Configure Rogue/COOP Exception List in ACI

Contents

Introduction

This document describes about **Rogue/COOP Exception List** feature in ACI (Application Centric Infrastructure) and covers configuration and verification.

Why Exception list?

The "Rogue EP Control" feature in ACI minimizes the impact of temporary loops by quarantining endpoints within the specific bridge domain where they occur. However, this feature can sometimes cause unnecessary disruptions. For example, during a firewall failover, both firewalls can momentarily transmit traffic using the same MAC (Media Access Control) address, resulting in glitches until the network converges. Prior to 5.2(3) If ACI detects 4 EP (Endpoint) moves in 60 seconds, it is then made static and not allowed to move for the next 30 minutes. 4 moves in 60 seconds can be realistic in some deployment. Hold time of 30 minutes is aggressive for scenarios where EP moves are expected.

Solution

In order to address this problem it is possible to configure an "**Rogue/COOP Exception List.**" MAC addresses in the Exception List it then uses a higher threshold criteria to detect Rogue. MAC configured in Exception List is made rogue after 3000 moves in 10-minute interval.MAC address in Exception List uses a higher COOP (Council of Oracle Protocol) Dampening threshold to avoid getting dampened in COOP. You can add upto 100 MAC address in exception list.

Prerequisite

- This feature is available from version starting 5.2(3)
- This option can be used only If the BD (Bridge Domain) is a L2 BD (As if the BD is not configured for IP routing)
- Rogue feature must be enabled for Rogue Exception List behavior to work.

Configuration of Rogue/COOP Exception List

This feature can be utilized in Layer 2 Bridge Domains (L2 BD) to prevent specific MAC addresses from being flagged as rogue due to legitimate movements.

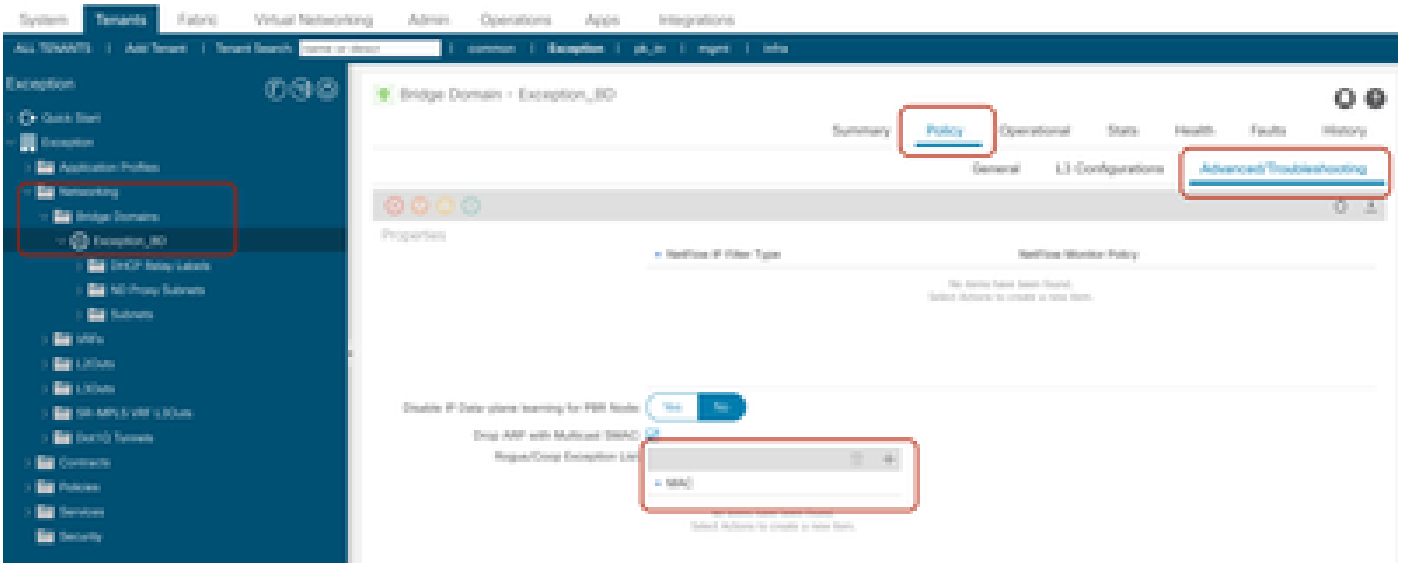
Configuration using APIC (Application Policy Infrastructure Controller) GUI

To configure:

Step 1. Log in to the Cisco APIC GUI.

