

排除ACI OSPF邻接故障

目录

[简介](#)

[拓扑](#)

[OSPF对等配置要求](#)

[OSPF邻接故障排除-常规检查表](#)

[排除OSPF邻接故障-故障](#)

[捕获节点上的控制平面流量](#)

[Wireshark验证](#)

[故障排除情况](#)

[排除OSPF邻接故障：区域ID不匹配](#)

[排除OSPF邻接故障：区域类型不匹配](#)

[OSPF邻接故障排除：重复路由器ID](#)

[排除OSPF邻接故障：MTU不匹配](#)

[排除OSPF邻接故障：身份验证不匹配](#)

[排除OSPF邻接故障：Hello/Dead计时器不匹配](#)

[排除OSPF邻接故障：接口类型不匹配](#)

[广播](#)

[点对点](#)

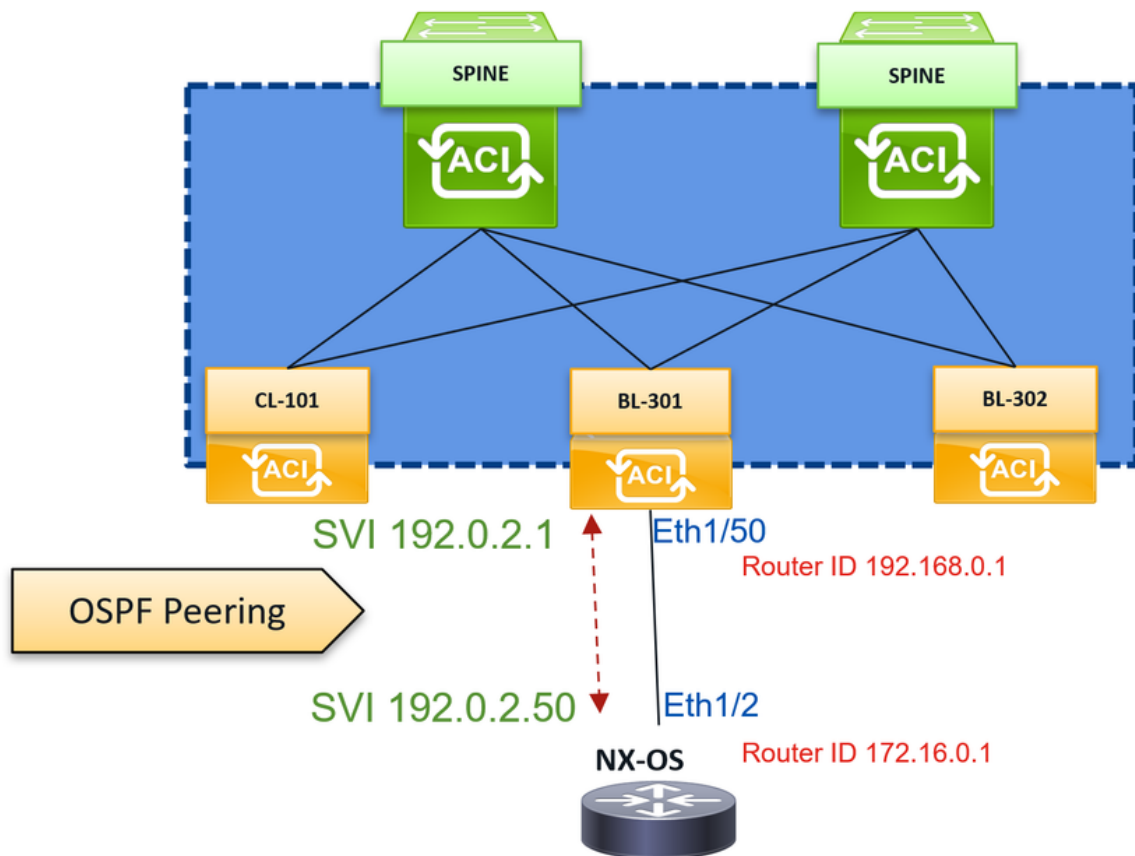
[验证命令清单](#)

[相关信息](#)

