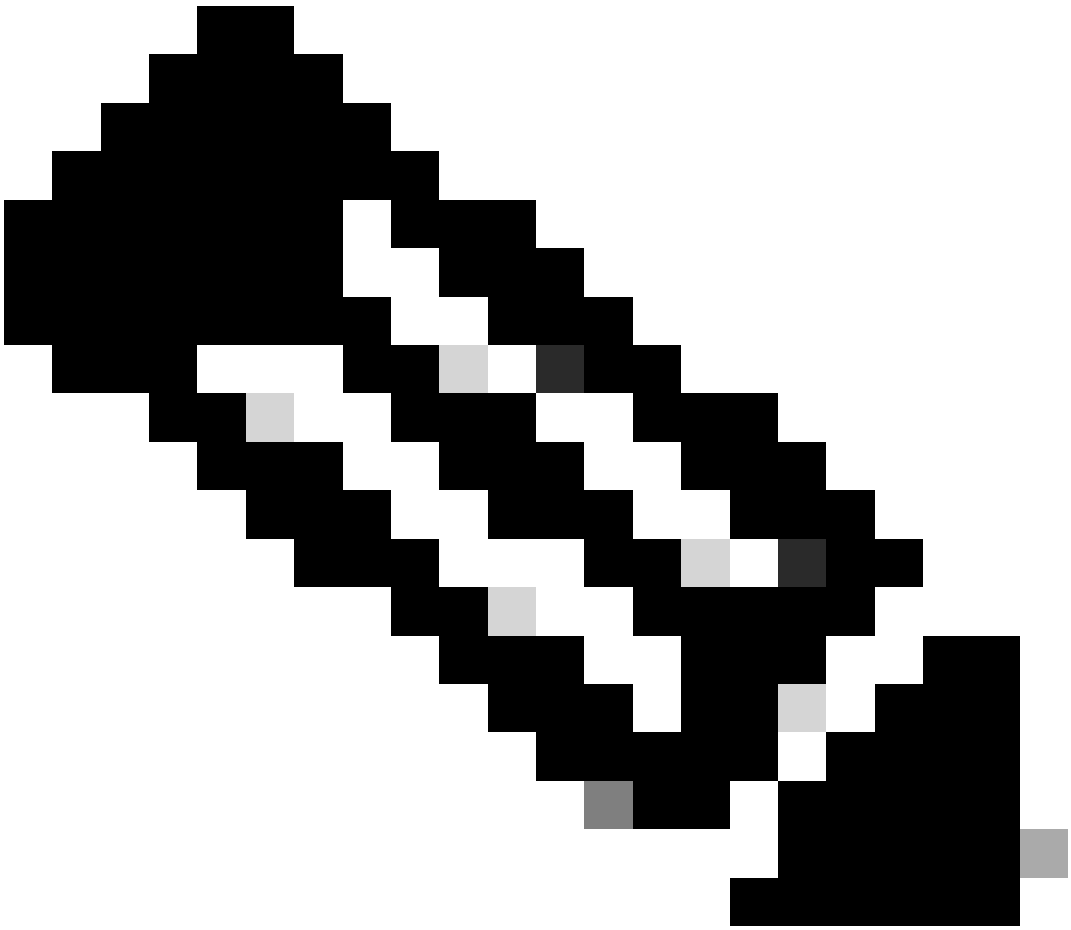


Mode (LACP Active or ON) are configured from the Advanced tab:



Duplex and Speed settings are configured from the Hardware Configuration tab:


Add Ether Channel Interface
Name:
INSIDE
Enabled
Management Only
Security Zone:
Description:
General
IPv4
IPv6
Advanced
Hardware Configuration
Duplex:
full
Speed:
1gbps
Auto-negotiation:



> **Note**: On FPR2100, you cannot create a Port-Channel from FXOS CLI unless you use an ASA as a logical device. After ASA 9.13.x, this is the case only in Platform Mode. In Appliance Mode (11xx/21xx), there is not FCM and all interface configuration is performed directly in the ASA CLI.

<#root>

```
Fp2110 /eth-uplink/fabric* #
```

create port-channel 16

```
Fp2110 /eth-uplink/fabric/port-channel* #
```

create member-port Ethernet1/10

```
Fp2110 /eth-uplink/fabric/port-channel/member-port* #
```

exit

```
Fp2110 /eth-uplink/fabric/port-channel* #
```

create member-port Ethernet1/11

```
Fp2110 /eth-uplink/fabric/port-channel/member-port* #
```

exit

```
Fp2110 /eth-uplink/fabric/port-channel* #
```

commit-buffer

```
Error: Changes not allowed. use: 'connect ftd' to make changes.
```

In case a physical interface is down and you want to enable it do this:

<#root>

```
firepower-2110#
```

scope eth-uplink

```
firepower-2110 /eth-uplink #
```

scope fabric a

```
firepower-2110 /eth-uplink/fabric #
```

show interface

```
Interface:
    Port Name      Port Type          Admin State Oper State       State Reason
    -------------- ------------------ ----------- ---------------- ------------
    Ethernet1/3    Data               Enabled     Up               Up
    Ethernet1/4    Data               Disabled    Link Down        Down
    Ethernet1/5    Data               Disabled    Link Down        Down
    Ethernet1/6    Data               Disabled    Link Down        Down
    Ethernet1/7    Data               Disabled    Link Down        Down
    Ethernet1/8    Data               Disabled    Link Down        Down
    Ethernet1/9    Data               Disabled    Link Down        Down
    Ethernet1/10   Data               Disabled    Link Down        Down
```

```
    Ethernet1/11   Data               Disabled    Link Down        Down
    Ethernet1/12   Data               Disabled    Link Down        Down
    Ethernet1/13   Data               Disabled    Link Down        Down
    Ethernet1/14   Data               Disabled    Link Down        Down
    Ethernet1/15   Data               Disabled    Link Down        Down
    Ethernet1/16   Data               Disabled    Link Down        Down
firepower-2110 /eth-uplink/fabric #
```

```
enter interface Ethernet1/4
```

```
firepower-2110 /eth-uplink/fabric/interface #
```

```
show
```

```
Interface:
    Port Name      Port Type          Admin State Oper State       State Reason
    -------------- ------------------ ----------- ---------------- ------------
    Ethernet1/4    Data               Disabled    Link Down        Down
firepower-2110 /eth-uplink/fabric/interface #
```

```
enable
```

```
firepower-2110 /eth-uplink/fabric/interface* #
```

```
commit-buffer
```

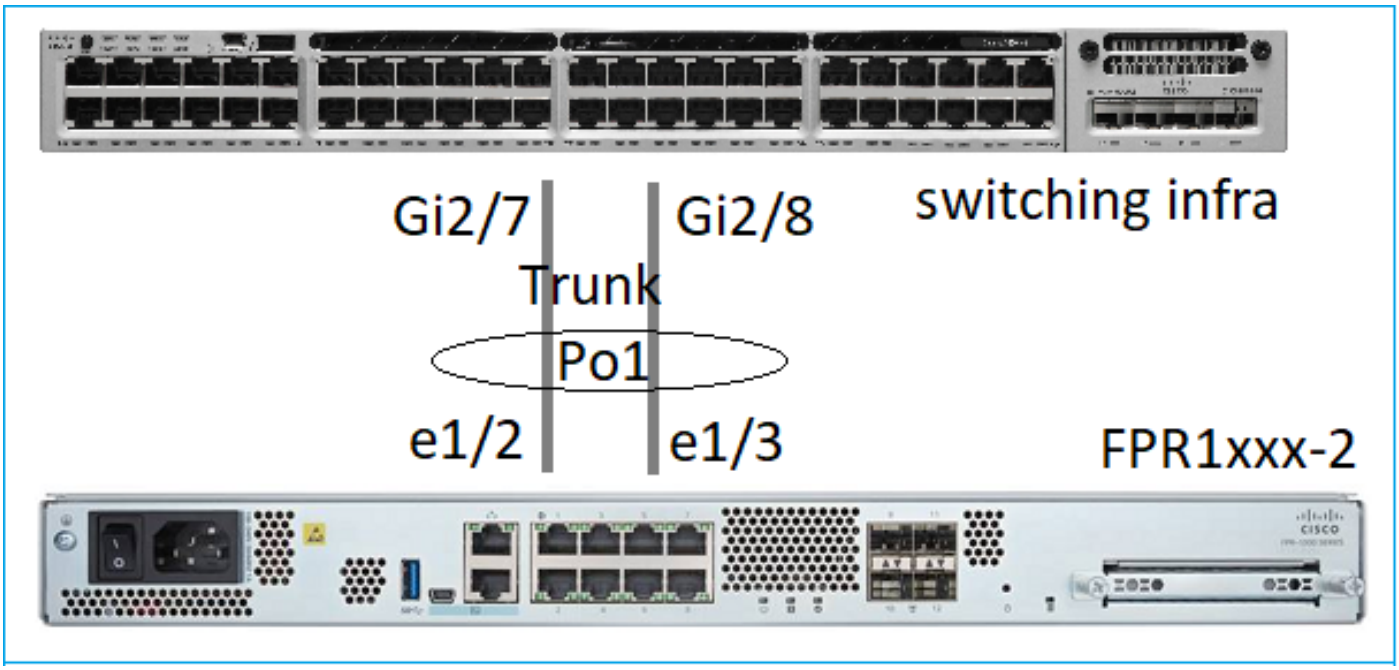
```
firepower-2110 /eth-uplink/fabric/interface #
```

```
show
```

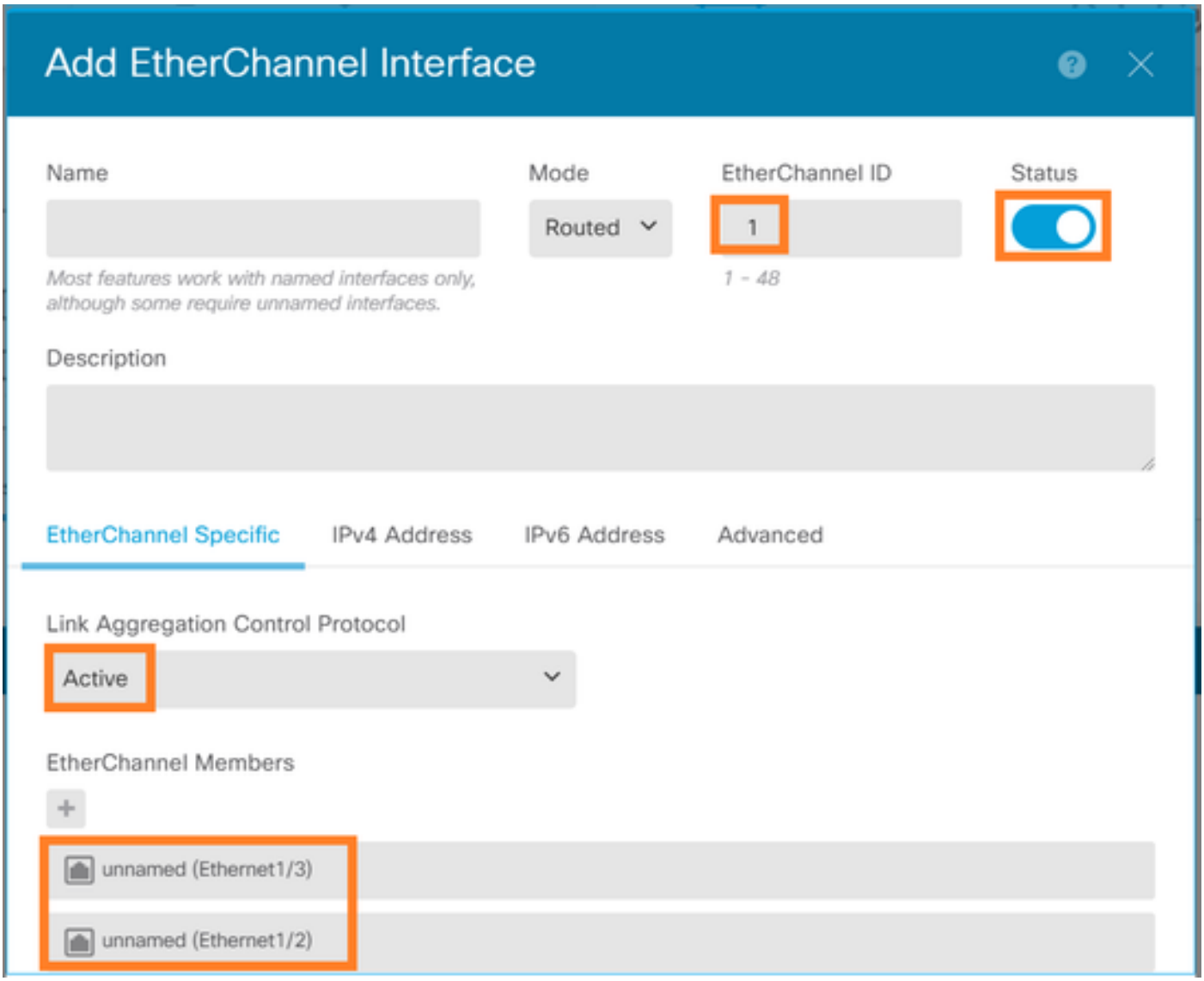
```
Interface:
    Port Name      Port Type          Admin State Oper State       State Reason
    -------------- ------------------ ----------- ---------------- ------------
    Ethernet1/4    Data               Enabled     Link Down        Down
firepower-2110 /eth-uplink/fabric/interface #
```

FDM Configuration

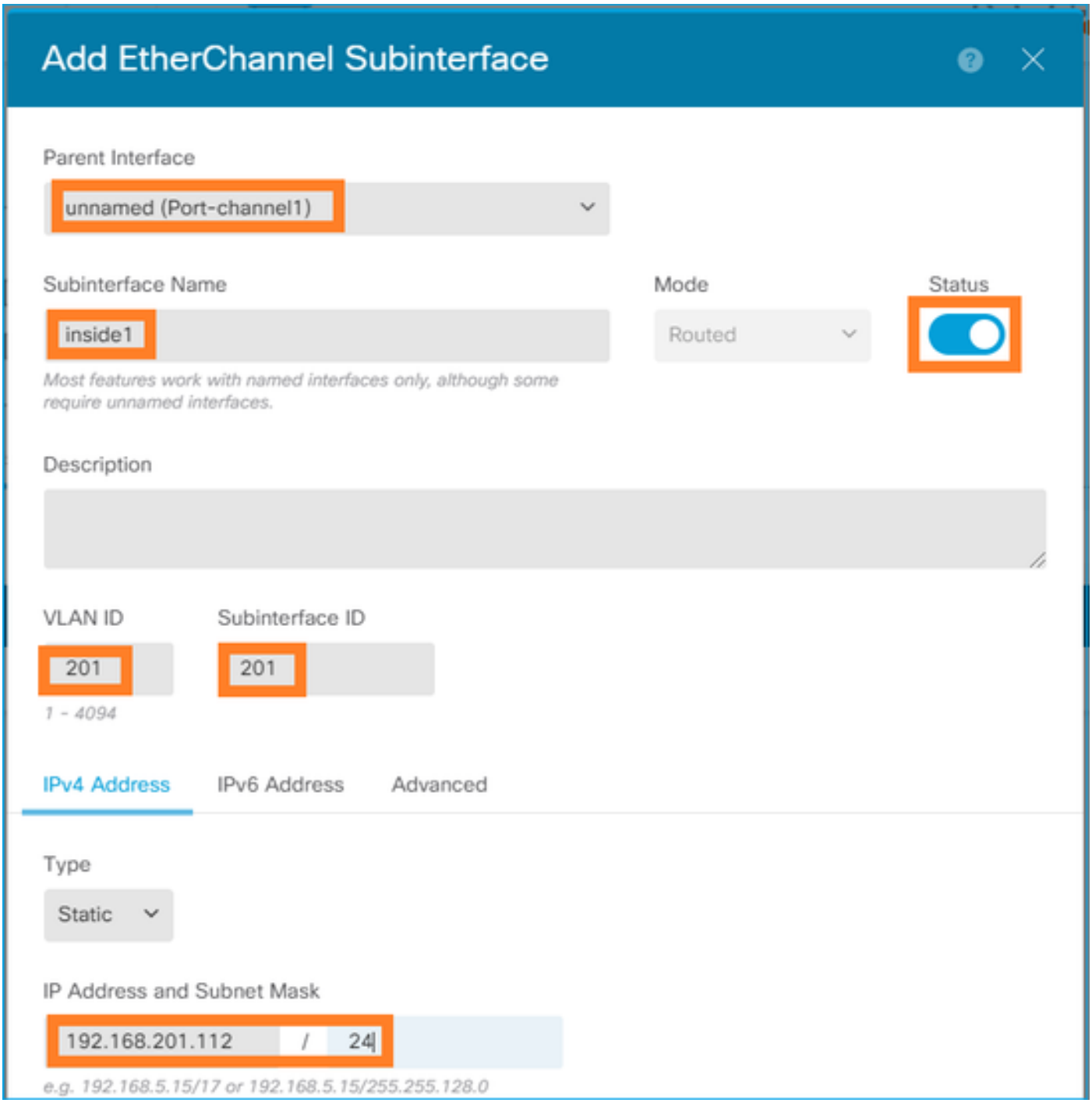
Consider this topology:



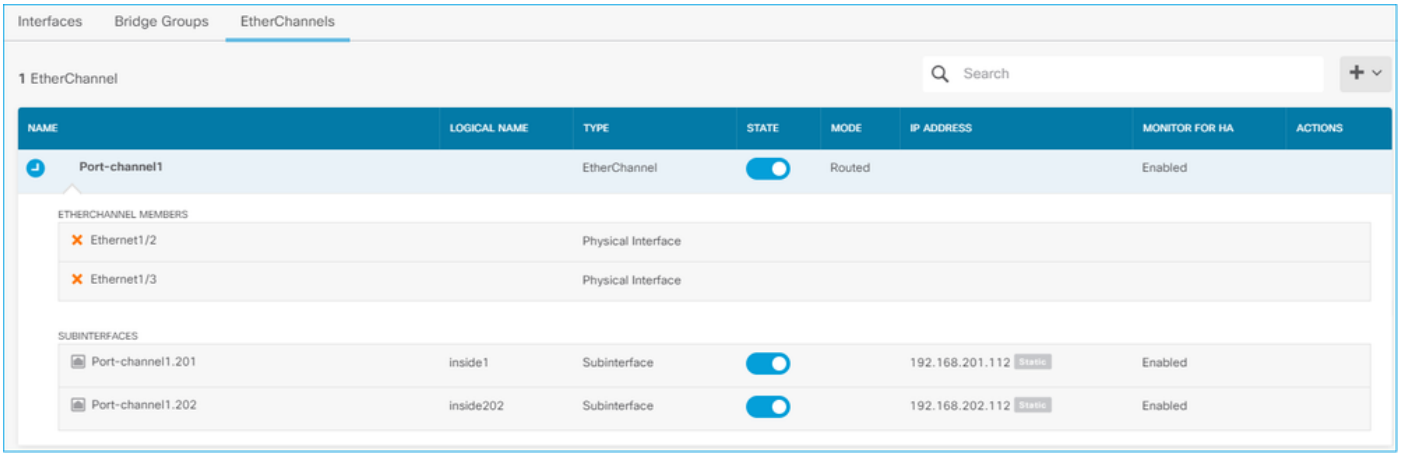
You can configure EtherChannel interfaces that use FDM as from 6.5 software release. Navigate to Device > Interfaces > EtherChannels and add an EtherChannel. Since in this case the EtherChannel is a trunk specify the EtherChannel ID, enable it (Status), and add the members. The EtherChannel supports LACP Active and mode On (no LACP). In this case, LACP Active mode is configured.