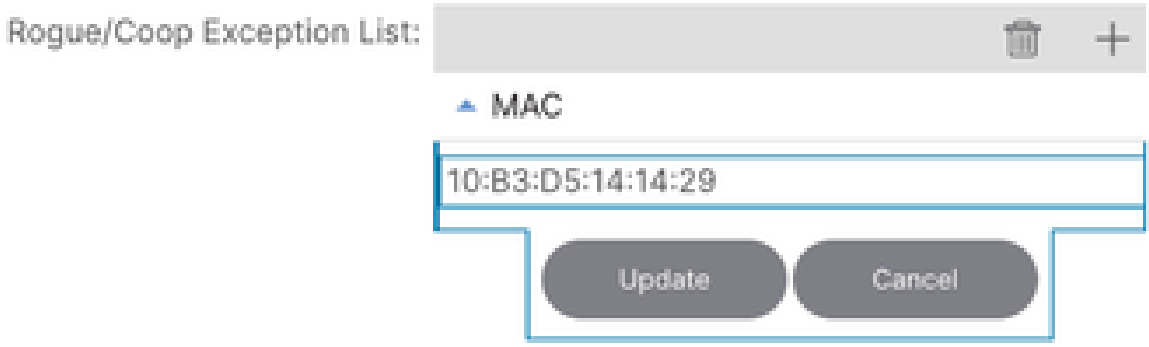
Step 2. Go to **Tenant > Networking > Bridge Domains > BD > Policy > Advanced/Troubleshooting Tab**

On This page you can add MAC addresses in Exception list.



Step 3. Select + icon to add MAC address in Rogue/COOP Exception List.

Step 4. Add MAC address and update.



Verification

To demonstrate this feature, There is an endpoint with the MAC address 10:B3:D5:14:14:29 connected to our ACI fabric within the Tenant Exception and Bridge Domain (BD) BD-Exception.

After adding the MAC address to the exception list in the "Configuration of Rogue/COOP Exception List" section of this document, the configuration can be verified using the Managed Object (MO) query: moquery -c fvRogueExceptionMac

APIC CLI:

<#root>

```
bgl-aci04-apic1#
```

```
moquery -c fvRogueExceptionMac
```

```
Total Objects shown: 1

# fv.RogueExceptionMac
mac : 10:B3:D5:14:14:29
annotation :
childAction :
descr :
dn : uni/tn-Exception/BD-Exception_BD/rgexpmac-10:B3:D5:14:14:29
extMngdBy :
lcOwn : local
modTs : 2024-07-17T04:57:04.923+00:00
name :
nameAlias :
rn : rgexpmac-10:B3:D5:14:14:29
status :
uid : 16222
userdom : :all:

bgl-aci04-apic1#
```

Leaf CLI:

This moquery provides the timers applied on rogue Exception list.

<#root>

```
bgl-aci04-leaf1#
```

```
moquery -c "topoctrlRogueExpP"
```

```
Total Objects shown: 1

# topoctrl.RogueExpP
childAction :
descr :
dn : sys/topoctrl/rogueexpp
lcOwn : local
modTs : 2024-07-13T15:51:57.921+00:00
name :
nameAlias :
rn : rogueexpp
rogueExpEpDetectIntvl : 600   <<< Detection Interval in second
rogueExpEpDetectMult : 3000   <<< Detection Multiple (No of moves)
rogueExpEpHoldIntvl : 30      <<< Hold Interval in second
status :
```

With moquery you can verify any particular mac is added in Exception list.

<#root>

```
bgl-aci04-leaf1#
```

```
moquery -c "l2RogueExpMac" -f 'l2.RogueExpMac.mac=="10:B3:D5:14:14:29"'
```

```
Total Objects shown: 1
# l2.RogueExpMac
mac : 10:B3:D5:14:14:29
childAction :
dn : sys/ctx-[vxlan-2293760]/bd-[vxlan-15957970]/rogueexpmac-10:B3:D5:14:14:29
lcOwn : local
modTs : 2024-07-17T04:57:04.939+00:00
name :
operSt : up
rn : rogueexpmac-10:B3:D5:14:14:29
status :
bgl-aci04-leaf1#
```

To confirm Exception list parameters from Leaf CLI:

<#root>

```
module-1#
```

```
show system internal epmc global-info | grep "Rogue Exception List"
```

```
Rogue Exception List Endpoint Detection Interval : 600
Rogue Exception List Endpoint Detection Multiple : 3000
Rogue Exception List Endpoint Hold Interval : 30
module-1#
module-1#
module-1#
```

To verify endpoint in learnt in EPMC and check the move counts as well for that endpoint.