简介

本文档介绍如何排除以应用为中心的基础设施(ACI)开放最短路径优先(OSPF)邻接故障。

拓扑



拓扑

OSPF对等配置要求

OSPF是可以在Cisco ACI和外部路由器之间启用的协议之一。思科ACI支持所有常用选项，例如OSPF区域（包括主干）、各种末节选项、邻居身份验证以及其他类似选项。

L3Out包括路由协议选项、交换机特定配置（节点配置文件）和接口特定设置（接口配置文件）。OSPF相关参数主要可在两个位置进行配置，就像普通路由器一样。第一个是全虚拟路由和转发(VRF)或全节点配置，例如可在L3Out自身上配置的区域ID和区域类型。第二个参数是接口级别参数，例如OSPF hello间隔或接口类型(广播、点对点(P2P))。

以下是在ACI边界枝叶与外部路由器之间建立OSPF邻接关系的要求：

1. OSPF区域ID和类型必须匹配
2. OSPF路由器ID必须唯一
3. 最大传输单位(MTU)必须匹配(默认情况下，交换矩阵将其设置为9000，大多数Cisco IOS®/NXOS将其设置为1500)
4. OSPF身份验证密钥和类型必须匹配（如果使用）
5. OSPF Hello间隔和Dead间隔必须匹配
6. OSPF网络类型必须匹配

[白皮书](#)详细介绍了与支持路由协议的ACI L3Out相关的设计概念和选项。

如果您不熟悉L3Out设置和其他基本要求，请参考白皮书。

OSPF邻接故障排除-常规检查表

无论OSPF邻接关系之前是启用还是从未启用，最好先验证基本要求。

步骤1:Ping远程终端接口。这有助于确认您是否具有到远端的IP可达性，这是OSPF出现的主要要求。

```
iping -V <vrf> <remote_end_IP>
example:
BL-301# iping -V abc1:vrf-1 192.0.2.50
```

第二步：验证基本配置参数：

1. OSPF区域ID和类型必须匹配
2. OSPF路由器ID必须唯一
3. MTU必须匹配（默认情况下，交换矩阵将其设置为9000，而大多数Cisco IOS/NXOS将其设置为1500）
4. OSPF身份验证密钥和类型必须匹配（如果使用）
5. OSPF Hello间隔和Dead间隔必须匹配
6. OSPF网络类型必须匹配

命令输出显示推送到枝叶的配置属性。

<#root>

```
BL-301# show ip int bri vrf abc1:vrf-1
IP Interface Status for VRF "abc1:vrf-1"(137)
Interface          Address          Interface Status
vlan1              192.0.2.1/24    protocol-up/link-up/admin-up --> l3out SVI
lo9                192.168.0.1/32  protocol-up/link-up/admin-up --> Router ID SVI
```

BL-301#

show ip ospf interface vlan 1

Vlan1 is up, line protocol is up
IP address

192.0.2.1/24

, Process ID default VRF

abc1:vrf-1

,

area backbone

Enabled by interface configuration

```
State P2P,  
Network type P2P  
  
 , cost 4  
Index 84, Transmit delay 1 sec  
1 Neighbors, flooding to 1, adjacent with 1  
Timer intervals:  
  
Hello 10, Dead 40  
  
 , Wait 40, Retransmit 5  
Hello timer due in 00:00:03  
  
No authentication
```

```
Number of opaque link LSAs: 0, checksum sum 0
```

```
BL-301#
```

```
show int vlan
```

```
1 | egrep "MTU"
```

```
MTU
```

```
9000
```

```
 bytes, BW 10000000 Kbit, DLY 1 usec
```

```
BL-301#
```

```
show ip ospf vrf abc1:vrf-1 | grep Routing
```

```
Routing Process default with ID
```

```
192.168.0.1
```

```
 VRF abc1:vrf-1 -->
```

```
Router ID
```

记下所有突出显示的详细信息，并确认对应的远程终端参数同步。

排除OSPF邻接故障-故障

```
<#root>
```

```
[+]From the border Leaf we can identify the state of the neighbor state  
BL-301# show ip ospf neighbors vrf
```

```
abc1:vrf-
```

```
1
```