Add the Subinterfaces:


Add EtherChannel Subinterface
Parent Interface
unnamed (Port-channel1)
Subinterface Name
inside1
Most features work with named interfaces only, although some require unnamed interfaces.
Mode
Routed
Status
Description
VLAN ID
201
1 - 4094
Subinterface ID
201
IPv4 Address
IPv6 Address
Advanced
Type
Static
IP Address and Subnet Mask
192.168.201.112 / 24
e.g. 192.168.5.15/17 or 192.168.5.15/255.255.128.0

The result:

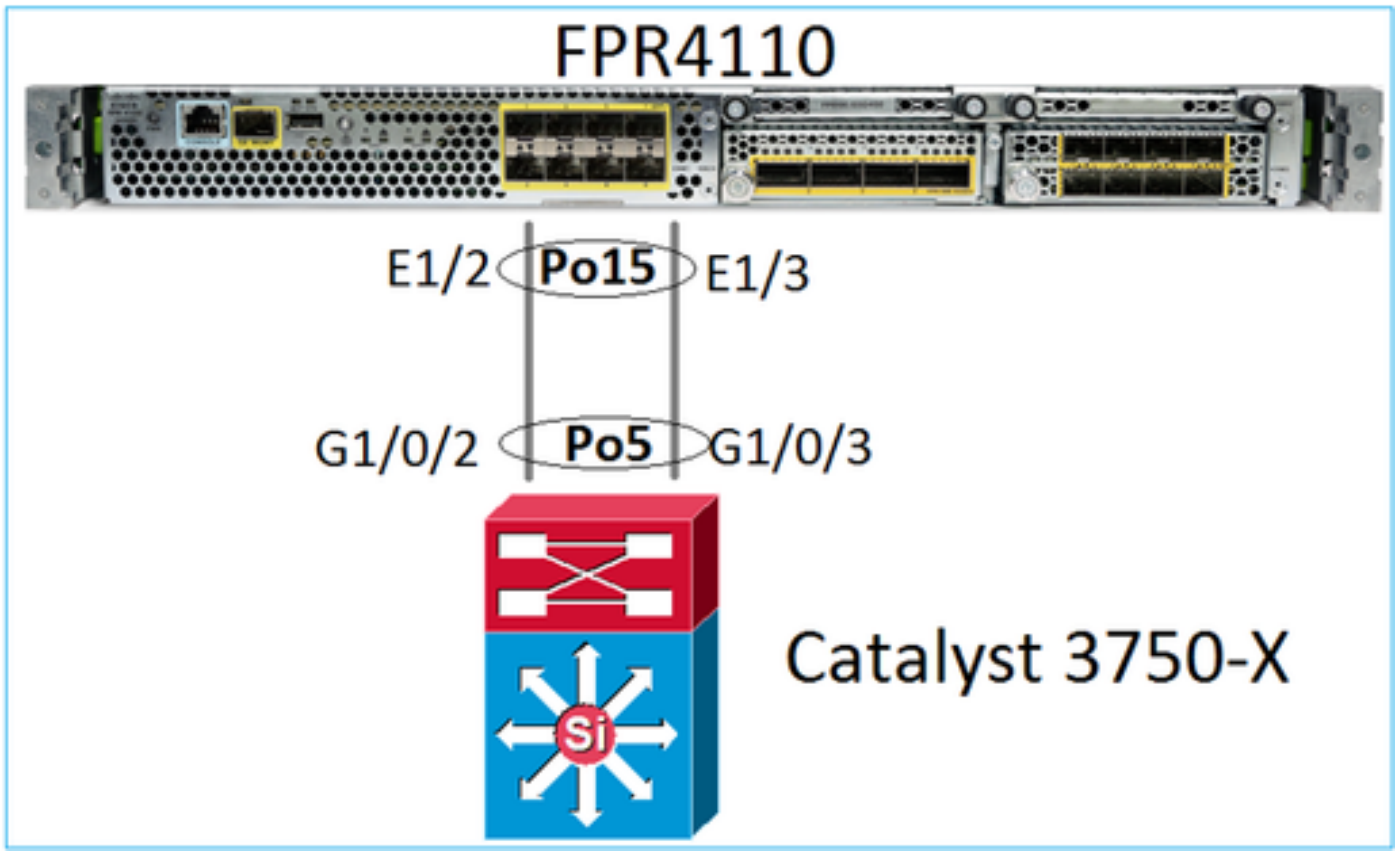

Interfaces
Bridge Groups
EtherChannels
1 EtherChannel
Search
NAME
LOGICAL NAME
TYPE
STATE
MODE
IP ADDRESS
MONITOR FOR HA
ACTIONS
Port-channel1
EtherChannel
Routed
Enabled
ETHERCHANNEL MEMBERS
Ethernet1/2
Physical Interface
Ethernet1/3
Physical Interface
SUBINTERFACES
Port-channel1.201
inside1
Subinterface
192.168.201.112
Enabled
Port-channel1.202
inside202
Subinterface
192.168.202.112
Enabled

Deploy the expected changes.

Verify

Verify Port-Channel on FPR4100/FPR9300

Network Diagram



The FTD (or ASA) is not aware of the Port-Channel individual members. Logical interfaces (subinterfaces) are configured on FMC:

<#root>

>

system support diagnostic-cli

firepower#

show interface ip brief

```
Interface                  IP-Address      OK? Method Status                Protocol
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
Port-channel15             unassigned      YES unset  up                    up
```

```
firepower# show nameif
Interface                  Name                       Security
```

```
Port-channel15           INSIDE                    0
Ethernet1/1              diagnostic                0
```

```
<#root>

firepower#

show interface Port-channel15 detail

Interface Port-channel15 "INSIDE", is up, line protocol is up
  Hardware is EtherSVI, BW 20000 Mbps, DLY 1000 usec
        MAC address 2c33.118e.07de, MTU 1500
        IP address unassigned
  Traffic Statistics for "INSIDE":
        6767 packets input, 566328 bytes
        0 packets output, 0 bytes
        6736 packets dropped
      1 minute input rate 4 pkts/sec,  375 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 4 pkts/sec
      5 minute input rate 4 pkts/sec,  401 bytes/sec
      5 minute output rate 0 pkts/sec,  0 bytes/sec
      5 minute drop rate, 4 pkts/sec
  Control Point Interface States:
        Interface number is 6
        Interface config status is active
        Interface state is active
```

To check the status of the Port-Channel and its members, navigate to **FXOS** mode:

```
<#root>

FP4110-7-A#

connect fxos

FP4110-7-A(fxos)#

show port-channel summary

Flags:  D - Down        P - Up in port-channel (members)
        I - Individual  H - Hot-standby (LACP only)
        s - Suspended   r - Module-removed
        S - Switched    R - Routed
        U - Up (port-channel)
        M - Not in use. Min-links not met
--------------------------------------------------------------------------------
Group Port-       Type     Protocol  Member Ports
      Channel
--------------------------------------------------------------------------------
15    Po15(SU)    Eth      LACP      Eth1/2(P)    Eth1/3(P)
48    Po48(SD)    Eth      NONE      --
```

To see the state of the Port-Channels along with last state history:

```
<#root>
```

```
FP4110-7-A(fxos)#
```

show port-channel database

```
port-channel15
    Last membership update is successful
    2 ports in total, 2 ports up
    First operational port is Ethernet1/3
    Age of the port-channel is 0d:00h:35m:00s
    Time since last bundle is 0d:00h:34m:56s
    Last bundled member is Ethernet1/3
    Ports:   Ethernet1/2     [active ] [up]
             Ethernet1/3     [active ] [up] *

port-channel48
    Last membership update is successful
    0 ports in total, 0 ports up
    Age of the port-channel is 5d:06h:35m:27s
```

To check traffic distribution among Port-Channel interface members:

<#root>

```
FP4110-7-A(fxos)#
```

show port-channel traffic

```
ChanId      Port Rx-Ucst Tx-Ucst Rx-Mcst Tx-Mcst Rx-Bcst Tx-Bcst
------ --------- ------- ------- ------- ------- ------- -------
    15    Eth1/2  20.83%  49.71%  17.75%  43.67%  20.11%  49.94%
    15    Eth1/3  79.16%  50.28%  82.24%  56.32%  79.88%  50.05%
```

LACP neighbor verification

<#root>

```
FP4110-7-A(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-channel15 neighbors
Partner's information
            Partner                Partner                     Partner
Port        System ID              Port Number     Age         Flags
Eth1/2      32768,28-6f-7f-ec-59-800x103           1984        FA

            LACP Partner           Partner                     Partner
            Port Priority          Oper Key                    Port State
            32768                  0x5                         0x3f

Partner's information
            Partner                Partner                     Partner
Port        System ID              Port Number     Age         Flags
Eth1/3      32768,28-6f-7f-ec-59-800x104           2221        FA

            LACP Partner           Partner                     Partner
```

```
            Port Priority          Oper Key                    Port State
            32768                  0x5                         0x3f
```

Partner Oper Key 0x5 = The switch is configured with Port-Channel ID 5.

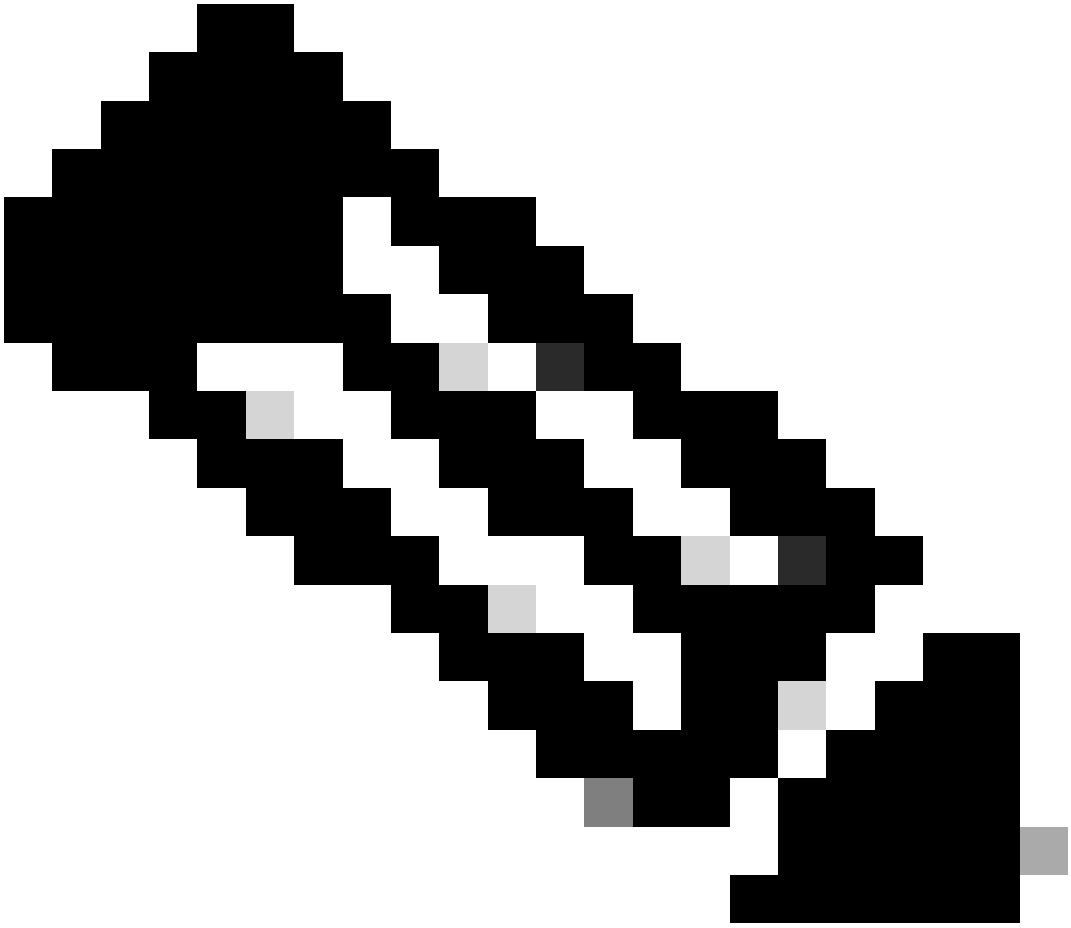
On the switch:

<#root>

```
Switch#
```

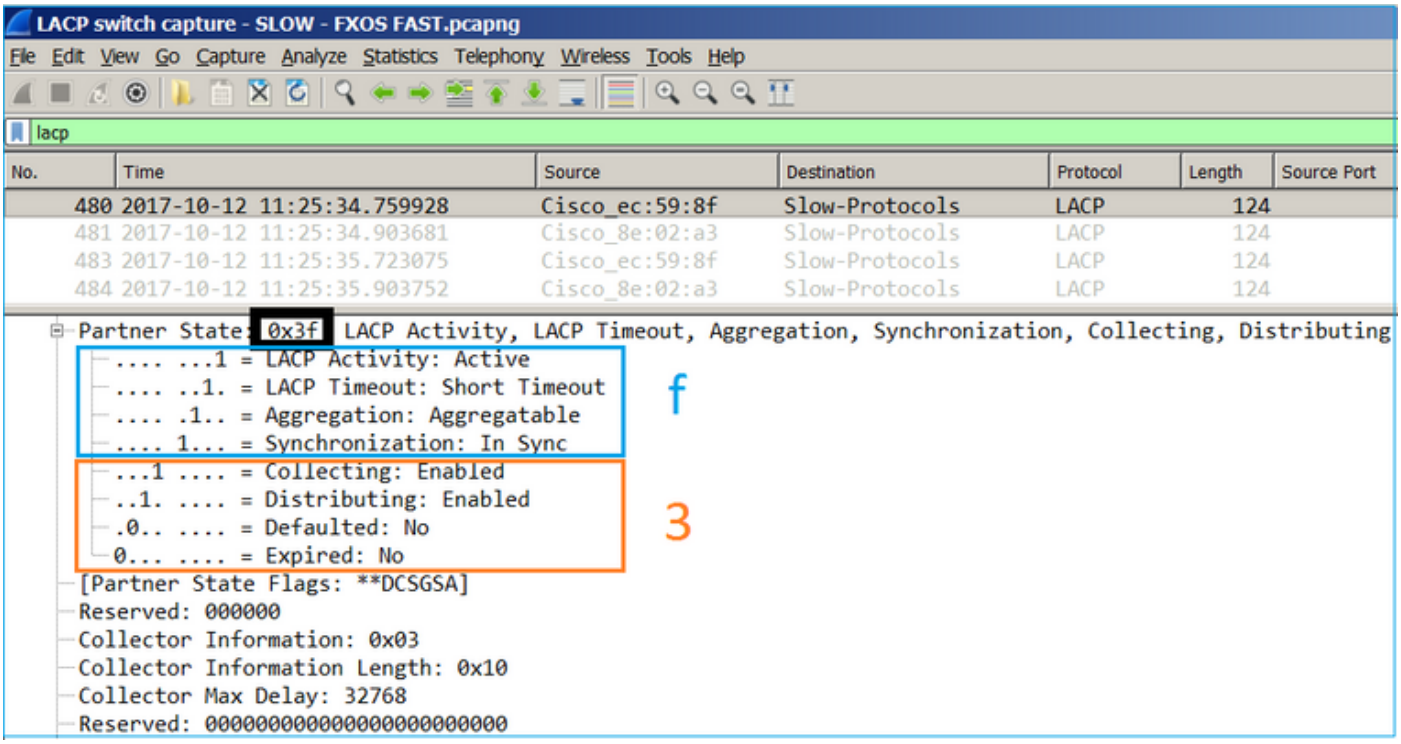
show lacp neighbor

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

Channel group 5 neighbors

Partner's information:

                  LACP port                        Admin  Oper   Port    Port
Port      Flags   Priority  Dev ID          Age    key    Key    Number  State
Gi1/0/2   FA      32768     2c33.118e.07b3   0s    0x0    0xE    0x42    0x3F
Gi1/0/3   FA      32768     2c33.118e.07b3   0s    0x0    0xE    0x43    0x3F
```



Note: On the adjacent Switch, the Partner Oper Key is shown as 0xE (14) although FXOS is configured with Port-Channel ID 15.

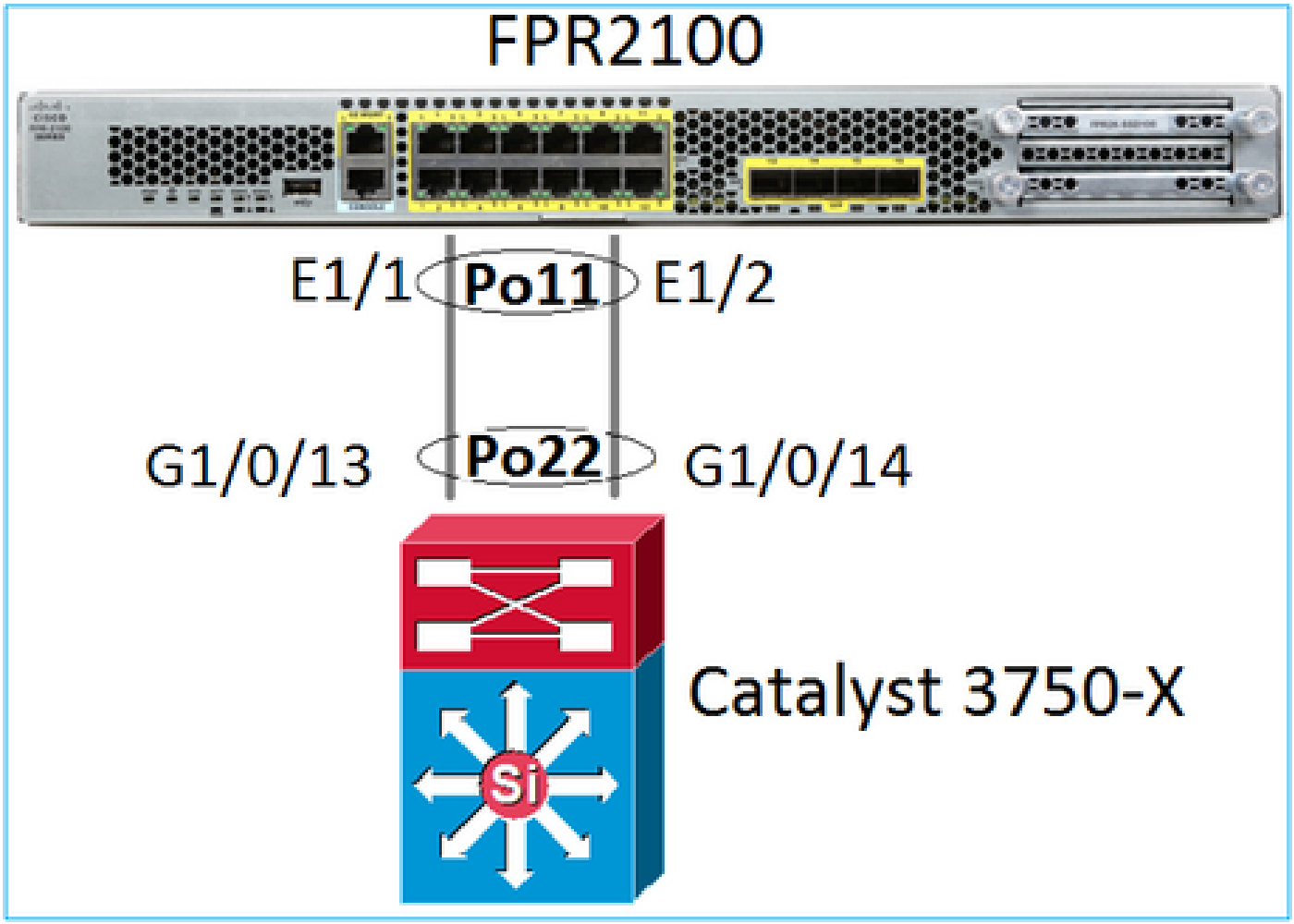
LACP packet capture in Wireshark:



	Partner State							
State	Expired	Defaulted	Distributed	Collected	Synchronization	Aggregation	LACP Timeout	LACP Activity
Value	0	0	1	1	1	1	1	1
Hex	3				f			

Verify Port-Channel on FPR21xx/FPR1xxx

Network Diagram



Port-Channel basic verification

<#root>

>

connect fxos

FP2110-2#

connect local-mgmt

FP2110-2(local-mgmt)#

show portchannel summary

```
Flags:  D - Down        P - Up in port-channel (members)
I - Individual  H - Hot-standby (LACP only)
s - Suspended   r - Module-removed
S - Switched    R - Routed
U - Up (port-channel)
M - Not in use. Min-links not met
--------------------------------------------------------------------------------
Group Port-       Type     Protocol  Member Ports
      Channel
--------------------------------------------------------------------------------
11    Po11(U)     Eth      LACP      Eth1/1(P)    Eth1/2(P)
```

Additional verification:

```
<#root>

FP2110-2#

scope eth-uplink

FP2110-2 /eth-uplink #

scope fabric a

FP2110-2 /eth-uplink/fabric #

show port-channel


Port Channel:
    Port Channel Id Name             Port Type          Admin State Oper State       State Reason
    --------------- ---------------- ------------------ ----------- ---------------- ------------
    11              Port-channel11   Data               Enabled     Up               Up
```

Verify the Port-Channel details:

```
<#root>

FP2110-2 /eth-uplink/fabric #

show port-channel detail


Port Channel:
    Port Channel Id: 11
    Name: Port-channel11
    Port Type: Data
    Description:
    Admin State: Enabled
    Oper State: Up
    Auto negotiation: Yes
    Speed: 1 Gbps
    Duplex: Full Duplex
    Oper Speed: 1 Gbps
    Band Width (Gbps): 2
    State Reason: Up
    flow control policy: default
    LACP policy name: default
    oper LACP policy name: org-root/lacp-default
    Lacp Mode: Active
    Inline Pair Admin State: Enabled
    Inline Pair Peer Port Name:
```

Verify the Port-Channel member details:

```
<#root>

FP2110-2#
```

```
scope eth-uplink

FP2110-2 /eth-uplink #
scope fabric a

FP2110-2 /eth-uplink/fabric #
scope port-channel 11
FP2110-2 /eth-uplink/fabric/port-channel #
show member-port

