# **Configure Rogue/COOP Exception List in ACI**

### Contents

Introduction	
Why Exception list?	
Solution	
<u>Prerequisite</u>	
Configuration of Rogue/COOP Exception List	
<u>Verification</u>	

## 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.

System Tenants Fabric V	Artual Networking	Admin Operations	Apps	Integrations				
ALL TOWARTS I AND TOWART I TOWARDS	wards proved at design	i commun i dae	aption 1 p	aja i ngat i lata				
Exception	038 .	Bridge Domain - Except	01, 10					0.0
- Gestanten - 📰 Geseten					Summary Policy	Coverational Sta	en Health	Faults History
1 Di Assission Polites						General 1.3 Contigo	atora Advard	pritrodisation? be
- 🔤 Indje Storains								0.2
- @ Looper, 80	·	toporten.		<ul> <li>Relifice # File Type</li> </ul>		Relifica Monto Pal	εų.	
i 🔤 Ni thuy Subnets					100	Annual factor bases (based) Antipera (bases annual factor)		
i 🖿 Subres								
s 📷 Lations								
a ன Littles a ன Sin Adv. i viti u blass		Disable IP Data-plane tearing	or PBR Noder					
> En berg heren		Dog ANP with M.	Access (1989-1)					
3 E Comune 3 E Polose		subscript .		- 1600)				
a 🛄 Beratana				Carlos Andrews Carlos and a strength of the	- 100			

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



Rogue/Coop Exception List:		1	+
	<ul> <li>MAC</li> </ul>		
	10:B3:D5:14:14:29		
	Update Cancel		

### 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:

```
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</pre> rogueExpEpDetectMult : 3000 <<< Detection Multiple (No of moves)</pre> 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=="l0: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
```

To confirm Exception list parameters from Leaf CLI:

<#root>

status :

bgl-aci04-leaf1#

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#
```

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</pre>

```
::: 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.

0.00.051414(29						Search	
Learned At	Tenant	Applica	filion	DPG	p.		
Posts Leaf-104, Portielt (Instruct)	WPG Exception	Exception	w,AP	Exception_BPG			
tate Transitions							
tate Transitions	p	MAC	696	Action	Node	interface	Encap
Cate     Conter     Date     Date     Date	P 0.000	MAC 8083-05-14-14-29	(PG Economicontecontor	Action	Node Pod-Misde-104	interface wintrid	Encap vian-242
Cate     Cate     Cate     Contended     Contend     Contended     Contended     Contended	(P 0.000 0.000	MAC 308305343429 308305343429	EPG Ecception/Ecception Ecception/Ecception	Action UA attached UA detached	Node Pod-Shiste-101 Pod-Shiste-101	interface ent/12 ent/11	Encep vian-141
* Cute * Cute 2024/04/20 04:54:19 2024/04/20 04:54:08 2024/04/20 04:53:19	(P 0.000 0.000 0.000	MAC 101031051414129 101031051414129 101031051414129	(PG Ecospice/Ecospice Ecospice/Ecospice Ecospice/Ecospice	Action UA. ettached UA. detached UA. detached	Node Pod-Shiede-104 Pod-Shiede-101 Pod-Shiede-104	interface ent/nz ent/nz ent/nz	Encep stan-242 stan-241 stan-241

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
```

```
• • • •
```

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#