Leaf CLI:

<#root>

```
module-1#
```

```
show system internal epmc endpoint mac 10:B3:D5:14:14:29
```

```
MAC : 10b3.d514.1429 ::: Num IPs : 0
Vlan id : 9 ::: Vlan vnid : 8193 ::: BD vnid : 15957970
Encap vlan : 802.1Q/101
VRF name : Exception:Exception_vrf ::: VRF vnid : 2293760
phy if : 0x1a015000 ::: tunnel if : 0 ::: Interface : Ethernet1/22
Ref count : 5 ::: sclass : 16386
Timestamp : 07/17/2024 05:20:20.523019
::: last mv ts: 07/17/2024 05:19:17.424213 ::: ep move cnt: 9   <<<< Shows how many times endpoint move
```

```
::: Learns Src: Hal
EP Flags : local|MAC|sclass|timer|
Aging: Timer-type : HT ::: Timeout-left : 784 ::: Hit-bit : Yes ::: Timer-reset count : 0

PD handles:
[L2]: Hdl : 0x18c1e ::: Hit: Yes
::::


module-1#
```

To check Exception list Configuration:

Leaf CLI:

<#root>

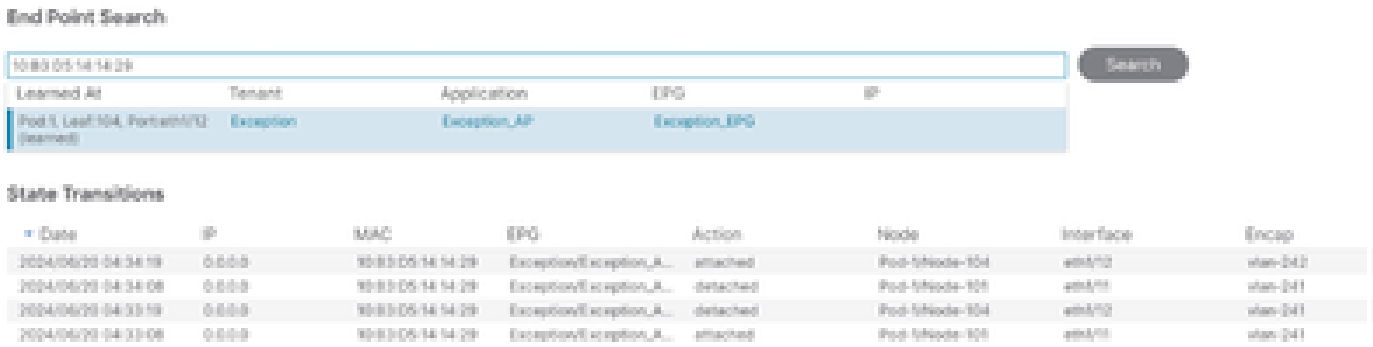
```
module-1#
```

show system internal epmc rogue-exp-ep

```
BD: 15957970 MAC:10b3.d514.1429
[01/01/1970 00:00:00.000000] : 0 Moves in 60 sec

module-1#
```

You can check the endpoint movements in APIC GUI at **Operations > EP tracker**, Search MAC address here.



As still there are movements for this MAC address but now there is no Rogue Flag for this Endpoint.

This can be verified with commands.

LEAF CLI:

To check if rogue flag is added to learned endpoint in leaf epm (endpoint manager)

<#root>

```
bgl-aci04-leaf1#
```

show system internal epm endpoint mac 10:B3:D5:14:14:29

```
MAC : 10b3.d514.1429 ::: Num IPs : 0
Vlan id : 9 ::: Vlan vnid : 8193 ::: VRF name : Exception:Exception_vrf
BD vnid : 15957970 ::: VRF vnid : 2293760
Phy If : 0x1a015000 ::: Tunnel If : 0
Interface : Ethernet1/22
Flags : 0x80004804 ::: sclass : 16386 ::: Ref count : 4
EP Create Timestamp : 07/17/2024 05:19:10.424033
EP Update Timestamp : 07/17/2024 05:22:03.674624
EP Flags : local|MAC|sclass|timer|                <<<< Once if endpoint is rogue a Rogue flag is added

::::

bgl-aci04-leaf1#
```

APIC CLI:

To Check if any fault is raised for Rogue Endpoint endpoint.

<#root>

```
bgl-aci04-apic1#
```

moquery -c faultInst -f 'fault.Inst.code=="F3014"'

```
No Mos found
bgl-aci04-apic1#
```