Member Port:
    Port Name       Membership         Oper State       State Reason
    --------------- ------------------ ---------------- ------------
    Ethernet1/1     Up                 Up               Up
    Ethernet1/2     Up                 Up               Up
```

Member port details:

<#root>

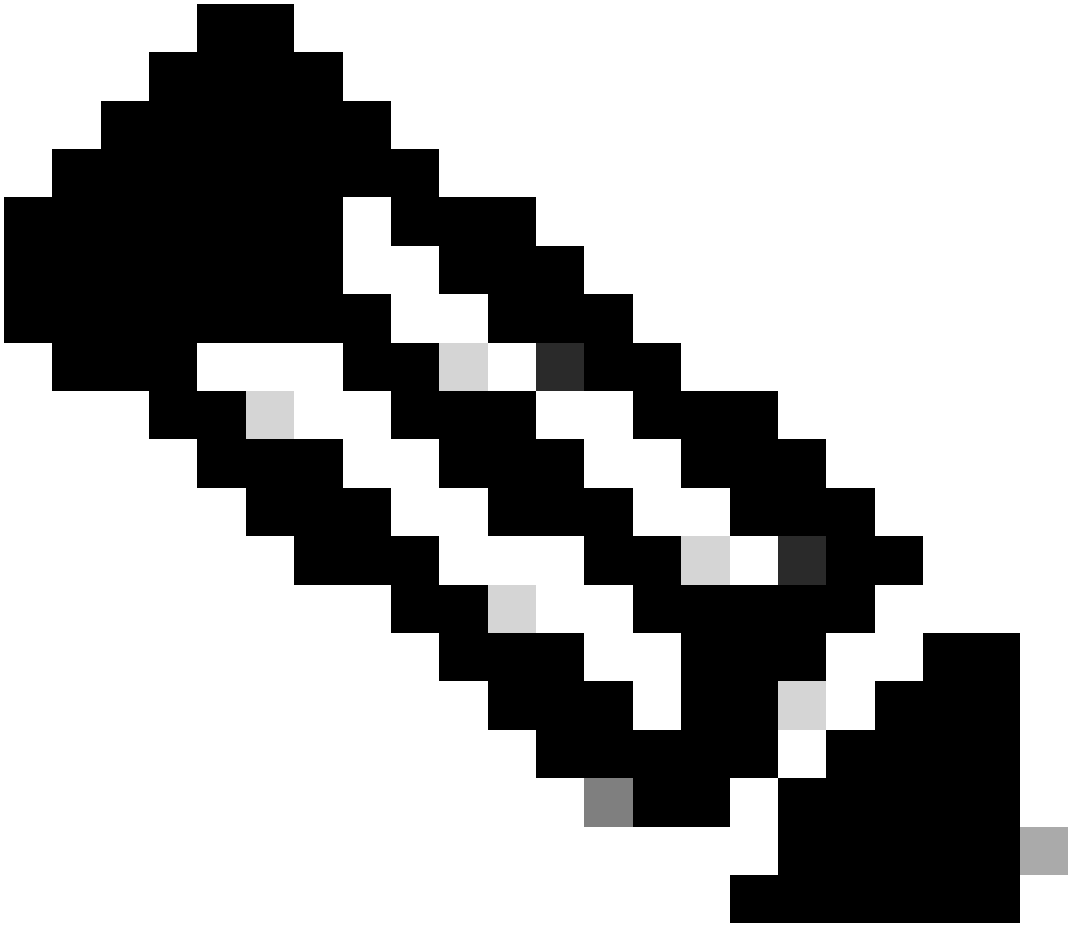
```
FP2110-2 /eth-uplink/fabric/port-channel #
show member-port detail

Member Port:
    Port Name: Ethernet1/1
    Membership: Up
    Oper State: Up
    State Reason: Up
    Ethernet Link Profile name: default
    Oper Ethernet Link Profile name: fabric/lan/eth-link-prof-default
    Udld Oper State: Unknown
    Current Task:

    Port Name: Ethernet1/2
    Membership: Up
    Oper State: Up
    State Reason: Up
    Ethernet Link Profile name: default
    Oper Ethernet Link Profile name: fabric/lan/eth-link-prof-default
    Udld Oper State: Unknown
    Current Task:
```

LACP verification

<#root>

```
FP2110-2(local-mgmt)#
show lacp neighbor
```

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

Channel group: 11

Partner (internal) information:

          Partner                Partner                       Partner
Port      System ID              Port Number     Age         Flags
Eth1/1    32768,286f.7fec.5980   0x10e           13 s        FA <-- the peer is requesting Fast Rate


          LACP Partner           Partner           Partner
          Port Priority        Oper Key        Port State
          32768                0x16            0x3f

          Port State Flags Decode:
          Activity:   Timeout:   Aggregation:   Synchronization:
          Active      Long       Yes            Yes

          Collected:   Distributing:   Defaulted:   Expired:
          Yes           Yes             No           No

          Partner                Partner                       Partner
Port      System ID              Port Number     Age         Flags
Eth1/2    32768,286f.7fec.5980   0x10f           5  s        FA <-- the peer is requesting Fast Rate


          LACP Partner           Partner           Partner
          Port Priority        Oper Key        Port State
          32768                0x16            0x3f

          Port State Flags Decode:
          Activity:   Timeout:   Aggregation:   Synchronization:
          Active      Long       Yes            Yes

          Collected:   Distributing:   Defaulted:   Expired:
          Yes           Yes             No           No
```



Note: On FPR21xx/FPR1xxx, the default LACP rate is Slow and cannot be changed.

LACP counters

<#root>

```
FP2110-2(local-mgmt)#
```

show lacp counters

```
            LACPDUs         Marker      Marker Response    LACPDUs
Port       Sent   Recv     Sent   Recv     Sent    Recv      Pkts Err
--------------------------------------------------------------------
Channel group: 11
Eth1/1     4435   3532     0      0        0       0         0
Eth1/2     4566   3532     0      0        0       0         0
FP2110-2(local-mgmt)#
```

show lacp counters

```
            LACPDUs         Marker      Marker Response    LACPDUs
Port       Sent   Recv     Sent   Recv    Sent    Recv      Pkts Err
--------------------------------------------------------------------
Channel group: 11
Eth1/1     4436   3532     0      0       0       0         0
Eth1/2     4567   3532     0      0       0       0         0
```

FPR2100 interface verification

How the physical interfaces map to the FPR2100 internal Switch:

Interface	Internal Switch on FPR2110/FPR2120	Internal Switch on FPR2130/FPR2140
E1/1	1	1
E1/2	0	0
E1/3	3	3
E1/4	2	2
E1/5	5	5
E1/6	4	4
E1/7	7	7
E1/8	6	6
E1/9	9	49
E1/10	8	48
E1/11	11	51
E1/12	10	50
E1/13	12	59

E1/14	13	58
E1/15	14	57
E1/16	15	56
E2/1	-	70
E2/2	-	71
E2/3	-	69
E2/4	-	68
E2/5	-	66
E2/6	-	67
E2/7	-	65
E2/8	-	64

Verify the physical interface status:

<#root>

```
FP2110-2(local-mgmt)#
```

show portmanager port-info ethernet 1 1

```
port_info:
        if_index:    0x1081000
        type:        PORTMGR_IPC_MSG_PORT_TYPE_PHYSICAL
        mac_address: 70:df:2f:18:d8:04
        flowctl:     PORTMGR_IPC_MSG_FLOWCTL_NONE
        role:        PORTMGR_IPC_MSG_PORT_ROLE_NPU
        admin_state: PORTMGR_IPC_MSG_PORT_STATE_ENABLED
        oper_state:  PORTMGR_IPC_MSG_PORT_STATE_UP
        admin_speed: PORTMGR_IPC_MSG_SPEED_AUTO
        oper_speed:  PORTMGR_IPC_MSG_SPEED_1GB
        admin_mtu:   9216
        admin_duplex: PORTMGR_IPC_MSG_PORT_DUPLEX_FULL
        oper_duplex: PORTMGR_IPC_MSG_PORT_DUPLEX_FULL
        pc_if_index: 0x200000b
        pc_membership_status: PORTMGR_IPC_MSG_MMBR_UP
        pc_protocol: PORTMGR_IPC_MSG_PORT_CHANNEL_PRTCL_LACP_ACTIVE
        native_vlan: 1011
```

```
        num_allowed_vlan: 1
                allowed_vlan[0]: 1011
```

Physical interface counters:

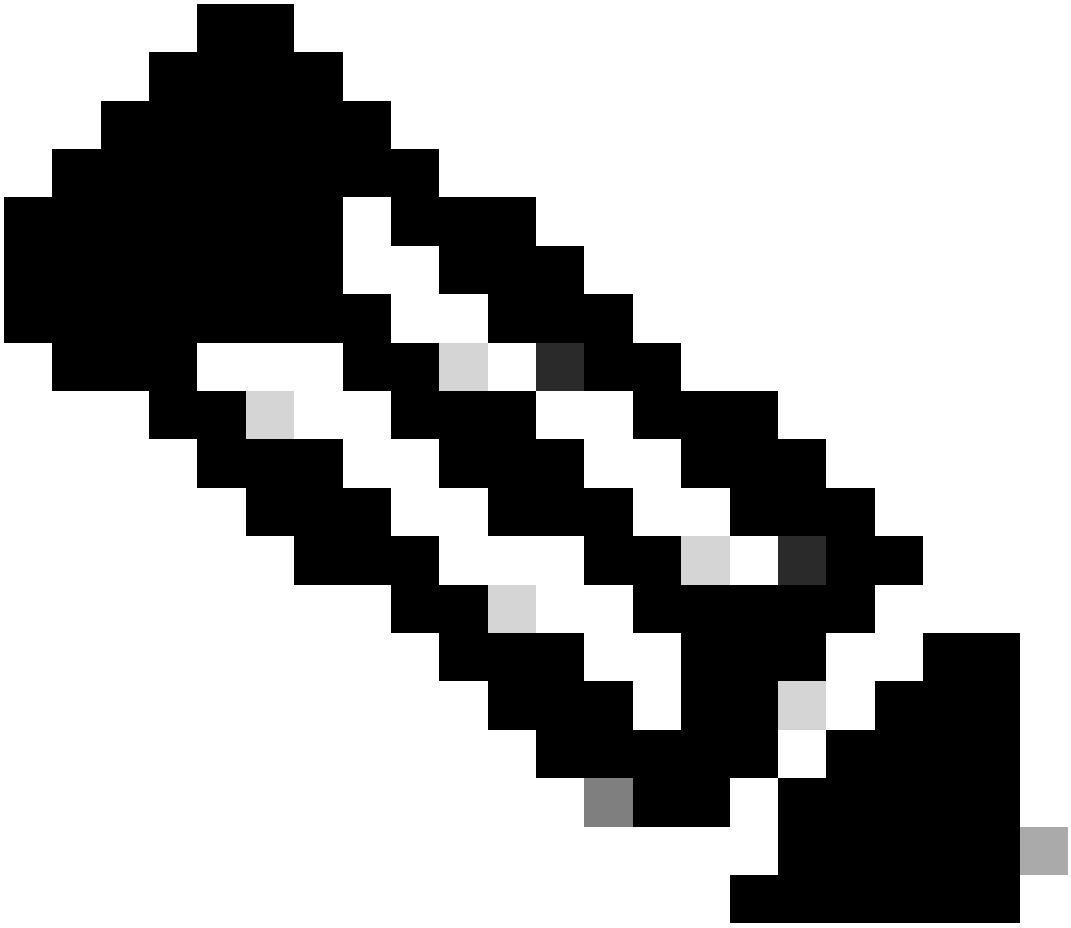
<#root>

```
FP2110-2(local-mgmt)#
```

```
show portmanager counters ethernet 1 1
```

```
Good Octets Received                              : 2692986
Bad Octets Received                               : 0
MAC Transmit Error                                : 0
Good Packets Received                             : 37038
Bad Packets Received                              : 0
BRDC Packets Received                             : 22290
MC Packets Received                               : 12538
Size 64                                           : 34193
Size 65 to 127                                    : 1531
Size 128 to 255                                   : 1515
Size 256 to 511                                   : 374
Size 512 to 1023                                  : 95
Size 1024 to Max                                  : 0
Good Octets Sent                                  : 87296
Good Packets Sent                                 : 682
Excessive Collision                               : 0
MC Packets Sent                                   : 682
BRDC Packets Sent                                 : 0
Unrecognized MAC Received                         : 0
FC Sent                                           : 0
Good FC Received                                  : 0
Drop Events                                       : 0
Undersize Packets                                 : 0
Fragments Packets                                 : 0
Oversize Packets                                  : 0
Jabber Packets                                    : 0
MAC RX Error Packets Received                     : 0
Bad CRC                                           : 0
Collisions                                        : 0
```

FPR2100 internal switch MAC table.



Note: 01:80:C2:00:00:02 = LACP

<#root>

```
FP2110-2(local-mgmt)#
```

```
show portmanager switch mac-filters
```

```
port ix          MAC               mask        action      packets       bytes

00   03e  70:DF:2F:18:D8:05  FF:FF:FF:FF:FF:FF  FORWARD
     043  01:80:C2:00:00:02  FF:FF:FF:FF:FF:FF  FORWARD         687       87936
     044  70:DF:2F:18:D8:2D  FF:FF:FF:FF:FF:FF  FORWARD
     045  FF:FF:FF:FF:FF:FF  FF:FF:FF:FF:FF:FF  FORWARD        5501      385360
     3d0  00:00:00:00:00:00  01:00:00:00:00:00  DROP           2101      141426
     3e8  01:00:00:00:00:00  01:00:00:00:00:00  DROP           7946     1524820

01   03f  70:DF:2F:18:D8:04  FF:FF:FF:FF:FF:FF  FORWARD
     040  01:80:C2:00:00:02  FF:FF:FF:FF:FF:FF  FORWARD         687       87936
     041  70:DF:2F:18:D8:2D  FF:FF:FF:FF:FF:FF  FORWARD
     042  FF:FF:FF:FF:FF:FF  FF:FF:FF:FF:FF:FF  FORWARD       22351     1451504
     3d1  00:00:00:00:00:00  01:00:00:00:00:00  DROP           2215      154542
     3e9  01:00:00:00:00:00  01:00:00:00:00:00  DROP          11886     1006067
```

```
02   03c  70:DF:2F:18:D8:07  FF:FF:FF:FF:FF:FF  FORWARD
     049  01:80:C2:00:00:02  FF:FF:FF:FF:FF:FF  FORWARD
     04a  70:DF:2F:18:D8:6D  FF:FF:FF:FF:FF:FF  FORWARD
     04b  FF:FF:FF:FF:FF:FF  FF:FF:FF:FF:FF:FF  FORWARD
     3d2  00:00:00:00:00:00  01:00:00:00:00:00  DROP
     3ea  01:00:00:00:00:00  01:00:00:00:00:00  DROP
```

Ports e1/1 and e1/2 correspond to 0/0 and 0/1 on the internal switch:

<#root>

```
FP2110-2(local-mgmt)#
```

show portmanager switch status

```
Dev/Port         Mode        Link   Speed  Duplex  Loopback Mode
---------  ----------------  -----  -----  ------  -------------

0/0             QSGMII        Up     1G     Full    None
0/1             QSGMII        Up     1G     Full    None
0/2             QSGMII       Down    1G     Half    None
0/3             QSGMII       Down    1G     Half    None
0/4             QSGMII       Down    1G     Half    None
0/5             QSGMII       Down    1G     Half    None
0/6             QSGMII       Down    1G     Half    None
0/7             QSGMII       Down    1G     Half    None
0/8             QSGMII       Down    1G     Half    None
0/9             QSGMII       Down    1G     Half    None
0/10            QSGMII       Down    1G     Half    None
0/11            QSGMII       Down    1G     Half    None
0/12            QSGMII       Down    10     Half    None
0/13            QSGMII       Down    10     Half    None
0/14            QSGMII       Down    10     Half    None
0/15            QSGMII       Down    10     Half    None
0/16             n/a         Down    n/a    Full    N/A
0/17             n/a         Down    n/a    Full    N/A
0/18             n/a         Down    n/a    Full    N/A
0/19             n/a         Down    n/a    Full    N/A
0/20             n/a         Down    n/a    Full    N/A
0/21             n/a         Down    n/a    Full    N/A
0/22             n/a         Down    n/a    Full    N/A
0/23             n/a         Down    n/a    Full    N/A
0/24              KR          Up     10G    Full    None
0/25              KR          Up     10G    Full    None
0/26              KR         Down    10G    Full    None
0/27              KR          Up     10G    Full    None
```

Troubleshoot

LACP Overview

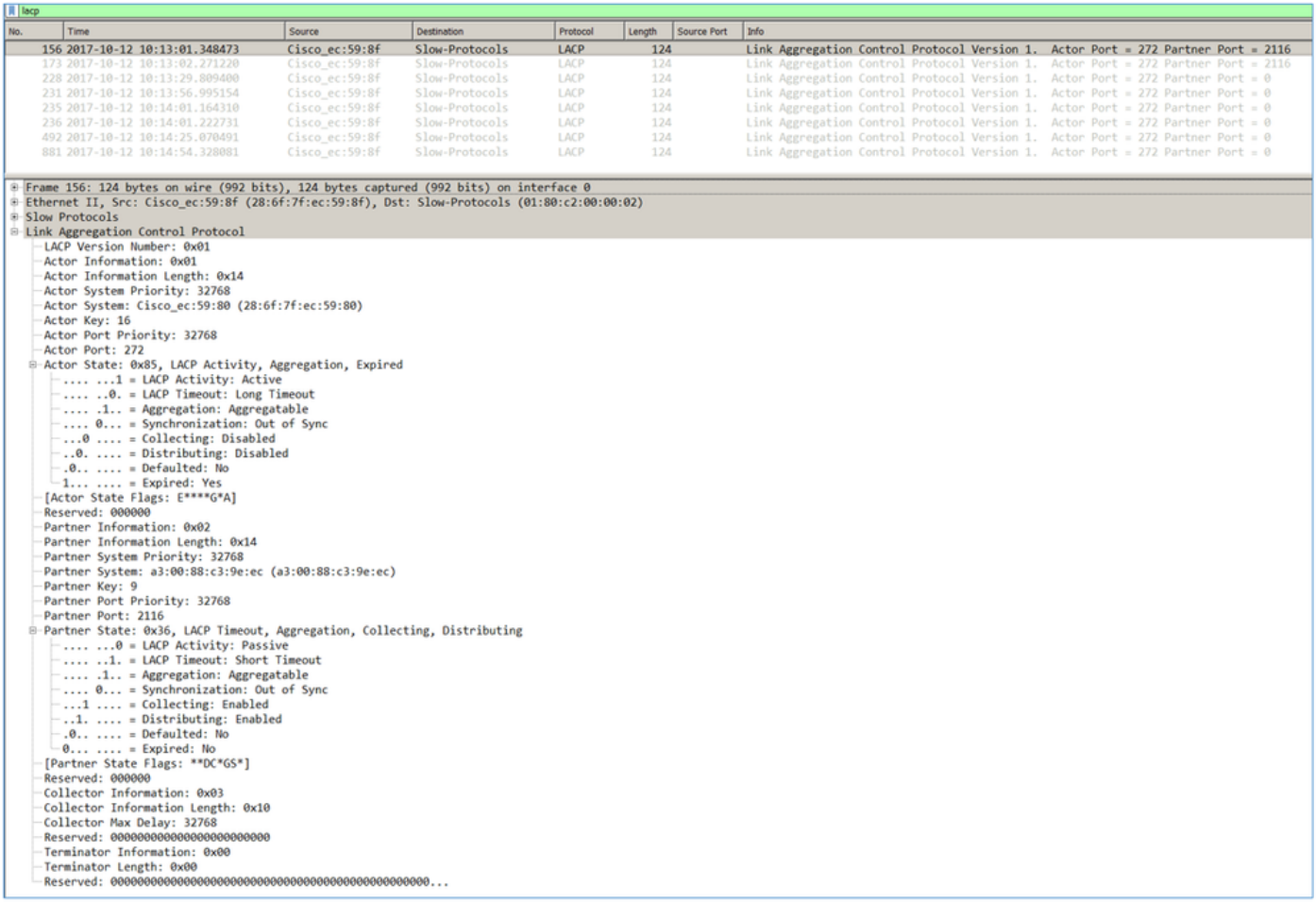
LACP Facts:

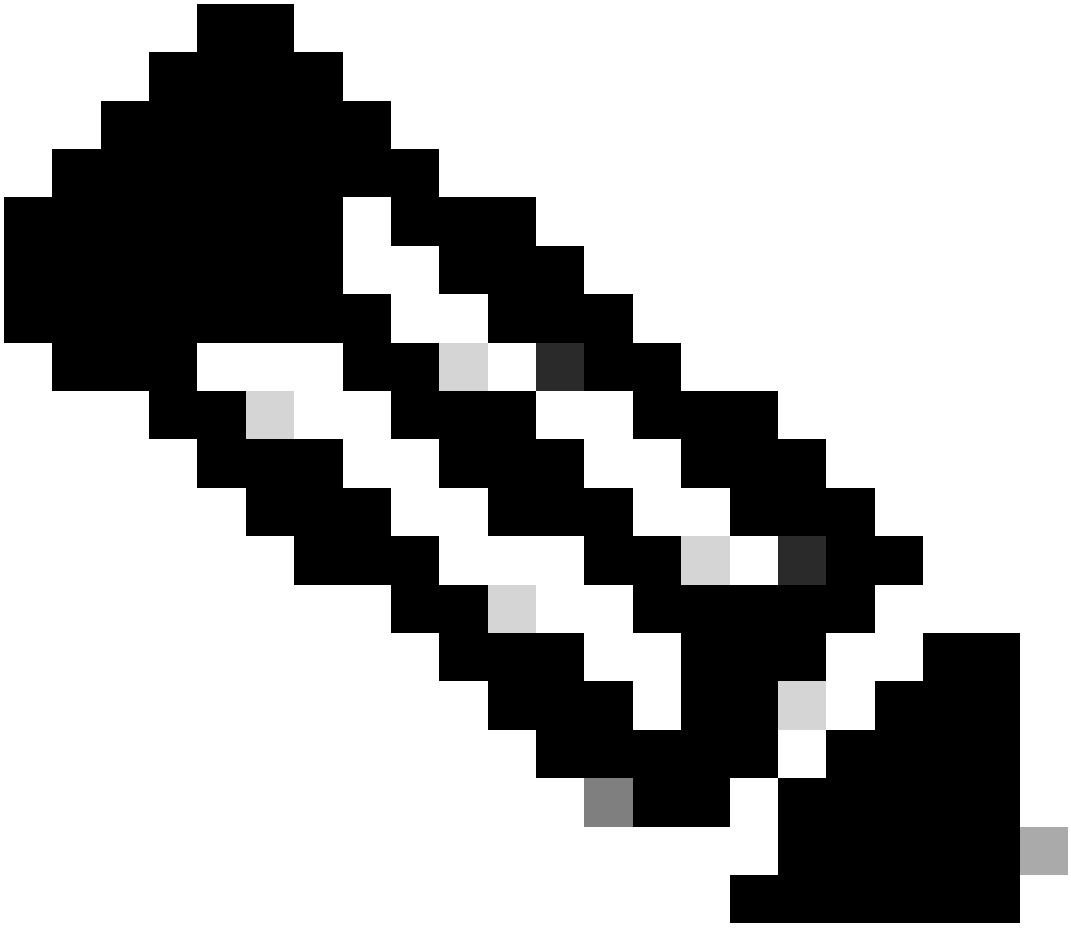
- IEEE standard (802.3ad) Link Aggregation Control Protocol (LACP) is a L2 protocol used for Port-Channel negotiation.
- LACP uses destination MAC 0180.c200.0002 and Ethernet Type 0x8809.
- LACP and Mode On (no LACP) are the only modes supported on Firepower appliances (Mode On was added on FP4100/FP9300 in 2.4.x FXOS release).
- LACP can be configured in one of the 2 modes (Active or Passive). FXOS always uses an Active mode.
- The main goal of LACP is to protect from Port-Channel misconfigurations.
- In order for an LACP PC to come UP, there is a need to have the same Speed/Duplex settings in Port-Channel interface members. On FXOS you set the speed at the Port-Channel level.
- LACP Actor = the local device
- LACP Partner = the remote device
- Each device has an LACP System ID which usually is the chassis' MAC. The LACP System ID is sent within each LACP packet.
- Each LACP packet has ~110 Bytes of size.
- LACP can work in Fast Rate or Slow (Normal) Rate. For FXOS the default is Fast Rate (except 1xxx/21xx where it is always Slow), but it can also be configured as Slow. The LACP mode on the switch side depends on the switch model and SW used. For example, a Cat3750 supports both Slow and Fast as from 15.2(4)E. Check the switch confirmation guide for more details.
- In the LACP detection period, LACPs are sent every 1 sec no matter what is the LACP rate. The LACP rate affects only the LACP Keepalive interval once the interface is UP.