<<EMPTY>>

[+] You can check the associated faults to the VRF.

```
BL-301# moquery -c faultInst -x 'query-target-filter=wcard(faultInst.dn,"
```

```
abc1:vrf-1
```

```
")' | egrep "code|rule|dn|descr|lastTransition"
```

<<EMPTY>>

有些场景在环境中没有活动故障，但枝叶上可能会出现一个故障记录F1385(protocol-ospf-adjacency-down)，表明该邻居上次运行或从未处于完全状态。

可使用moquery -c faultRecord -f 'fault.Inst.code=="F1385"' -x 'query-target-filter=wcard(faultRecord.dn,"abc1:vrf-1")' | grep dn命令来识别此问题。

使用moquery -c faultRecord -f 'fault.Inst.code=="F1385"' -x 'query-target-filter=wcard(faultRecord.dn,"abc1:vrf-1")' -x 'query-target-filter=wcard(faultRecord.created,"2024-01-01")' | egrep "dn" | wc -l命令检查任何特定日期的故障记录数。

您必须确定OSPF接口以及本地和远程配置的IP。

<#root>

[+] Identify the IP applied on the external device from the ARP associated to the interface

```
BL-301# moquery -c arpAdjEp -x 'query-target-filter=wcard(arpAdjEp.ifId,"
```

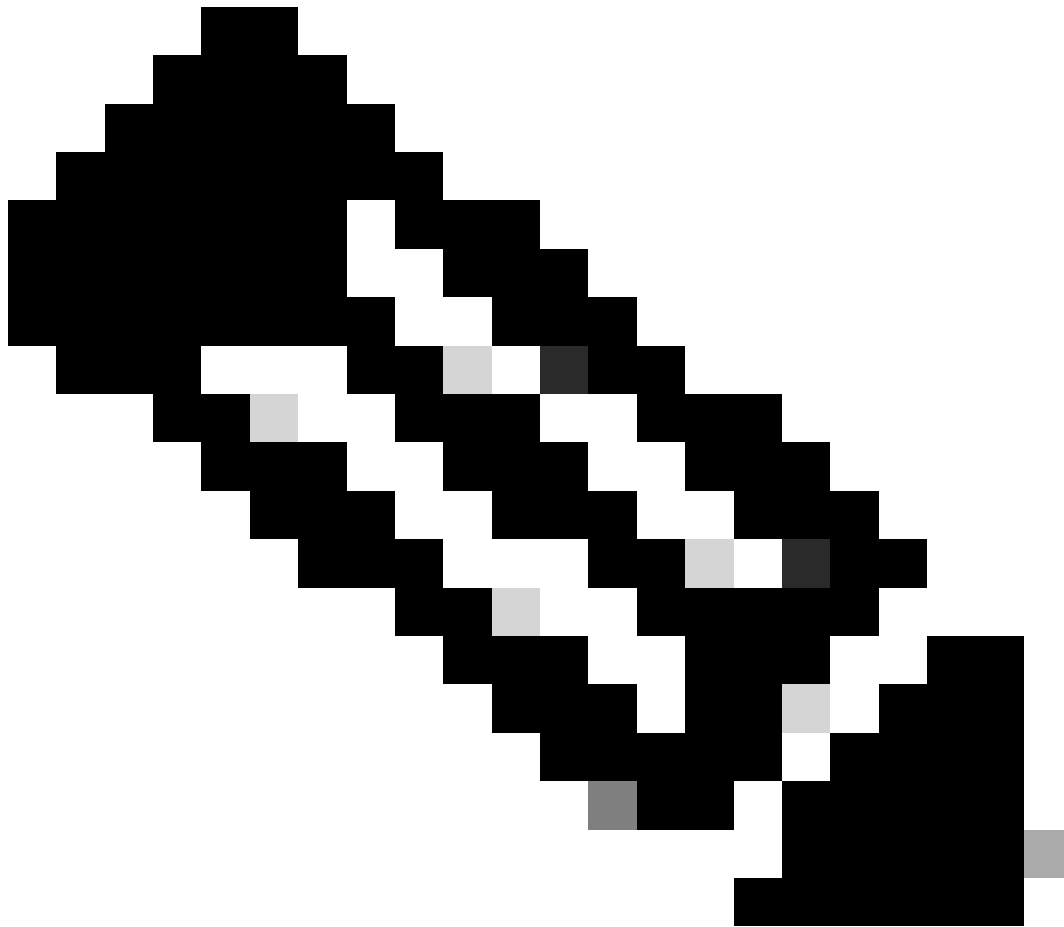
```
vlan1
```

```
")' | grep "ip "  
ip          :
```

```
192.0.2.50
```