Benefits of LACP Keepalive

The LACP keepalive is helpful in scenarios when the remote interface is not functional anymore, but still UP (no direct failure was detected). This could be the case of driver/L2 problem or if there is some device in the path (for example, IPS) which does not allow the detection of remote link failures. LACP Keepalive has a timeout of peer rate x 3. For example, if the remote peer sends every 1 sec then the local device declares the remote peer down if no LACP packet is received within 3 sec. In the case of Slow Rate, this is after 90 sec.

All the fields of an LACP packet as they are shown in Wireshark:


lacp
No. Time Source Destination Protocol Length Source Port Info
156 2017-10-12 10:13:01.348473 Cisco_ec:59:8f Slow-Protocols LACP 124 Link Aggregation Control Protocol Version 1. Actor Port = 272 Partner Port = 2116
173 2017-10-12 10:13:02.271220 Cisco_ec:59:8f Slow-Protocols LACP 124 Link Aggregation Control Protocol Version 1. Actor Port = 272 Partner Port = 2116
228 2017-10-12 10:13:29.809400 Cisco_ec:59:8f Slow-Protocols LACP 124 Link Aggregation Control Protocol Version 1. Actor Port = 272 Partner Port = 0
231 2017-10-12 10:13:56.995154 Cisco_ec:59:8f Slow-Protocols LACP 124 Link Aggregation Control Protocol Version 1. Actor Port = 272 Partner Port = 0
235 2017-10-12 10:14:01.164310 Cisco_ec:59:8f Slow-Protocols LACP 124 Link Aggregation Control Protocol Version 1. Actor Port = 272 Partner Port = 0
236 2017-10-12 10:14:01.222731 Cisco_ec:59:8f Slow-Protocols LACP 124 Link Aggregation Control Protocol Version 1. Actor Port = 272 Partner Port = 0
492 2017-10-12 10:14:25.070491 Cisco_ec:59:8f Slow-Protocols LACP 124 Link Aggregation Control Protocol Version 1. Actor Port = 272 Partner Port = 0
881 2017-10-12 10:14:54.328081 Cisco_ec:59:8f Slow-Protocols LACP 124 Link Aggregation Control Protocol Version 1. Actor Port = 272 Partner Port = 0
Frame 156: 124 bytes on wire (992 bits), 124 bytes captured (992 bits) on interface 0
Ethernet II, Src: Cisco_ec:59:8f (28:6f:7f:ec:59:8f), Dst: Slow-Protocols (01:80:c2:00:00:02)
Slow Protocols
Link Aggregation Control Protocol
LACP Version Number: 0x01
Actor Information: 0x01
Actor Information Length: 0x14
Actor System Priority: 32768
Actor System: Cisco_ec:59:80 (28:6f:7f:ec:59:80)
Actor Key: 16
Actor Port Priority: 32768
Actor Port: 272
Actor State: 0x85, LACP Activity, Aggregation, Expired
....1 = LACP Activity: Active
.... ..0. = LACP Timeout: Long Timeout
.... .1.. = Aggregation: Aggregatable
.... 0... = Synchronization: Out of Sync
...0 .... = Collecting: Disabled
..0. .... = Distributing: Disabled
.0.. .... = Defaulted: No
1... .... = Expired: Yes
[Actor State Flags: E****G*A]
Reserved: 000000
Partner Information: 0x02
Partner Information Length: 0x14
Partner System Priority: 32768
Partner System: a3:00:88:c3:9e:ec (a3:00:88:c3:9e:ec)
Partner Key: 9
Partner Port Priority: 32768
Partner Port: 2116
Partner State: 0x36, LACP Timeout, Aggregation, Collecting, Distributing
....0 = LACP Activity: Passive
.... ..1. = LACP Timeout: Short Timeout
.... .1.. = Aggregation: Aggregatable
.... 0... = Synchronization: Out of Sync
...1 .... = Collecting: Enabled
..1. .... = Distributing: Enabled
.0.. .... = Defaulted: No
0... .... = Expired: No
[Partner State Flags: **DC*GS*]
Reserved: 000000
Collector Information: 0x03
Collector Information Length: 0x10
Collector Max Delay: 32768
Reserved: 00000000000000000000000000
Terminator Information: 0x00
Terminator Length: 0x00
Reserved: 000000000000000000000000000000000000000000000000000000...



Note: When a port-channel is terminated on the FTD, the FXOS capture does not show LACP packets (ingress or egress).

LACP Fast Rate vs Slow Rate

In general, the recommendation is to use Fast Rate on both sides (FXOS on 4100/9300 uses Fast Rate by default, on FPR2100 the default LACP Send Rate is Slow). The LACP rate fast can increase the Port-Channel bundling speed.

	FXOS Configured Slow	FXOS Configured Fast
Switch Configured Slow	Switch requests Slow FXOS Requests Slow Switch sends 1 LACP/30sec	Switch requests Slow FXOS Requests Fast Switch sends 1 LACP/sec

	FXOS sends 1 LACP/30sec	FXOS sends 1 LACP/30sec
Switch Configured Fast	Switch requests Fast FXOS Requests Slow Switch sends 1 LACP/30sec FXOS sends 1 LACP/sec	Switch requests Fast FXOS Requests Fast Switch sends 1 LACP/sec FXOS sends 1 LACP/sec

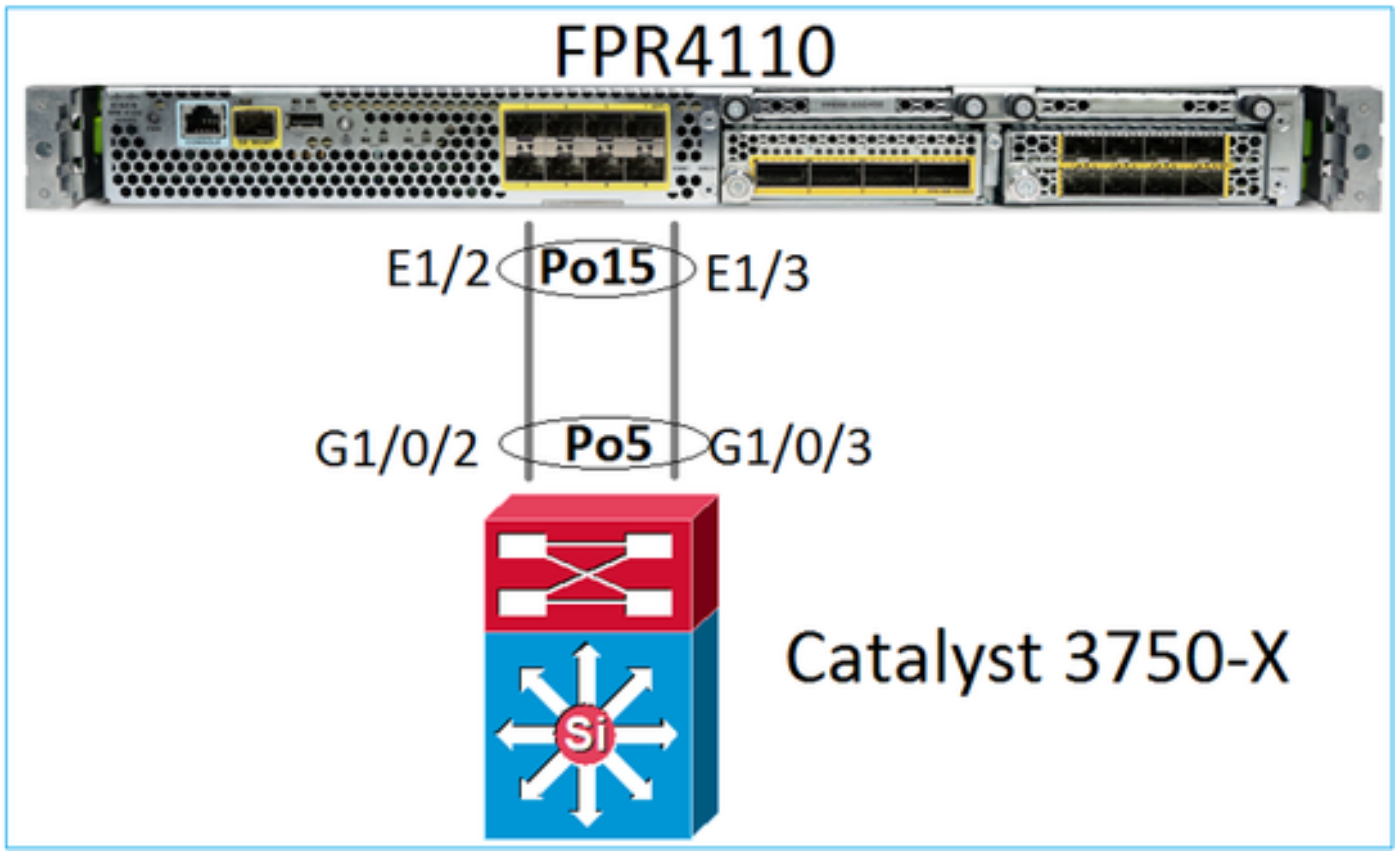
To configure the LACP mode on FXOS (41xx/93xx):

<#root>

```
KSEC-FPR4100-1#
scope org
KSEC-FPR4100-1 /org #
show lacppolicy

LACP policy:
    Name       LACP rate
    ---------- ---------
    default    Fast
KSEC-FPR4100-1 /org # scope lacppolicy default
KSEC-FPR4100-1 /org/lacppolicy # set lacp-rate
  fast    lacp rate fast
  normal  lacp rate normal
```

Troubleshoot Port-Channel on FPR4100/FPR9300

Network Diagram



The FPR4100 and FPR9300 chassis contain an internal switch where the Port-Channel is terminated. Since the internal switch is similar to a Nexus 5K and FXOS supports only LACP the troubleshoot approach is similar to a Nexus 5K.

Check 1 – Verify the Port-Channel status.

<#root>

```
FP4110-7-A(fxos)#
```

show port-channel summary

```
Flags:  D - Down        P - Up in port-channel (members)
        I - Individual  H - Hot-standby (LACP only)
        s - Suspended   r - Module-removed
        S - Switched    R - Routed
        U - Up (port-channel)
        M - Not in use. Min-links not met
--------------------------------------------------------------------------------
Group Port-       Type     Protocol  Member Ports
      Channel
--------------------------------------------------------------------------------
15    Po15(SU)    Eth      LACP      Eth1/2(P)    Eth1/3(P)
```

Verify the FXOS interface status:

<#root>

```
FP4110-7-A(fxos)#
```

show interface brief

```
--------------------------------------------------------------------------------
Ethernet      VLAN   Type Mode   Status  Reason                   Speed     Port
Interface                                                                   Ch #
--------------------------------------------------------------------------------
Eth1/1        1       eth  1qtunl up      none                      1000(D) --
Eth1/2        1       eth  1qtunl up      none                      1000(D) 15
Eth1/3        1       eth  1qtunl up      none                      1000(D) 15
Eth1/4        1       eth  1qtunl down    SFP not inserted           10G(D) --
Eth1/5        1       eth  1qtunl down    Administratively down     1000(D) --
Eth1/6        1       eth  1qtunl down    Administratively down     1000(D) --
Eth1/7        1       eth  1qtunl down    Administratively down      10G(D) --
Eth1/8        1       eth  1qtunl down    SFP not inserted           10G(D) --
Eth1/9        1       eth  vntag  up      none                       40G(D) --
Eth1/10       1       eth  access down    Administratively down      40G(D) --
Eth1/11       1       eth  access down    Administratively down     1000(D) --
Eth1/12       1       eth  access down    Administratively down     1000(D) --
```

Check 2 – Verify that the FXOS sends and receives LACPs (run the command a few times).

<#root>

FP4110-7-A(fxos)#

show lacp counters interface port-channel 15

```
                    LACPDUs         Marker      Marker Response    LACPDUs
Port              Sent   Recv     Sent   Recv     Sent   Recv      Pkts Err
--------------------------------------------------------------------------
port-channel15
Ethernet1/2        223019 207280   0      0        0      0        0
Ethernet1/3        296532 207744   0      0        0      0        0
```

Verify the same on the switch:

<#root>

Switch#

show lacp 5 counters

```
             LACPDUs         Marker      Marker Response    LACPDUs
Port       Sent   Recv     Sent   Recv     Sent   Recv      Pkts Err
--------------------------------------------------------------------
Channel group: 5
Gi1/0/2     627    596      0      0        0      0         0
Gi1/0/3     623    593      0      0        0      0         0
```

Verify the LACP details of an individual FXOS interface:

<#root>

```
FP4110-7-A(fxos)#
```

```
show lacp interface ethernet 1/2
```

```
Interface Ethernet1/2 is up
  Channel group is 15 port channel is Po15
  PDUs sent: 222828
  PDUs rcvd: 207074
  Markers sent: 0
  Markers rcvd: 0
  Marker response sent: 0
  Marker response rcvd: 0
  Unknown packets rcvd: 0
  Illegal packets rcvd: 0
Lag Id: [ [(8000, 28-6f-7f-ec-59-80, 5, 8000, 103), (8000, 2c-33-11-8e-7-b3, e,
8000, 42)] ]
Operational as aggregated link since Tue Oct 31 19:14:57 2017

Local Port: Eth1/2   MAC Address= 2c-33-11-8e-7-b3
  System Identifier=0x8000,2c-33-11-8e-7-b3
  Port Identifier=0x8000,0x42
  Operational key=14
  LACP_Activity=active
  LACP_Timeout=Short Timeout (1s)
  Synchronization=IN_SYNC
  Collected=true
  Distributing=true
```

Check 3 - Verify the LACP IDs of the local and remote device.

<#root>

```
FP4110-7-A(fxos)#
```

```
show lacp port-channel interface port-channel 15
```

```
port-channel15
  System Mac=2c-33-11-8e-7-b3
  Local System Identifier=0x8000,2c-33-11-8e-7-b3
  Admin key=0xe
  Operational key=0xe
  Partner System Identifier=0x8000,28-6f-7f-ec-59-80
  Operational key=0x5
  Max delay=0
  Aggregate or individual=1
  Member Port List=
```

Check 4 (optional) - Collect this output (can be used by Cisco TAC).

<#root>

```
FP4110-7-A(fxos)#
```

```
show lacp internal event-history errors
```

```
1) Event:E_DEBUG, length:74, at 574387 usecs after Tue Oct 31 19:14:57 2017
    [102] lacp_proto_set_ntt(1780): Restarting periodic tx timer in 0x210 msecs
```

```
2) Event:E_DEBUG, length:467, at 544757 usecs after Tue Oct 31 19:14:57 2017
    [102] lacp_ac_init_port_channel_member(1660): TYPE1 UPDATE lacp_ac_init_port
_channel_member port-channel port-channel15(0x1600000e) lacp_mcec_type1_upd_sent
...
```

Check 5 - Check the LACP FSM transition for the specific port that has the problem. The messages are shown with the oldest at the top of the output.

<#root>

```
FP4110-7-A(fxos)#
```

show lacp internal event-history interface ethernet 1/2

```
>>>>FSM: <Ethernet1/2> has 975 logged transitions<<<<<

1) FSM:<Ethernet1/2> Transition at 257150 usecs after Sun Oct 29 12:35:16 2017
    Previous state: [LACP_ST_WAIT_FOR_HW_TO_PROGRAM_RECEIVE_PATH]
    Triggered event: [LACP_EV_PORT_RECEIVE_PATH_ENABLED_AS_CHANNEL_MEMBER_MESSAGE]
    Next state: [LACP_ST_PORT_MEMBER_RECEIVE_ENABLED]

...

4) FSM:<Ethernet1/2> Transition at 966987 usecs after Sun Oct 29 12:35:19 2017
    Previous state: [LACP_ST_PORT_MEMBER_COLLECTING_AND_DISTRIBUTING_ENABLED]
    Triggered event: [LACP_EV_PARTNER_PDU_IN_SYNC]        <--- Good (Received LACP with ‘Synchronizatio
    Next state: [LACP_ST_PORT_IS_DOWN_OR_LACP_IS_DISABLED]

...
207) FSM:<Ethernet1/4> Transition at 482767 usecs after Sun Oct 29 13:18:40 2017
    Previous state: [LACP_ST_ATTACHED_TO_AGGREGATOR]
    Triggered event: [LACP_EV_PARTNER_PDU_OUT_OF_SYNC]
    Next state: [FSM_ST_NO_CHANGE]

208) FSM:<Ethernet1/4> Transition at 363720 usecs after Sun Oct 29 13:18:41 2017
    Previous state: [LACP_ST_ATTACHED_TO_AGGREGATOR]
    Triggered event: [LACP_EV_PARTNER_PDU_OUT_OF_SYNC]        <--- Bad (Received LACP with ‘Synchroniza
    Next state: [FSM_ST_NO_CHANGE]
```

Check 6 - Collect the Port-Channel event history (can be used by Cisco TAC).

<#root>

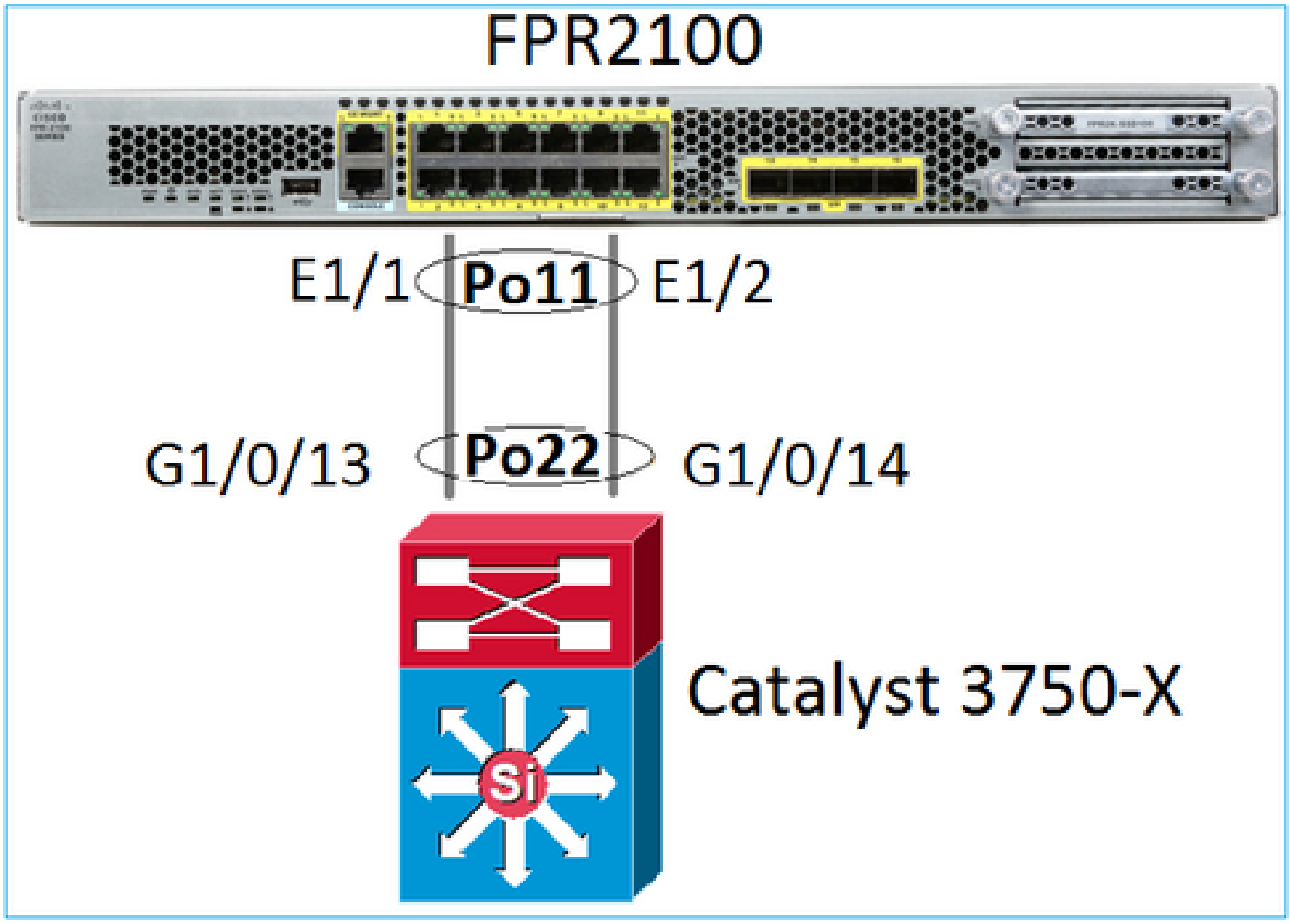
```
FP4110-7-A(fxos)#
```

show port-channel internal event-history all

```
Low Priority Pending  queue: len(0), max len(1) [Tue Oct 31 19:37:03 2017] High Priority Pending queue: l
```

Troubleshoot Port-Channel on FPR21xx/FPR1xxx

Network Diagram



Check 1. In case LACP is used, verify the LACP counters.

You see both sides (switch and FXOS) send and receive:

<#root>

```
FP2110-2(local-mgmt)#
```

`show lacp counters`

```
              LACPDUs         Marker      Marker Response    LACPDUs
Port       Sent   Recv     Sent   Recv     Sent    Recv      Pkts Err
--------------------------------------------------------------------
Channel group: 11
Eth1/1     4435   3532     0      0        0       0         0
Eth1/2     4566   3532     0      0        0       0         0
```

Another way to verify the same:

<#root>

```
FP2110-2(local-mgmt)#
```

show pktmgr counters

```
Ports           Tx        Tx        Tx        Rx      Rx        Rx        Rx
           Packets     Drops     Bytes   Packets   Drops     Bytes  Forwards
-------------------------------------------------------------------------------
Eth1/1       4575         0    567300      3537       0    452736      3537 < LACP PDUs forwarded inter
Eth1/2       4706         0    583544      3537       0    452736      3537 < LACP PDUs forwarded inter
Eth1/3          0         0         0         0       0         0         0
Eth1/4          0         0         0         0       0         0         0
Eth1/5          0         0         0         0       0         0         0
Eth1/6          0         0         0         0       0         0         0
Eth1/7          0         0         0         0       0         0         0
Eth1/8          0         0         0         0       0         0         0
Eth1/9          0         0         0         0       0         0         0
Eth1/10         0         0         0         0       0         0         0
Eth1/11         0         0         0         0       0         0         0
Eth1/12         0         0         0         0       0         0         0
Eth1/13         0         0         0         0       0         0         0
Eth1/14         0         0         0         0       0         0         0
Eth1/15         0         0         0         0       0         0         0
Eth1/16         0         0         0         0       0         0         0
Misc.           0         0         0         0       0         0       n/a
```

Check 2. Verify the upstream switch status.

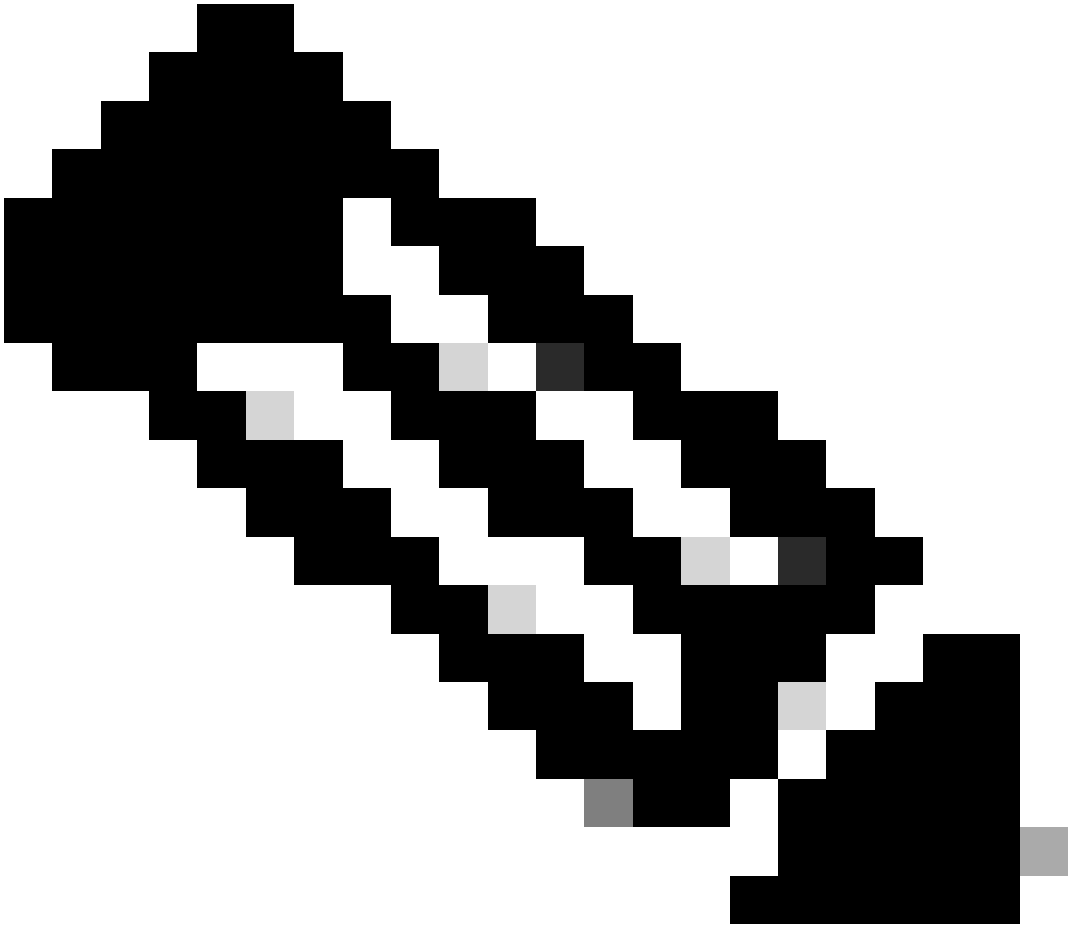
<#root>

```
FP2110-2(local-mgmt)#
```

show lacp neighbor

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

Channel group: 11

Partner (internal) information:

          Partner                  Partner                       Partner
Port      System ID              Port Number     Age         Flags
Eth1/1    32768,286f.7fec.5980  0x10e           9  s        FA


          LACP Partner           Partner           Partner
          Port Priority        Oper Key        Port State
          32768                0x16            0x3f

          Port State Flags Decode:
          Activity:   Timeout:   Aggregation:   Synchronization:
          Active      Long       Yes            Yes

          Collected:   Distributing:   Defaulted:   Expired:
          Yes           Yes             No           No

          Partner                  Partner                       Partner
Port      System ID              Port Number     Age         Flags
Eth1/2    32768,286f.7fec.5980  0x10f           24 s        FA
```

```
LACP Partner           Partner           Partner
Port Priority        Oper Key        Port State
32768                0x16            0x3f

Port State Flags Decode:
Activity:   Timeout:   Aggregation:   Synchronization:
Active      Long       Yes             Yes

Collected:   Distributed:   Defaulted:   Expired:
Yes           Yes             No           No
```



Note: If Collected and Distributed are not Yes and Defaulted is No then LACP is not converged.

Check 3. Verify that the local LACP system-ID is not 0.

<#root>

```
FP2110-2(local-mgmt)#
```

```
show lacp sys-id

32768, 70df.2f18.d813
```

Additional Troubleshoot (Common in all Platforms)

Check 1

Ensure that both sides (Firewall and switch) have matched settings (for example, Speed is the same, Port-Channel mode is the same).

Check 2

Check for FXOS faults. You can do this check from the chassis User Interface (UI) or from the CLI that uses this command:

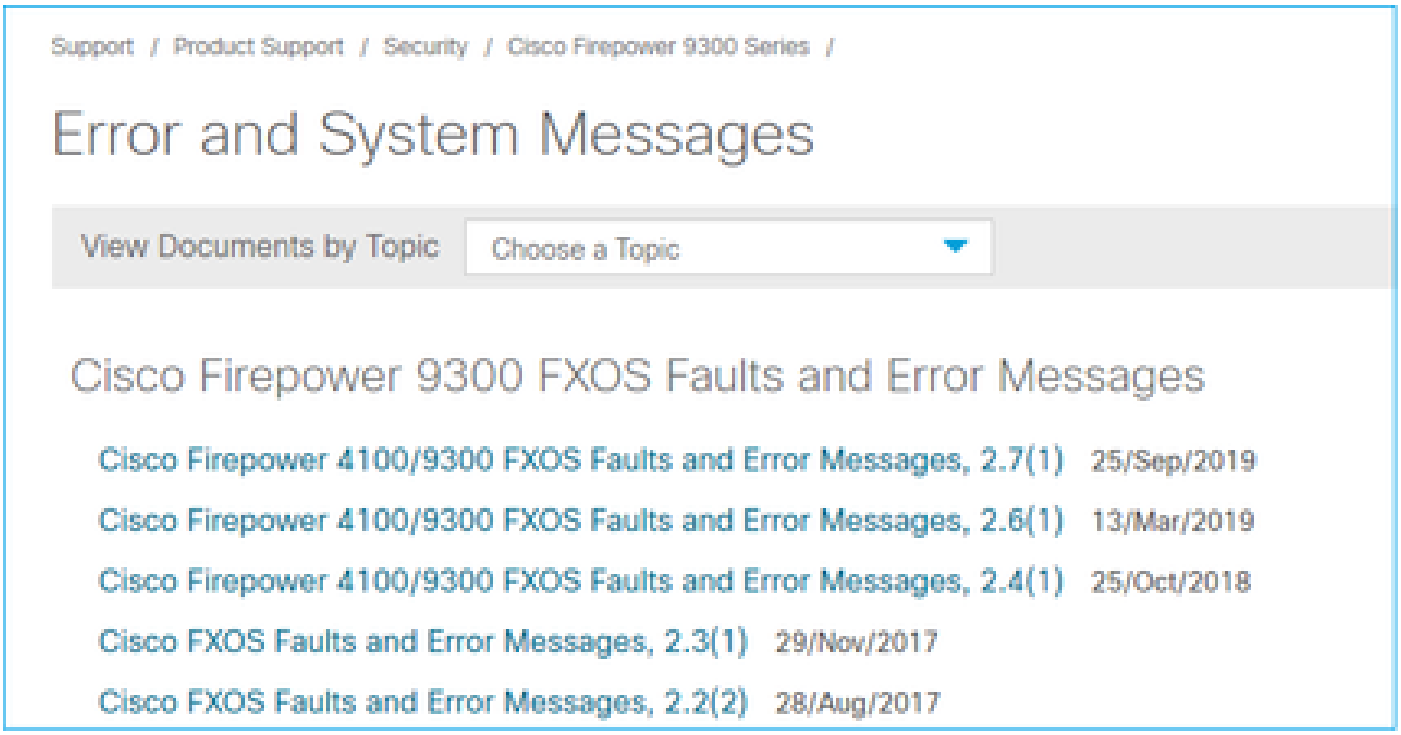
<#root>

```
FPR4100#

show fault

Severity  Code     Last Transition Time     ID       Description
--------- -------- ----------------------- -------- -----------
Major     F0479    2020-03-19T11:50:44.322    543322 Virtual interface 781 link state is down
Major     F0373    2020-03-19T10:55:13.778     34178 Fan 1 in Fan Module 1-5 under chassis 1 operabilit
Minor     F0480    2020-03-19T10:55:13.777     34177 Fan module 1-5 in chassis 1 operability: degraded
Major     F1767    2020-03-19T10:54:04.162    531228 The password encryption key has not been set.
Major     F0727    2020-03-19T09:50:02.891    522921 lan Member 1/5 of Port-Channel 10 on fabric interc
Major     F0282    2020-03-19T09:49:31.462    522922 lan port-channel 10 on fabric interconnect A oper
Major     F0277    2020-03-19T09:49:31.437    522929 ether port 1/5 on fabric interconnect A oper state
Info      F0279    2020-01-17T11:06:45.472    300958 ether port 1/7 on fabric interconnect A oper state
Info      F0279    2020-01-17T11:06:37.941    300903 ether port 1/6 on fabric interconnect A oper state
Minor     F1437    2020-01-16T10:11:39.675    291723 Config backup may be outdated
```

The faults are shown in chronological order. The Severity reflects the importance of the fault, while the description provides a brief overview. The focus is mainly on the severity, the timestamp, and the description. The fault severity order from most severe to least severe is:

- Critical
- Major
- Minor
- Warning
- Info/Condition
- Cleared

For details about each fault check the FXOS Faults and Error Messages guide: FXOS Error and System Messages



Check 3

If you did some recent changes related to Port-Channel configuration on FMC, ensure that the policy was deployed from FMC to FTD.

Check 4

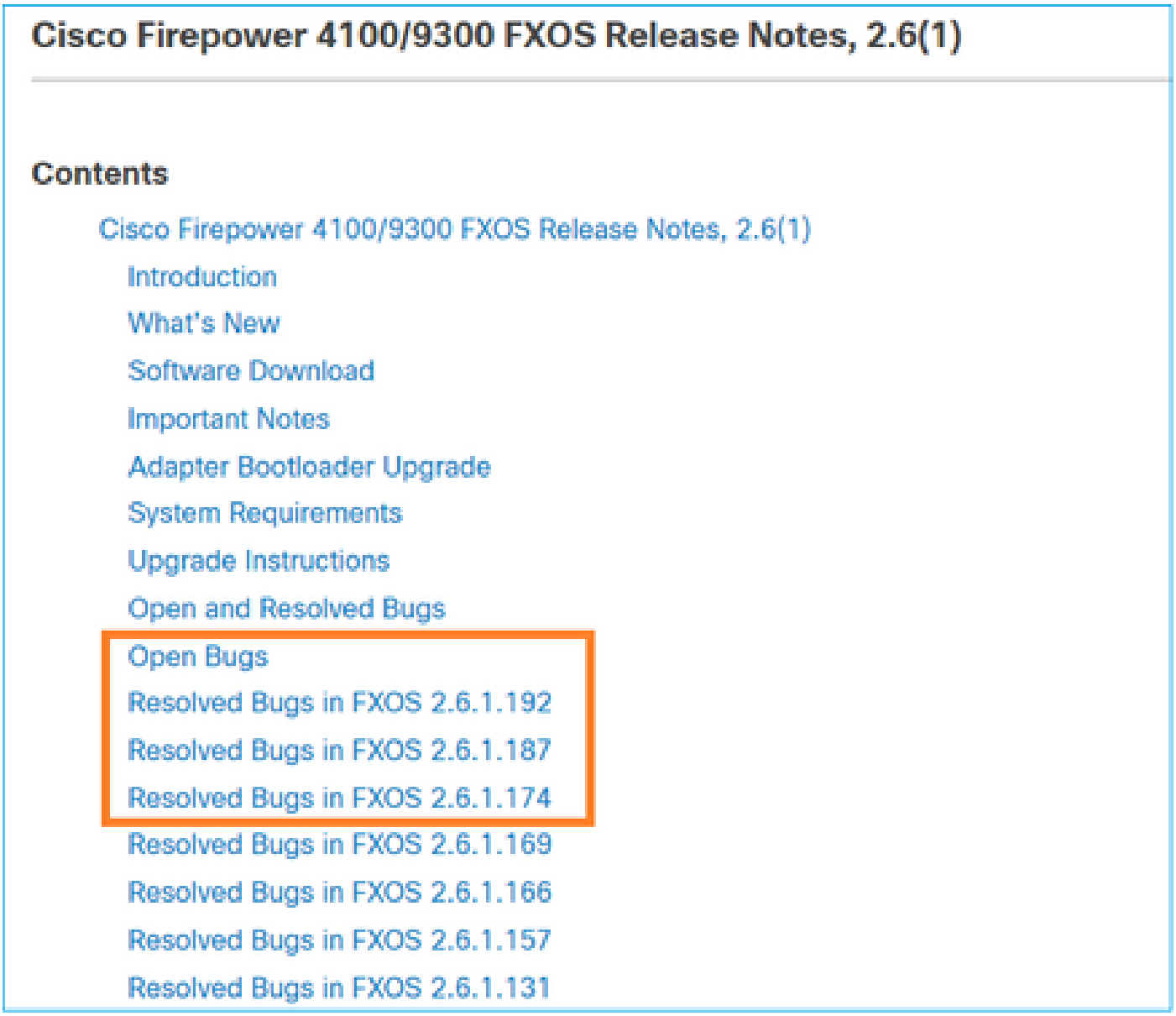
If the Port-Channel is in Failed state, and the device belongs to a Cluster, then ensure that the Cluster is enabled on the device. A device that is kicked off the cluster is normal to have the Port-Channel in a failed state.

Check 5

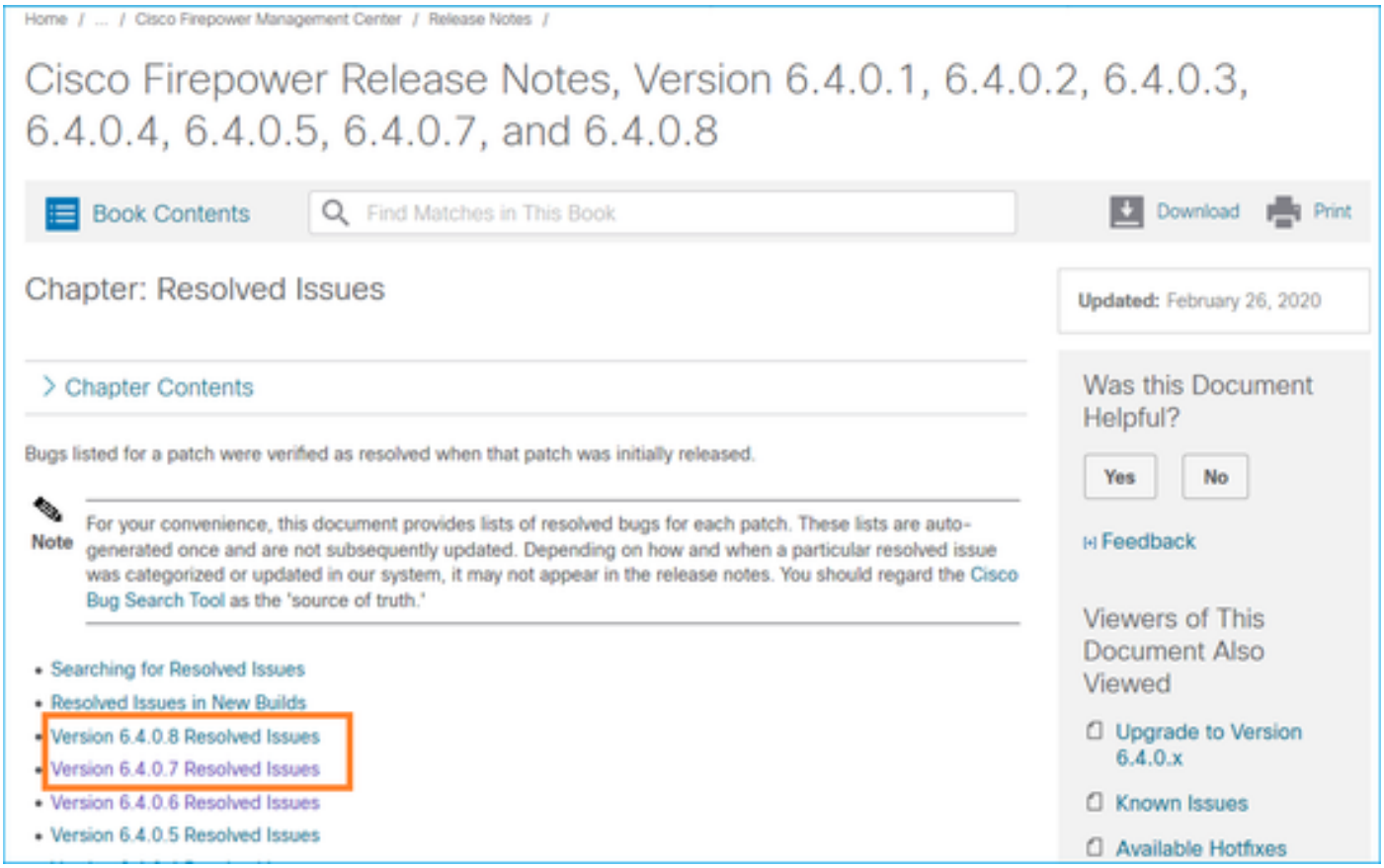
If the configuration is correct, but the interface does not come UP check and replace the cable and/or Small Form-Factor Pluggable (SFP) transceiver.

Check 6

Check the firepower Release Notes for known issues related to Port-Channel. For example, if you run FXOS version 2.6.1.169 and FTD 6.4.0.6 check these sections:



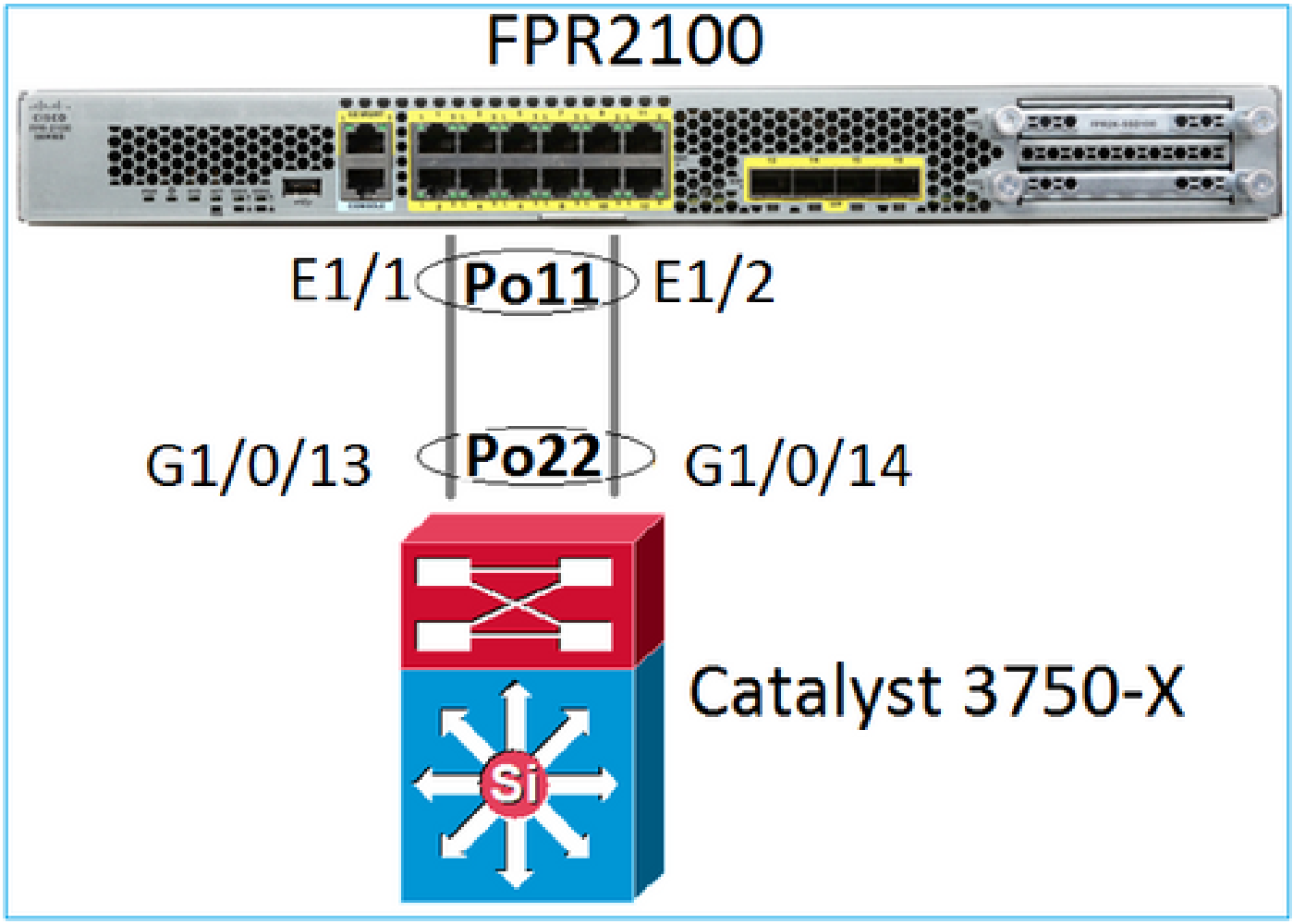
Additionally, check the related FMC/FTD Release Notes. Since in this example the FTD runs 6.4.0.5 there is need to check the 6.4.x Release Notes:



Common Issues

Case 1. EtherChannel Mode Mismatch

Consider this topology:



The Problem Symptoms

On Firepower the Port-Channel is Down and the Negotiation protocol is LACP:

<#root>