捕获节点上的控制平面流量

通过预期的来自边界枝叶的源和目标交换机虚拟接口(SVI)，您可以使用tcpdump实用程序进行检查。



注意：为此，使用允许您查看所有CPU带内控制平面网络流量的接口kpm_inb。

<#root>

```
[+] Capture a single OSPF hello packet using TCPDUMP coming for local BL OSPF IP 192.0.2.1
BL-301# tcpdump src host 192.0.2.1 -vv -e -i kpm_inb
tcpdump: listening on kpm_inb, link-type EN10MB (Ethernet), capture size 262144 bytes
192.0.2.1 > ospf-all.mcast.net:
```

OSPFv2

```
, Hello, length 44
  Router-ID 192.168.0.1,
```

Backbone Area

,
Authentication Type: none (0)

Options [

External

]

Hello Timer 10s, Dead Timer 40s,
Mask 255.255.255.0, Priority 1

[+] Capture a single OSPF hello packet using TCPDUMP coming from external device OSPF IP 192.0.2.50
BL-301# tcpdump src host 192.0.2.50 -vv -e -i kpm_inb
tcpdump: listening on kpm_inb, link-type EN10MB (Ethernet), capture size 262144 bytes
192.0.2.50 > ospf-all.mcast.net:

OSPFv2

, Hello, length 44
Router-ID 172.16.0.1,

Backbone Area, Authentication Type: none (0)

Options [

External

]

Hello Timer 10s, Dead Timer 40s,
Mask 255.255.255.0, Priority 1

Wireshark验证

您可以在Wireshark上捕获OSPF和特定于HOST的流量以对其进行分析。

```
BL-301# tcpdump -i kpm_inb proto ospf -vv -e -w - | tee /data/techsupport/Node-XXX_OSPF.pcap | tcpdump -r - host any
```

```
BL-301# tcpdump -xxxvi kpm_inb 'proto ospf and (host <<X.X.X.X>> or host <<Y.Y.Y.Y>>)' -w /data/techsupport/Node-XXX_OSPF_HOST.pcap
```

```
BL-301# tcpdump -i kpm_inb proto ospf -vv -e -w - | tee /data/techsupport/Node-XXX_OSPF_HOST.pcap | tcpdump -r - host X.X.X.X
```