```
FP2110-2(local-mgmt)#
```

show portchannel summary

```
Flags:  D - Down        P - Up in port-channel (members)
I - Individual  H - Hot-standby (LACP only)
s - Suspended   r - Module-removed
S - Switched    R - Routed
U - Up (port-channel)
M - Not in use. Min-links not met
--------------------------------------------------------------------------------
Group Port-       Type     Protocol  Member Ports
      Channel
--------------------------------------------------------------------------------
11    Po11(D)     Eth      LACP      Eth1/1(D)    Eth1/2(D)
```

On FXOS the LACP Sent counters increment every 30 sec, but the Receive counters do not:

<#root>

```
FP2110-2(local-mgmt)#
```

show lacp counters

```
              LACPDUs         Marker      Marker Response    LACPDUs
Port       Sent   Recv     Sent   Recv     Sent    Recv      Pkts Err
--------------------------------------------------------------------
Channel group: 11
Eth1/1     11356  3762     0      0        0       0         0
Eth1/2     11393  3761     0      0        0       0         0
FP2110-2(local-mgmt)#
```

show lacp counters

```
              LACPDUs         Marker      Marker Response    LACPDUs
Port       Sent   Recv     Sent   Recv     Sent    Recv      Pkts Err
--------------------------------------------------------------------
Channel group: 11
Eth1/1     11357  3762     0      0        0       0         0
Eth1/2     11394  3761     0      0        0       0         0
```

The Root Cause

The Port-Channel on the switch is UP, but notice the absence of Negotiation protocol:

<#root>

```
Switch#
```

show etherchannel 22 summary

```
…
Number of channel-groups in use: 15
Number of aggregators:           15

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
22     Po22(SU)         -        Gi1/0/13(P) Gi1/0/14(P)
```

The switch port configuration confirms this:

<#root>

```
Switch#
```

show run int g1/0/13

```
interface GigabitEthernet1/0/13
 lacp rate fast
 channel-group 22 mode on
end

Switch#
```

show run int g1/0/14

```
interface GigabitEthernet1/0/14
 lacp rate fast
 channel-group 22 mode on
end
```

Solution

Since this is an FPR21xx appliance, there are 2 possible solutions:

1. Change the Port-Channel mode on the switch side from ON to LACP (Active or Passive).
2. Change the Port-Channel mode on the FTD side from LACP to ON.

In this scenario, the second solution was chosen (set FTD Port-Channel to mode ON):

<#root>

```
FP2110-2(local-mgmt)#
```

show portchannel summary

```
Flags:  D - Down        P - Up in port-channel (members)
I - Individual  H - Hot-standby (LACP only)
s - Suspended   r - Module-removed
S - Switched    R - Routed
U - Up (port-channel)
M - Not in use. Min-links not met
--------------------------------------------------------------------------------
Group Port-       Type     Protocol  Member Ports
      Channel
--------------------------------------------------------------------------------
11    Po11(U)     Eth      ON        Eth1/1(P)    Eth1/2(P)
```

The LACP counters are not shown any more:

<#root>

```
FP2110-2(local-mgmt)#
```

show lacp counters

```
FP2110-2(local-mgmt)#
```

Case 2. Wrong Port-Channel Design

The Problem Symptoms

<#root>

```
FP4110-7-A(fxos)#
```

show port-channel summary

```
Flags:  D - Down        P - Up in port-channel (members)
        I - Individual  H - Hot-standby (LACP only)
        s - Suspended   r - Module-removed
        S - Switched    R - Routed
        U - Up (port-channel)
        M - Not in use. Min-links not met
--------------------------------------------------------------------------------
Group Port-       Type     Protocol  Member Ports
      Channel
--------------------------------------------------------------------------------
15    Po15(SD)    Eth      LACP      Eth1/2(P)    Eth1/3(s)
48    Po48(SD)    Eth      NONE      --
```

FXOS LACP counters increase in both directions:

<#root>

```
FP4110-7-A(fxos)#
```

show lacp counters

```
                    LACPDUs         Marker      Marker Response    LACPDUs
Port              Sent   Recv     Sent   Recv     Sent   Recv      Pkts Err
--------------------------------------------------------------------------
port-channel15
Ethernet1/2        419219 451268   0      0        0      0        0
Ethernet1/3        419215 446806   0      0        0      0        0

FP4110-7-A(fxos)# show lacp counters
                    LACPDUs         Marker      Marker Response    LACPDUs
Port              Sent   Recv     Sent   Recv     Sent   Recv      Pkts Err
--------------------------------------------------------------------------
port-channel15
Ethernet1/2        419219 451269   0      0        0      0        0
Ethernet1/3        419216 446807   0      0        0      0        0
```

The Root Cause

The output of show lacp neighbor shows different Partner System ID on each port:

<#root>

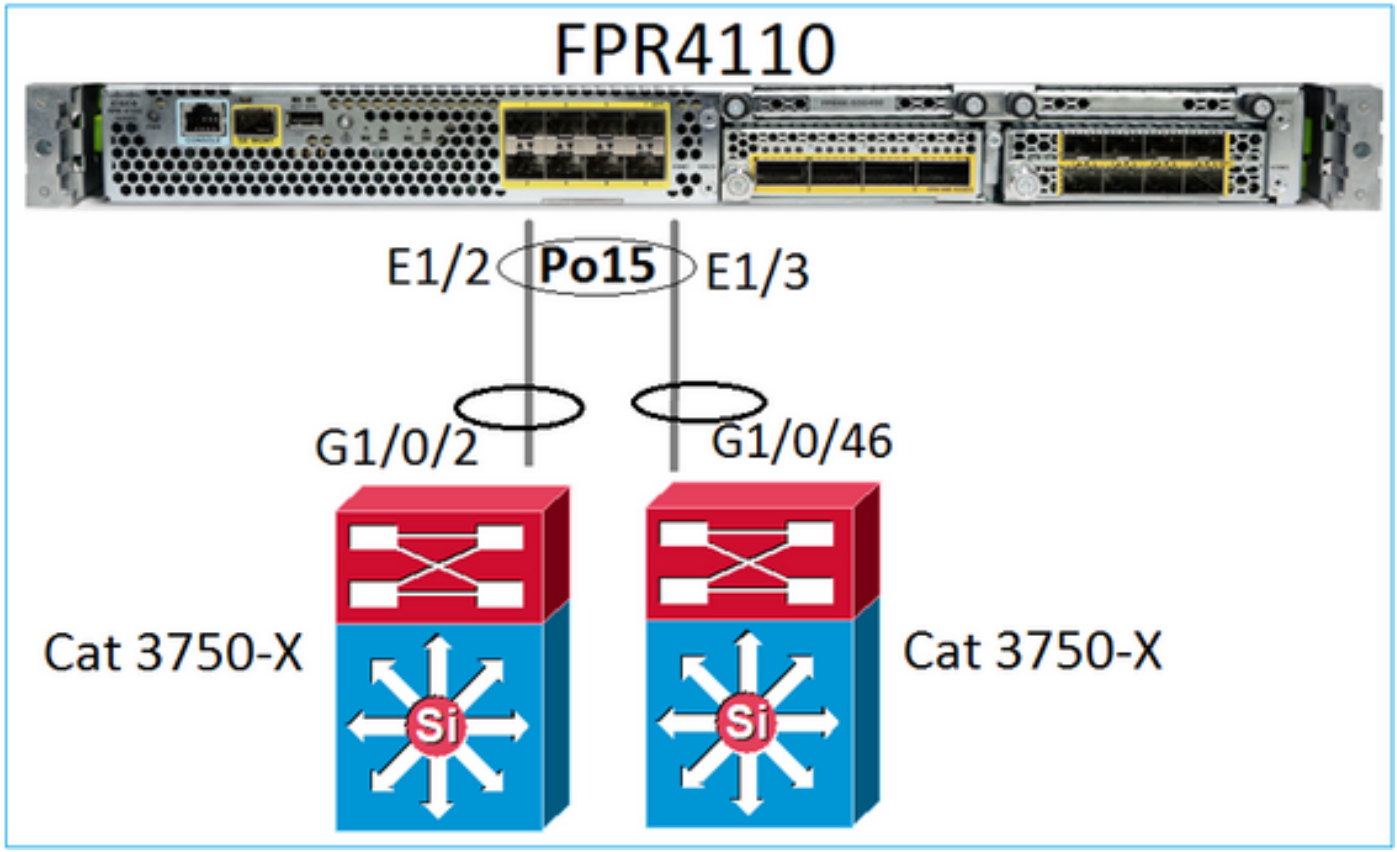
```
FP4110-7-A(fxos)#
```

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-channel15 neighbors
Partner's information
           Partner               Partner                     Partner
Port       System ID             Port Number     Age         Flags
Eth1/2     32768,28-6f-7f-ec-59-800x103          419611      FA

           LACP Partner          Partner                     Partner
           Port Priority         Oper Key                    Port State
           32768                 0x5                         0x3d
```

```
Partner's information
            Partner                 Partner                         Partner
Port        System ID               Port Number     Age             Flags
Eth1/3      32768,4-62-73-d2-65-0    0x12f          419610          SA

            LACP Partner            Partner                         Partner
            Port Priority           Oper Key                        Port State
            32768                   0x16                            0xd
```

This can be visualized as:

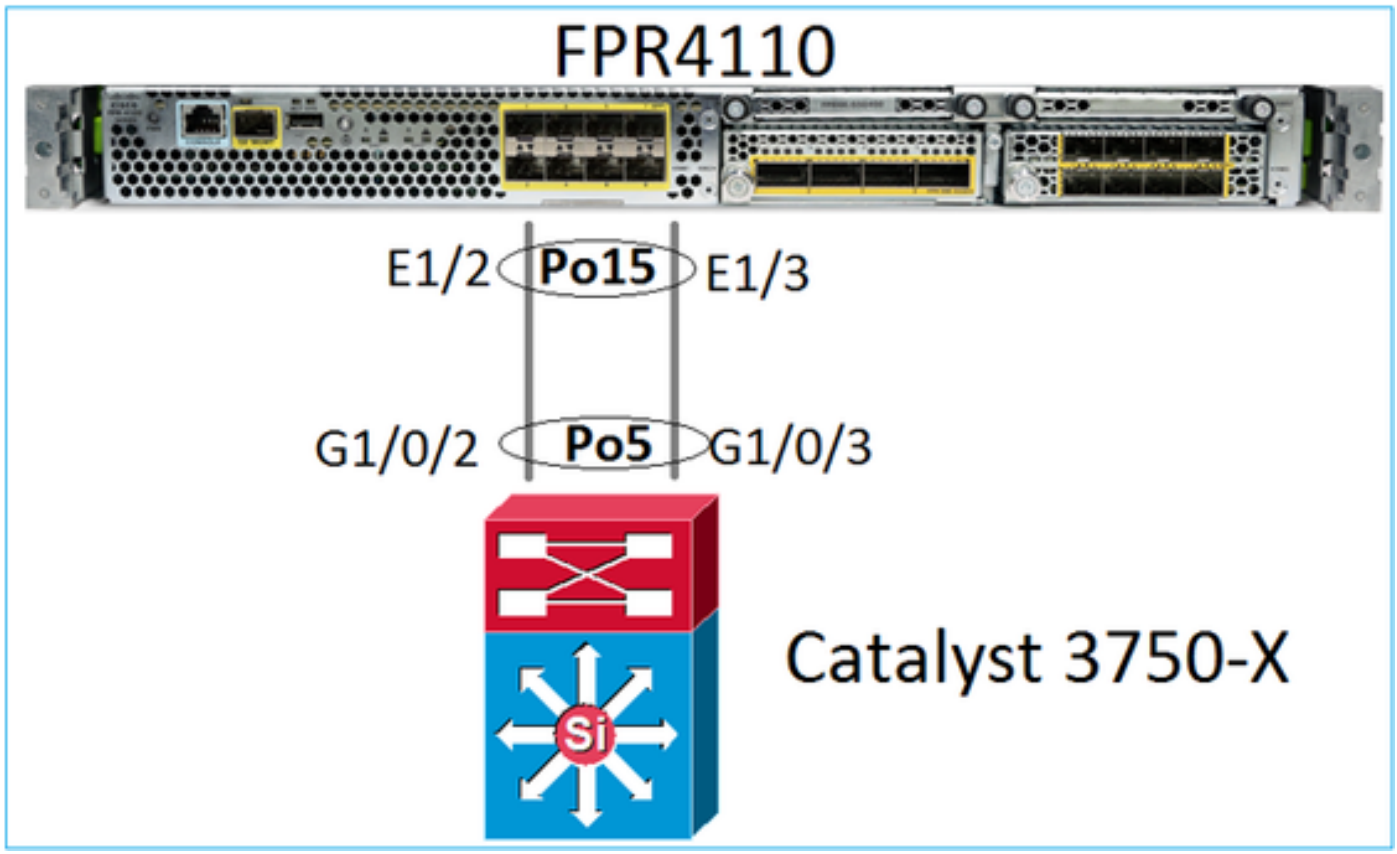


Solution

- In the case of 2960, you need to configure stacking (FlexStack).
- In the case of 3750-X/3850 and so on, you need to configure stacking (StackWise Plus).
- In the case of 4500, 6500, 6800, you need to use Virtual Switching System (VSS).
- In the case of Nexus 5K, 7K or 9K, you need to use Virtual Port-Channel (vPC).
- In a different case, you need to connect the FXOS to the same physical switch.