对于pcap捕获，您可以通过搜索并使用**Analyze > Apply as a Column**来使用Wireshark过滤器。

ospf.area_id =用于标识区域ID

ospf.auth.type =以检查配置的身份验证类型是否匹配

ospf.hello.hello_interval =以检查不同的MTU

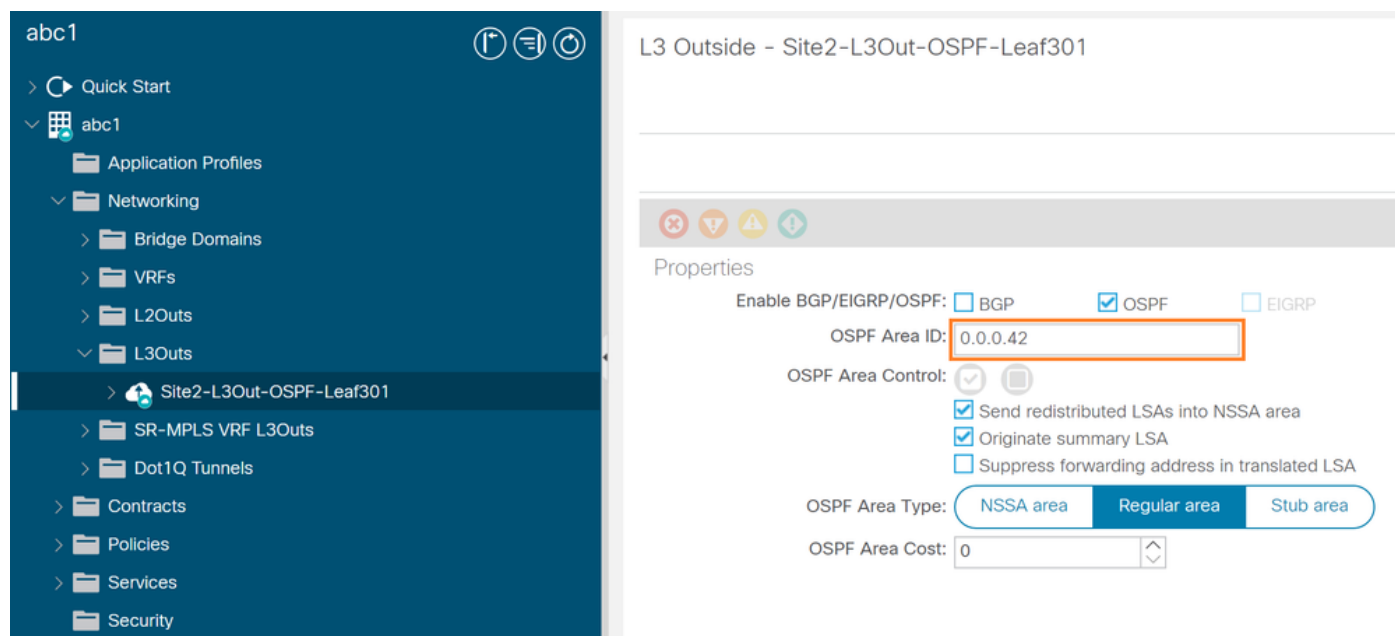
ospf.hello.router_dead_interval =以检查不同的dead间隔配置

ospf.srcrouter = RouterID

故障排除情况

排除OSPF邻接故障：区域ID不匹配

从区域ID为0.0.0.42的APIC配置中，导航到**Fabric > Tenants > Networking > L3Outs > <<L3outName>> > Policy > Main**。



配置了错误的OSPF区域ID 0.0.0.42

从边界枝叶：

<#root>

[+] Check OSPF interface details to confirm current area

BL-301# show ip ospf interface vlan 1 | grep area

IP address 192.0.2.1/24, Process ID default VRF abc1:vrf-1, area

0.0.0.42

Or

```
BL-301# moquery -c ospfIf -x 'query-target-filter=wcard(ospfIf.id,"vlan1")' | grep area
area          :
```

0.0.0.42

[+] Capture a single packet TCPDUMP for local BL OSPF IP

```
BL-301# tcpdump src host 192.0.2.1 -vv -e -i kpm_inb -c 1
192.0.2.1 > ospf-all.mcast.net: OSPFv2, Hello, length 44
Router-ID 192.168.0.1,
```

Area

0.0.0.42

```
, Authentication Type: none (0)
Options [External]
Hello Timer 10s, Dead Timer 40s, Mask 255.255.255.0, Priority 1
```

[+] Capture a single OSPF hello packet using TCPDUMP coming from external device OSPF IP

```
BL-301# tcpdump src host 192.0.2.50 -vv -e -i kpm_inb -c 1
192.0.2.50 > ospf-all.mcast.net: OSPFv2, Hello, length 44
Router-ID 172.16.0.1,
```

Backbone Area

```
, Authentication Type: none (0)
Options [External]
Hello Timer 10s, Dead Timer 40s, Mask 255.255.255.0, Priority 1
```

从外部设备：

<#root>

```
NX-OS# show logging log | tail -n 100 | grep ospf-bootcamp
```

```
2023 Dec 28 15:17:09 NX-OS %OSPF-4-AREA_ERR: ospf-bootcamp [22263] (301-l3-abc1) Packet from 192.0.2.1 on Ethernet1/2 received for wrong area
```