Case 3. FXOS Port-Channel Unassigned

Network Diagram



The Problem Symptoms

On FXOS side the Port-Channel members are Suspended:

<#root>

```
FP4110-7-A(fxos)#
```

show port-channel summary

```
Flags:  D - Down        P - Up in port-channel (members)
        I - Individual  H - Hot-standby (LACP only)
        s - Suspended   r - Module-removed
        S - Switched    R - Routed
        U - Up (port-channel)
        M - Not in use. Min-links not met
--------------------------------------------------------------------------------
Group Port-       Type     Protocol  Member Ports
      Channel
--------------------------------------------------------------------------------
15    Po15(SD)    Eth      LACP      Eth1/2(s)    Eth1/3(s)
48    Po48(SD)    Eth      NONE      --
```

The same on the switch side:

<#root>

```
Switch#
```

show etherchannel 5 summary

```
…
Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
5      Po5(SD)         LACP      Gi1/0/2(s)  Gi1/0/3(s)
```

FXOS LACP counters shows packets that are sent and received:

<#root>

FP4110-7-A(fxos)#

show lacp counters

```
                    LACPDUs         Marker      Marker Response    LACPDUs
Port              Sent   Recv     Sent   Recv     Sent   Recv      Pkts Err
--------------------------------------------------------------------------
port-channel15
Ethernet1/2        420839 452531   0      0        0      0        0
Ethernet1/3        420793 447409   0      0        0      0        0
```

FP4110-7-A(fxos)#

show lacp counters

```
                    LACPDUs         Marker      Marker Response    LACPDUs
Port              Sent   Recv     Sent   Recv     Sent   Recv      Pkts Err
--------------------------------------------------------------------------
port-channel15
Ethernet1/2        421026 452537   0      0        0      0        0
Ethernet1/3        420981 447416   0      0        0      0        0
```

On the switch side, the LACP counters also show packets that are sent, but not received:

<#root>

Switch#

show lacp 5 counters

```
             LACPDUs         Marker      Marker Response    LACPDUs
Port       Sent   Recv     Sent   Recv     Sent   Recv      Pkts Err
--------------------------------------------------------------------
Channel group: 5
Gi1/0/2     452539 420223   0      0        0      0         0
Gi1/0/3     447232 415274   0      0        0      0         0
```

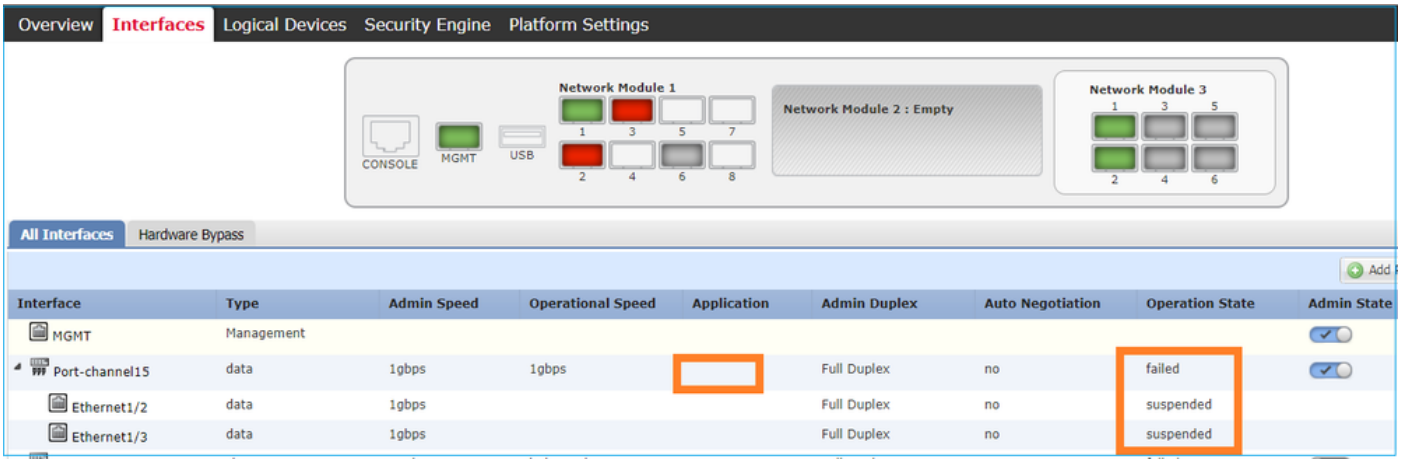
Switch#

show lacp 5 counters

```
             LACPDUs         Marker      Marker Response    LACPDUs
Port       Sent   Recv     Sent   Recv     Sent   Recv      Pkts Err
--------------------------------------------------------------------
Channel group: 5
Gi1/0/2     452540 420223   0      0        0      0         0
Gi1/0/3     447233 415274   0      0        0      0         0
```

The Root Cause

The problem, in this case, is that the FXOS Port-Channel is not assigned to the logical device (FTD application):

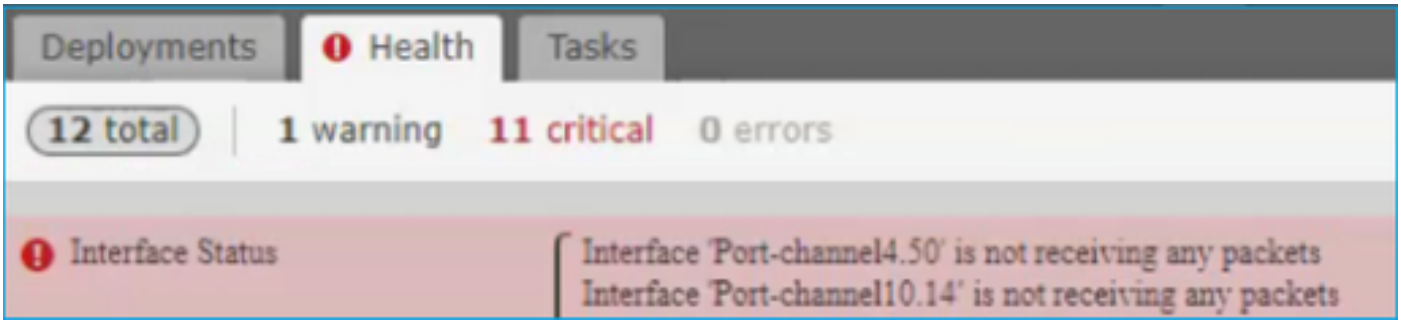


Solution

Assign the Port-Channel to the logical device.

Case 4. Health Alerts About Port-Channel Do Not Receive Any Packets

The device (FTD) sends every 5 minutes info about the interface traffic received on each interface that has a name configured and is UP. If there are no packets received in the last interval messages like this appear on FMC UI:



Recommended Action

From the FTD CLI, check the show traffic output and focus on the 5-minute input rate. For example,

```
Interface Port-channel10.14
INSIDE:
        received (in 237938.740 secs):
                2 packets       84 bytes
                0 pkts/sec      0 bytes/sec
        transmitted (in 237938.740 secs):
                5 packets       140 bytes
                0 pkts/sec      0 bytes/sec
      1 minute input rate 0 pkts/sec,  0 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  0 bytes/sec
```

```
5 minute output rate 0 pkts/sec,  0 bytes/sec
5 minute drop rate, 0 pkts/sec
```

Case 5. Health Alert on FMC: Port-Channel Disassociated or Interface Added

The Health alert states: "Interface with physical-name: "Port-Channel" disassociated." or ‘"Interface with physical-name: \"name_if\" added."

Recommended Action

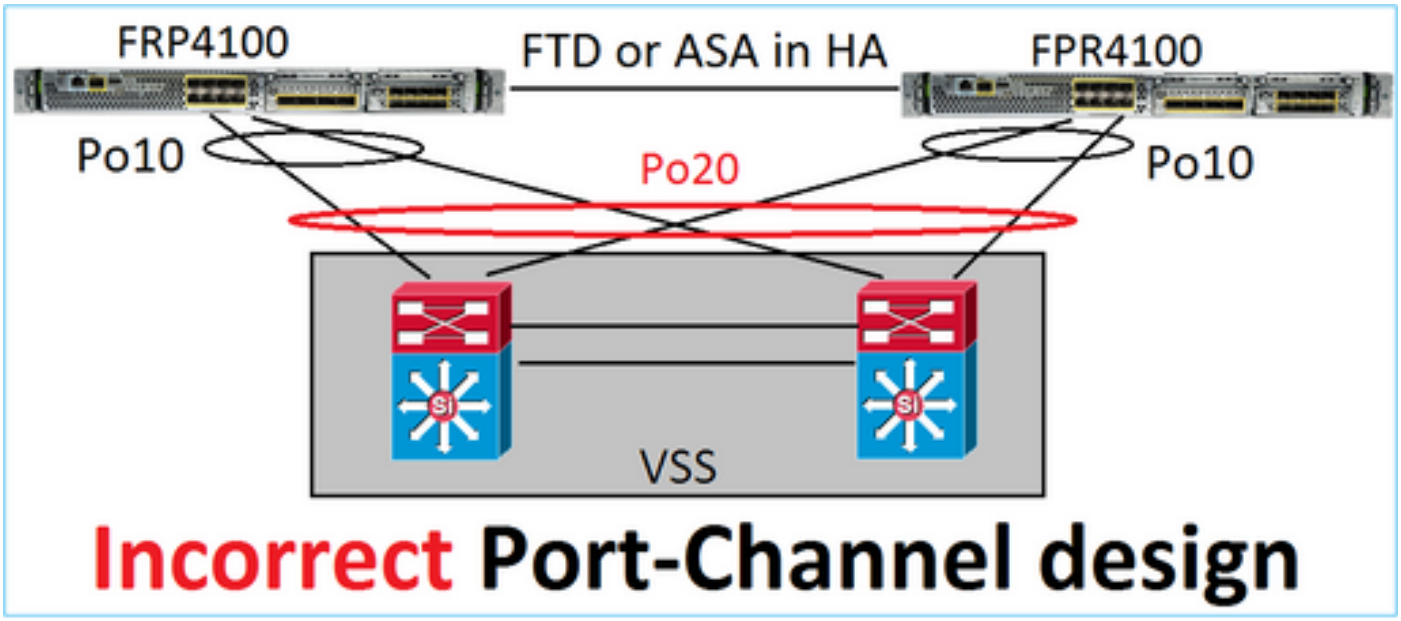
This is a known, cosmetic issue tracked by Cisco bug ID CSCvb15074

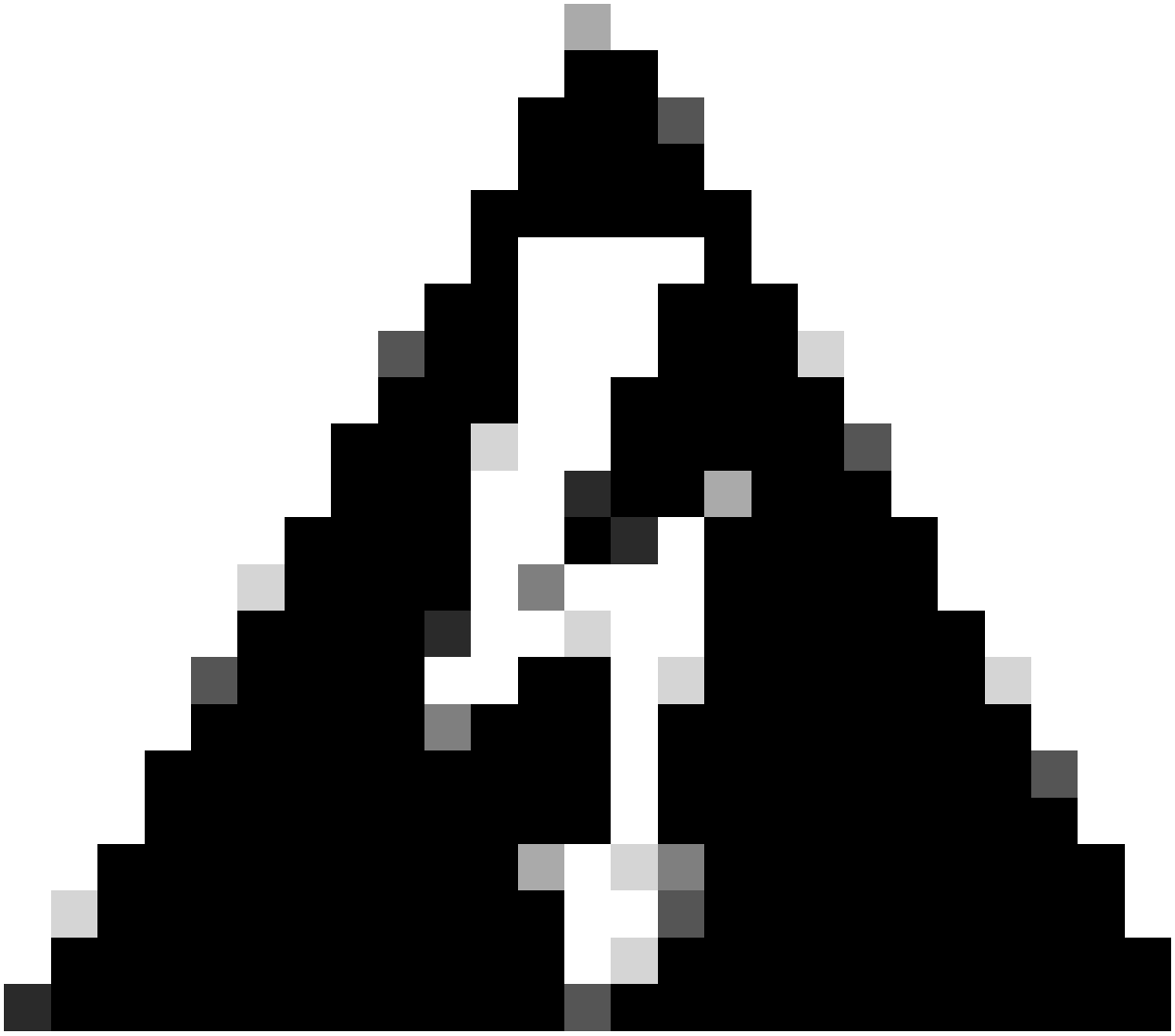
Port-Channel Considerations

Design Considerations

Case 1. FTD/ASA Blade in HA

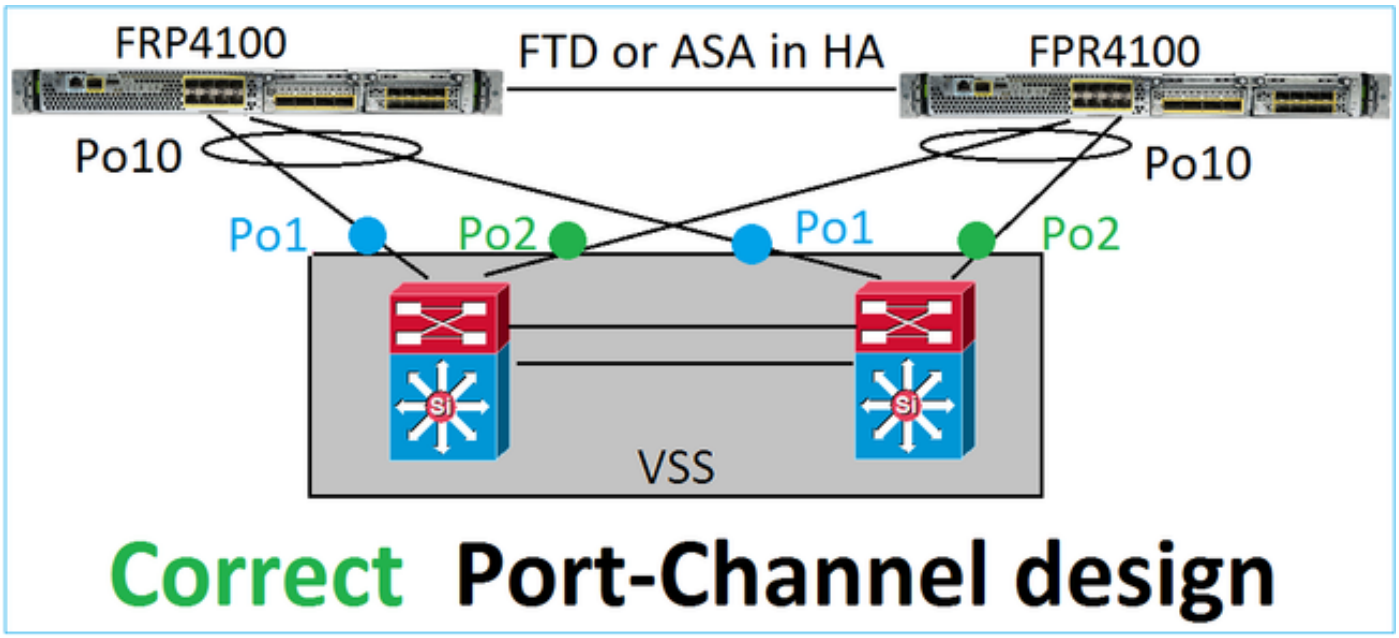
This setup is unsupported. The reason is the Port-Channel configuration on the switch side is incorrect and leads to traffic block on the standby device. Such design is only supported when you configure ASA or FTD in Cluster Spanned mode.





Warning: This scenario is incorrect in failover (high-availability).

This is the proper Port-Channel design for High Availability:



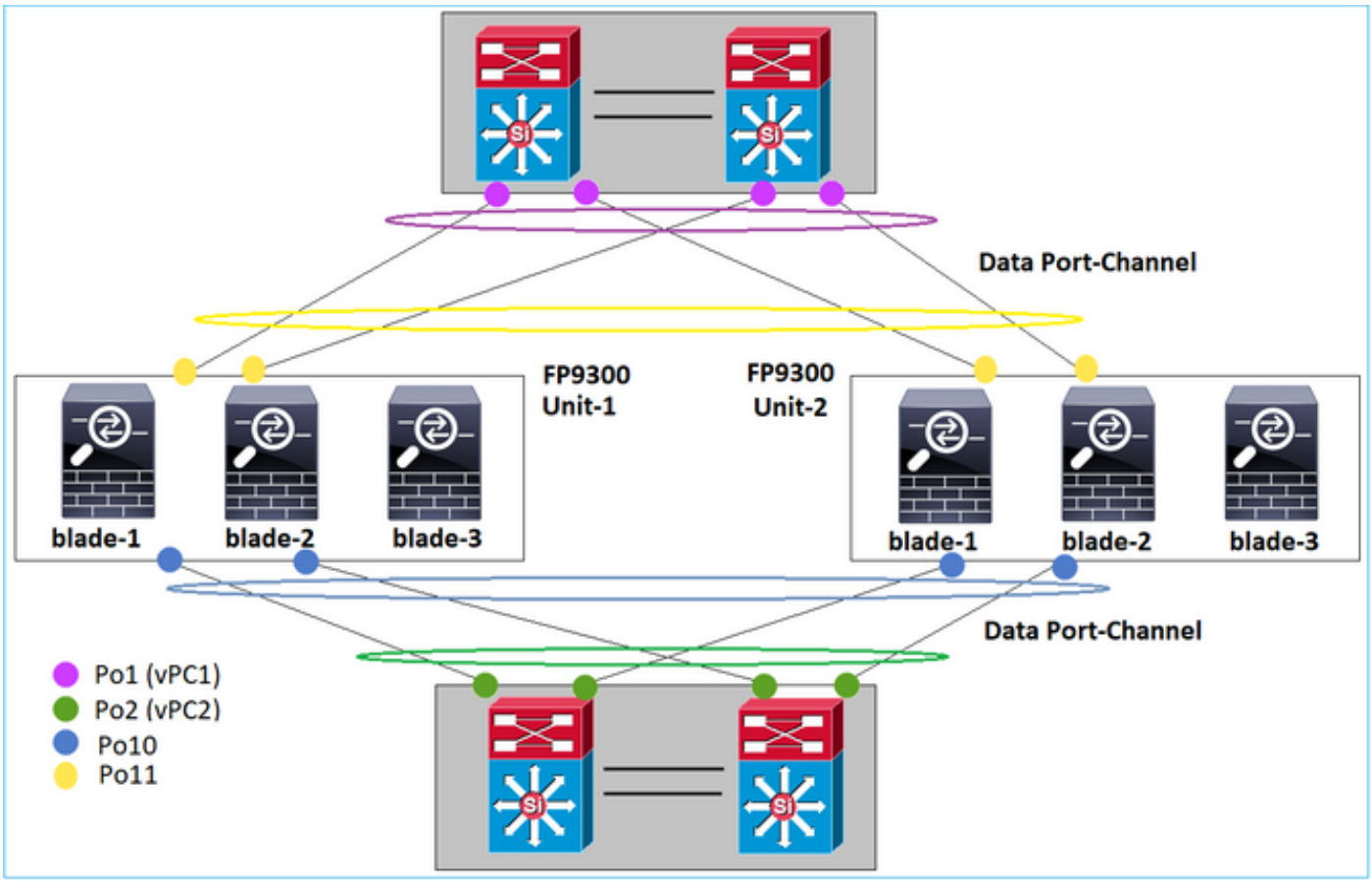
Related Information

- Connecting to an EtherChannel on Another Device
- EtherChannels for Inter-Chassis Clustering

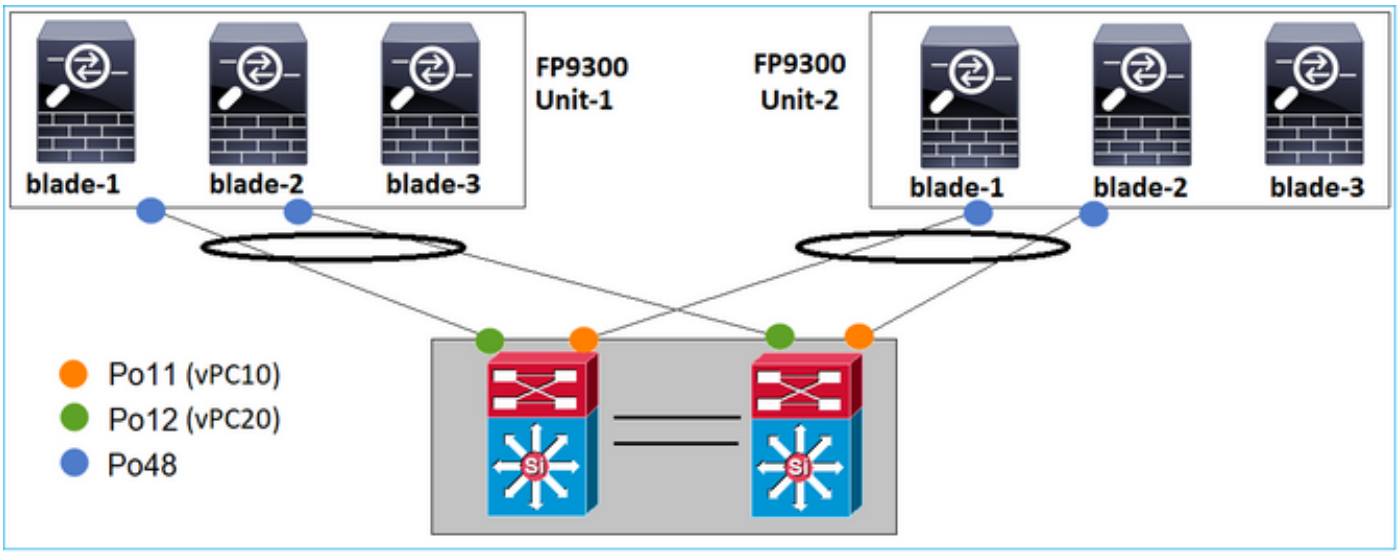
Case 2. FTD/ASA in Cluster

Each firewall data interface Port-Channel uses Spanned mode (this is the only mode supported on Firepower platforms). From a design point of view, on the switch side, the switchports for a single data interface belong to one port-channel.