0.0.0.42

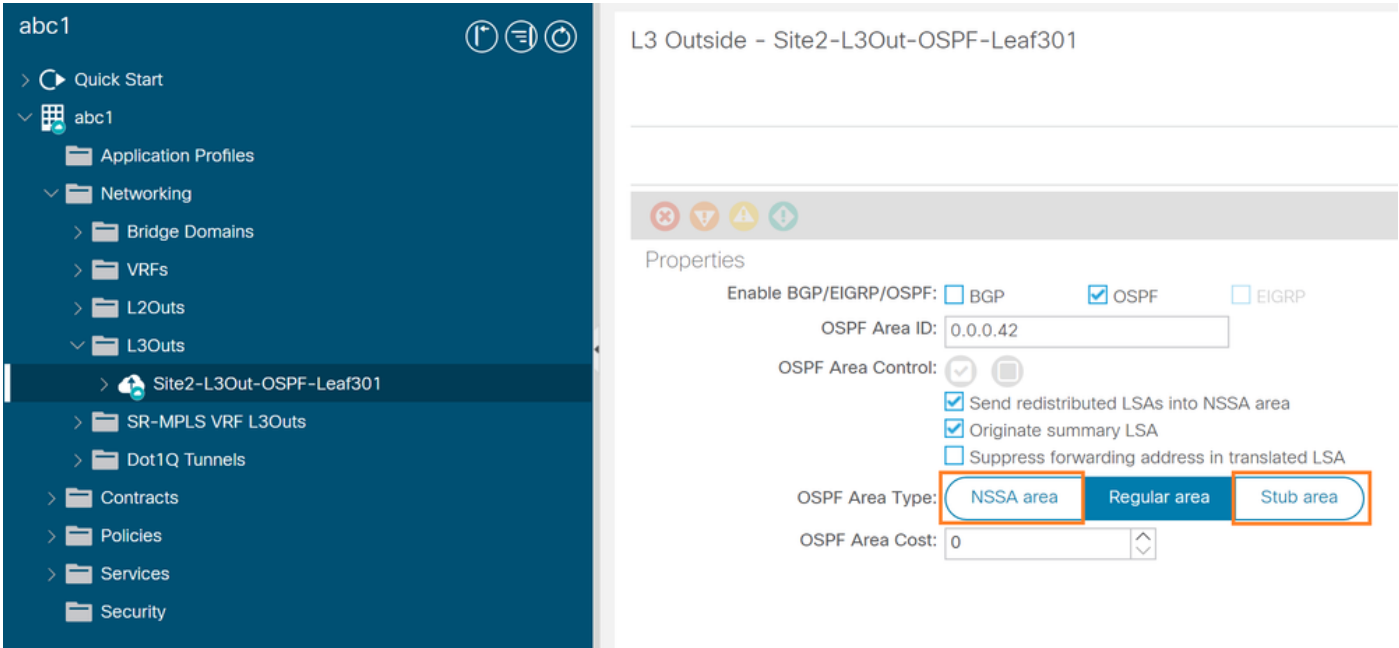
```
NX-OS# show ip ospf interface Ethernet1/2 | grep area
Process ID bootcamp VRF 301-l3-abc1,
```

area 0.0.0.0

解决方案：将OSPF区域与BL上的0.0.0.0或主干网或外部设备上的0.0.0.42匹配。

排除OSPF邻接故障：区域类型不匹配

在ACI GUI中，使用区域类型（NSSA或未节）进行配置时，导航到Fabric > Tenants > Networking > L3Outs > "L3outName" > Policy > Main。



NSSA或末节区域配置。

从边界枝叶：

```
<#root>

[+] Capture a single packet TCPDUMP for local BL OSPF IP
BL-301# moquery -c ospfArea -x 'query-target-filter=wcard(ospfArea.dn,"abc1:vrf-1")' | egrep "type"
type :
```

nssa

```
BL-301# tcpdump src host 192.0.2.1 -vv -e -i kpm_inb -c 1
192.0.2.1 > ospf-all.mcast.net: OSPFv2, Hello, length 44
Router-ID 192.168.0.1, Area 0.0.0.42, Authentication Type: none (0)
Options [
```