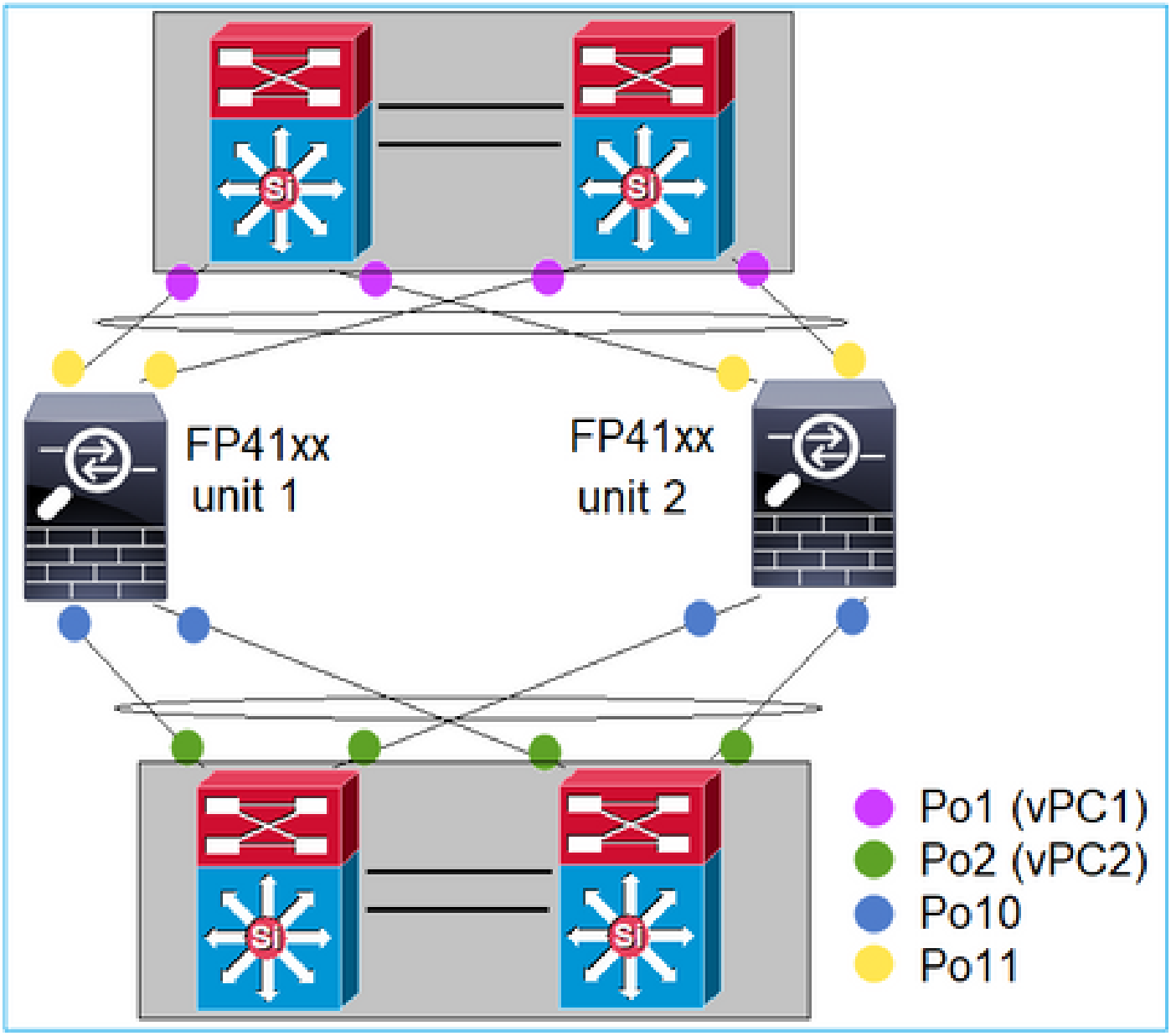
For example, in the case of FP9300 (2 chassis, 6 blades) the data ports can be configured like this:



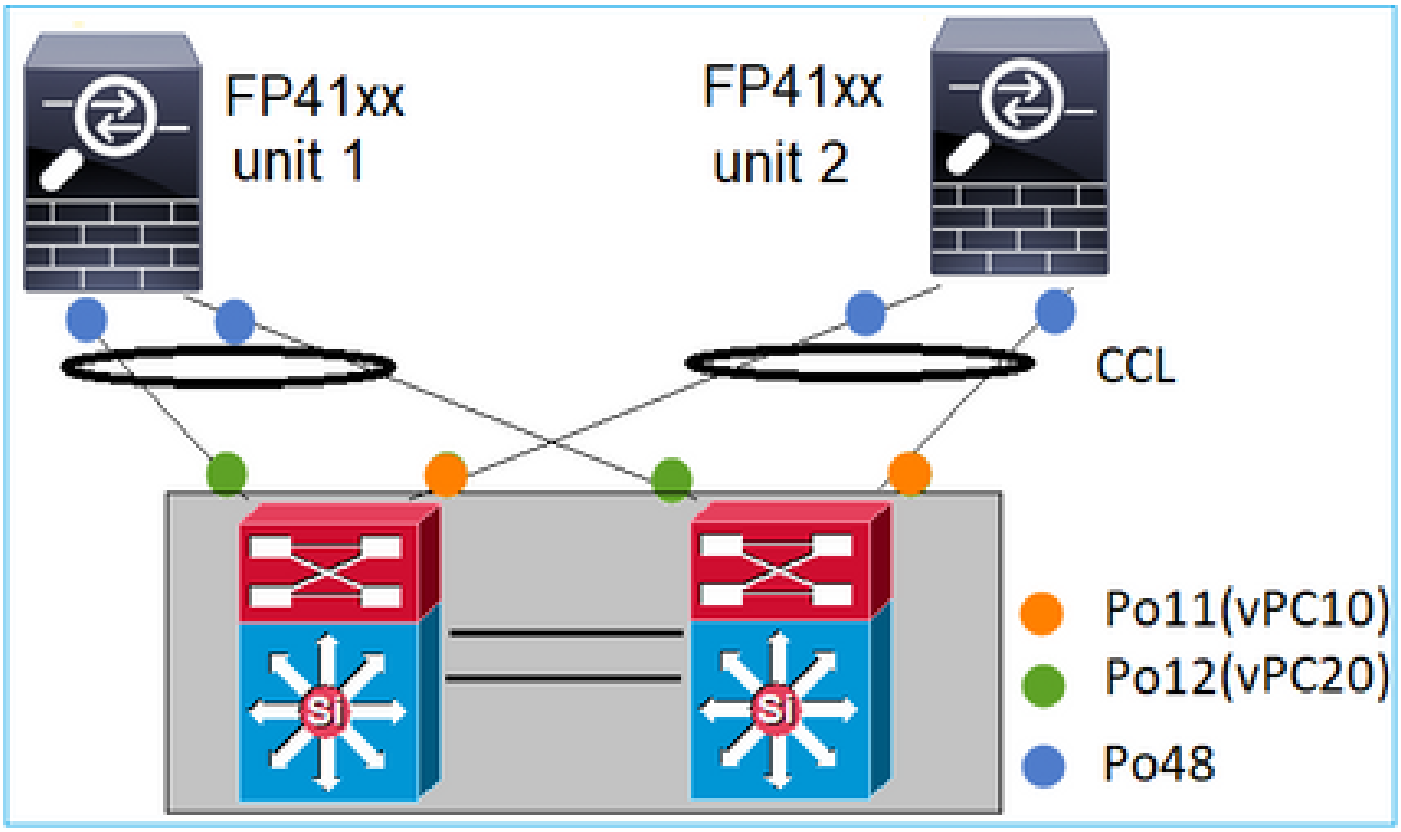
On the other hand, the Cluster Control Link (CCL) uses Individual port-channel mode and per best practices, the bandwidth must match the maximum capacity of each member. Additionally, in the case of Nexus, each port-channel belongs to a different vPC.



Similarly, in case of FP41xx:

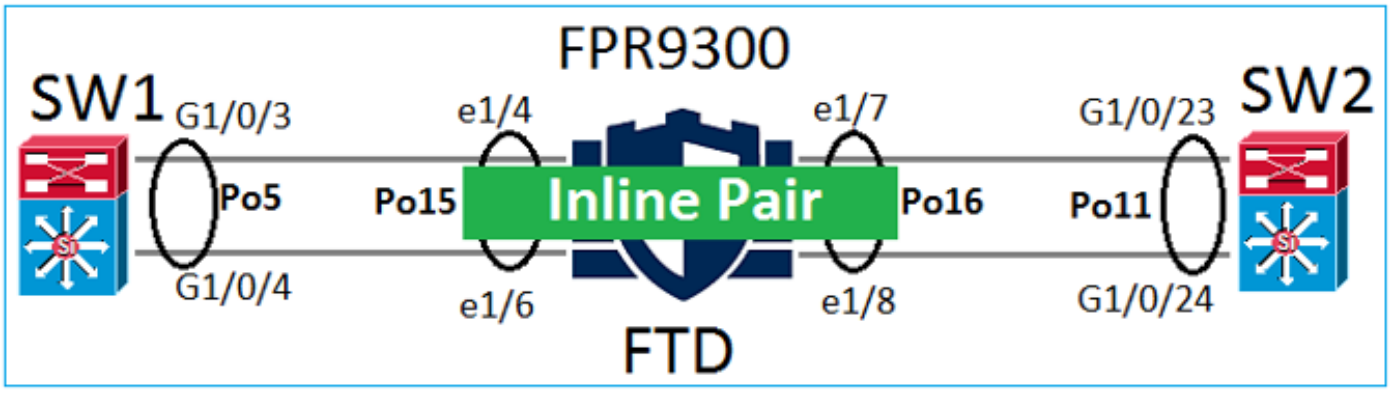


And the CCL:



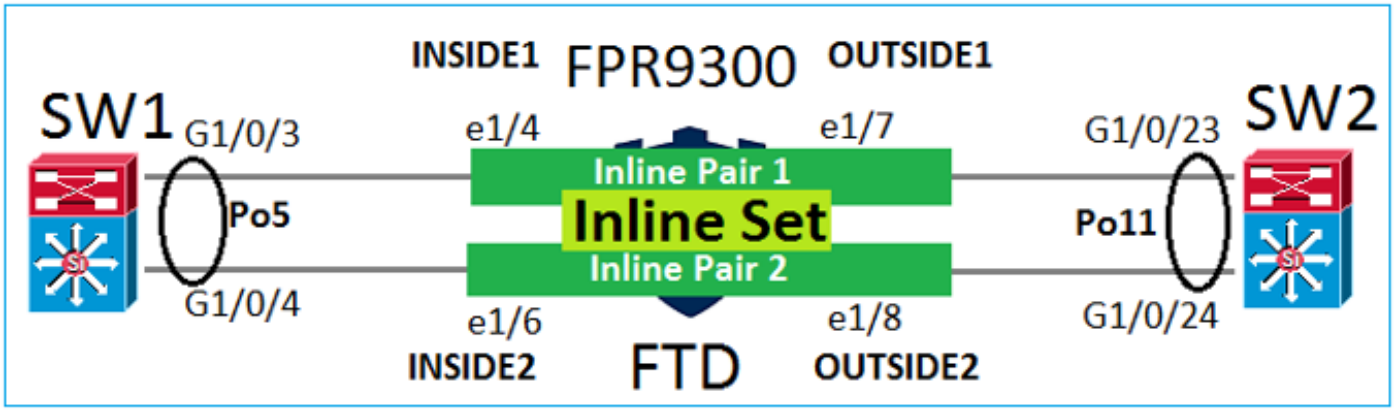
Case 3. Port-ChannelTerminated on FXOS

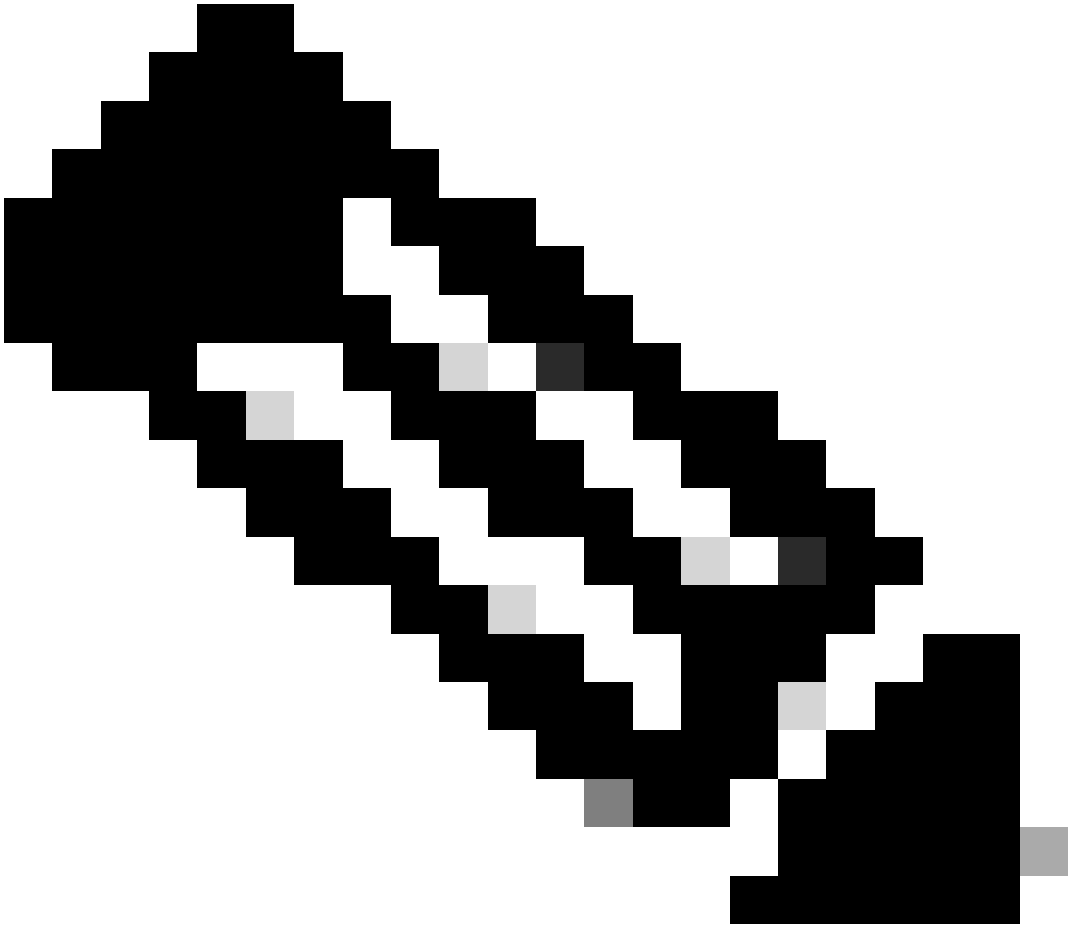
Port-Channel terminated on FXOS chassis. Here is an example of this design:



Case 4. Port-Channel Through FXOS

The Port-Channel goes through the FXOS chassis. Here is an example of this design:





Note: In the second scenario, there is no Port-Channel configured on the Firepower appliance.

Port-Channel terminated on FXOS vs Port-Channel through FXOS

Feature	Comments

Port-Channel terminated on FXOS chassis (MIO)	Works as from FXOS 2.1.1
Port-Channel goes through FXOS chassis (MIO)	• Works before FXOS 2.1.1.58 • Does not work on FXOS >= 2.1.1.58 and < 2.3.1.3 (due to Cisco bug ID CSCva00405) • Works after FXOS 2.3.1.3

Additional Considerations

LACP Graceful Convergence

In case of a Cluster setup (ASA or FTD), the recommendation is for LACP Graceful Convergence to be enabled on Nexus.

Frequently Asked Questions (FAQ)

Q. Is SSP port-channel hash distribution fixed or adaptive?

FXOS uses resilient hash distribution. This seems to be equivalent to the fixed hash-distribution mode described in Nexus 7000/9k documentation online. In resilient hashing, if a link fails, the flows assigned to the failed link are redistributed uniformly among the active links. The current flows through the active links are not rehashed and their packets are not delivered out of order. When a link is added to the port-channel or ECMP group, some of the flows hashed to the current links are rehashed to the new link, but not across all current links.

Q. What happens if the switchports connected to the Port-Channel go down? Does FTD monitor the physical link, or the port-channel?

If all the port-channel interface members go down, the port-channel does down as well. The Port Channel Operation State is shown as failed. From the FTD point of view, the port-channel is shown as down. On the other hand, in this rule, there is an exception: When the switches use stacking. With LACP, the system ID uses the stack MAC address from the active switch, and if the active switch changes, the LACP system ID can change. If the LACP system ID changes, the entire EtherChannel flaps, and there is STP re-convergence. Use the stack-mac persistent timer command to control whether or not the stack MAC address changes after an active switch failover.

Q. Would like to use the command "port-channel min-bundle 2" so that if one link in the port-channel goes down then the port-channel goes down and the firewall does a failover.
This option is not possible on FXOS chassis. As a workaround and whenever possible, configure the lacp min-links command on the peer switches.

Q. How to Capture LACP packets?

Case 1. Port-Channel terminated on the logical appliance (FTD/ASA)

- The Port-Channel is actually terminated at the chassis level (FXOS).
- You cannot capture LACP packets (ingress or egress) at neither chassis level (FXOS) nor application level (FTD/ASA).

Case 2. Port-Channel through the FTD – FTD interface deployed as inline-set:

```
inline-set set1
    snort fail-open down
    interface-pair INSIDE OUTSIDE
!
interface Ethernet1/2
 nameif INSIDE
 cts manual
  propagate sgt preserve-untag
  policy static sgt disabled trusted
!
interface Ethernet1/3
 nameif OUTSIDE
 cts manual
  propagate sgt preserve-untag
  policy static sgt disabled trusted

LACP Ethertype is 0x8809 (dec 34825):
firepower# capture CAP interface INSIDE ethernet-type 34825
firepower# show capture CAP
   1: 21:15:00.403131       2894.0f57.271d 0180.c200.0002 0x8809 Length: 124 <-- LACP packet

                          0101 0114 8000 0017 dfd6 ec00 0016 8000
                          0223 3d00 0000 0214 8000 0017 dfd6 ec00
                          0015 8000 0222 3d00 0000 0310 8000 0000
                          0000 0000 0000 0000 0000 0000 0000 0000
                          0000 0000 0000 0000 0000 0000 0000 0000
                          0000 0000 0000 0000 0000 0000 0000 0000
                          0000 0000 0000 0000 0000 0000 0000
```

Case 3. Port-Channel through the FTD – FTD interface deployed as bridge-group mode:

```
interface Ethernet1/2
 bridge-group 1
 nameif INSIDE
 cts manual
  propagate sgt preserve-untag
  policy static sgt disabled trusted
 security-level 0
!
interface Ethernet1/3
 bridge-group 1
 nameif OUTSIDE
 cts manual
  propagate sgt preserve-untag
  policy static sgt disabled trusted
 security-level 0
!
interface BVI1
 ip address 192.168.201.134 255.255.255.0

firepower# capture CAP interface INSIDE ethernet-type 34825
firepower# show capture CAP
```

```
1 packet captured

   1: 21:21:29.731987       2894.0f57.271c 0180.c200.0002 0x8809 Length: 124 <-- LACP packet

                          0101 0114 8000 0017 dfd6 ec00 0015 8000
                          0222 7d00 0000 0214 0000 0000 0000 0000
                          0000 0000 0000 0000 0000 0310 8000 0000
                          0000 0000 0000 0000 0000 0000 0000 0000
                          0000 0000 0000 0000 0000 0000 0000 0000
                          0000 0000 0000 0000 0000 0000 0000 0000
                          0000 0000 0000 0000 0000 0000 0000
1 packet shown
```

Q. How to migrate from a single port to a Port-Channel?

This change requires a Maintenance Window (MW) and is intrusive. Once you migrate from a single interface to Port-Channel all configuration related to the single interface is disassociated from it. Once you create the Port-Channel there is a need to re-associate the same configuration with the newly configured Port-Channel, for example, NAT, Routing, VPN, and so on. For FTD there is a note in this document:
Configure an EtherChannel
For an ASA device the procedure is described in this document:
Converting In-Use Interfaces to a Redundant or EtherChannel Interface

Q. How to change FTD high availability (HA) link to Port-Channel?

This change requires a Maintenance Window (MW) and is intrusive. You must break the HA and reconfigure it. In the new HA pair specify as an HA link the Port-Channel. Related document:
Configure FTD High Availability on Firepower Appliances

Q. Firepower with ASA shows port-channel Up, physical interface status down

This is related to Cisco bug ID CSCvp03354

Q. Does it matter what to choose for the Port-Channel ID on the FMC? Does it have to match anything on the switch side?

No, it does not matter. You can use whatever Port-Channel ID you want.

Q. Under the Port-Channel Advanced tab, is there a need to do anything for the active/standby MAC?
If you plan to use the Port-Channel in Access Mode (no trunk) and you use High Availability (HA) setup, then Active/Standby MAC is highly recommended to be configured. This recommendation is not Port-Channel-specific but is applicable to any HA setup.

Q. Is it possible to configure descriptions for interface members of a Port-Channel?

Currently (FXOS 2.13.x), it is not supported. Check the latest FXOS configuration guide for additional details.

Q. It is possible to change the FXOS port-channel load-balancing algorithm?

Currently (FXOS 2.13.x), it is not supported. Check the latest FXOS configuration guide for additional details.

Q. Is it possible to configure the minimum number (min-links) of member interfaces in a port-channel in order to transition the port-channel into the bundled state?

Currently (FXOS 2.13.x), it is not supported. Check the latest FXOS configuration guide for additional details.

Related Information

- FXOS Configuration Guides
- FMC/FTD Configuration Guides