NSSA

```
]
Hello Timer 10s, Dead Timer 40s, Mask 255.255.255.0, Priority 1
```

or

```
BL-301# moquery -c ospfArea -x 'query-target-filter=wcard(ospfArea.dn,"abc1:vrf-1")' | egrep "type"
type :
```

stub

```
BL-301# tcpdump src host 192.0.2.1 -vv -e -i kpm_inb -c 1
192.0.2.1 > ospf-all.mcast.net: OSPFv2, Hello, length 44
Router-ID 192.168.0.1, Area 0.0.0.42, Authentication Type: none (0)
Options [
```

none

```
]
Hello Timer 10s, Dead Timer 40s, Mask 255.255.255.0, Priority 1
```

```
[+] Capture a single OSPF hello packet using TCPDUMP coming from external device OSPF IP
BL-301# tcpdump src host 192.0.2.50 -vv -e -i kpm_inb -c 1
192.0.2.50 > ospf-all.mcast.net: OSPFv2, Hello, length 44
Router-ID 172.16.0.1, Area 0.0.0.42, Authentication Type: none (0)
Options [
```

External

```
]
Hello Timer 10s, Dead Timer 40s, Mask 255.255.255.0, Priority 1
```

从外部设备：

<#root>

[+] Check OSPF interfaces con vrf

```

NX-OS# show ip int bri vrf 301-l3-abc1
IP Interface Status for VRF "301-l3-abc1"(21)
Interface          IP Address      Interface Status
Lo1001             110.1.0.1       protocol-up/link-up/admin-up
Eth1/2.1120        192.0.2.50      protocol-up/link-up/admin-up

```

```

NX-OS# show ip ospf interface Ethernet1/2 | grep area
Process ID bootcamp VRF 301-l3-abc1,

```

area 0.0.0.0

解决方案：在L3Out上定期匹配OSPF区域类型，或从外部设备开始匹配。

OSPF邻接故障排除：重复路由器ID

重复的路由器ID会阻止形成OSPF邻接关系。在ACI交换矩阵中，配置OSPF路由器ID后，枝叶使用路由器ID IP地址创建环回。由于此地址用于环回，因此当它发生故障时，不能与使用的接口IP重叠。

在本例中，您可以确认邻居设备的路由器ID配置错误。

从ACI GUI中，导航至Fabric > Tenants > Networking > L3Outs > "L3outName" > "Node-X" > Configured Nodes > topology/pod-Y/node-X。

The screenshot displays the ACI GUI configuration for a node. On the left, the navigation pane shows the hierarchy: abc1 > Networking > L3Outs > Site2-L3Out-OSPF-Leaf301 > Logical Node Profiles > node-301 > Configured Nodes > topology/pod-1/node-301. The right pane, titled 'Node Association', shows the configuration for 'node-301'. The 'Router ID' field is highlighted with an orange box and contains the value '172.16.0.1'. Below it, the 'Use Router ID as Loopback Address' checkbox is checked. The 'Loopback Addresses' section is empty.

来自邻居设备的路由器ID配置错误。

从边界枝叶：

<#root>

[+] Check OSPF interfaces associated with the VRF

BL-301# show ip int bri vrf abc1:vrf-1

IP Interface Status for VRF "abc1:vrf-1"(137)

Interface	Address	Interface Status
vlan1	192.0.2.1/24	protocol-up/link-up/admin-up
lo9		

172.16.0.1

/32 protocol-up/link-up/admin-up

[+] Capture a single packet TCPDUMP for local BL OSPF IP

BL-301# tcpdump src host 192.0.2.1 -vv -e -i kpm_inb -c 1

192.0.2.1 > ospf-all.mcast.net: OSPFv2, Hello, length 44

Router-ID

172.16.0.1

, Backbone Area, Authentication Type: none (0)

Options [External]

Hello Timer 10s, Dead Timer 40s, Mask 255.255.255.0, Priority 1

[+] Capture a single OSPF hello packet using TCPDUMP coming from external device OSPF IP

BL-301# tcpdump src host 192.0.2.50 -vv -e -i kpm_inb -c 1

192.0.2.50 > ospf-all.mcast.net: OSPFv2, Hello, length 48

Router-ID

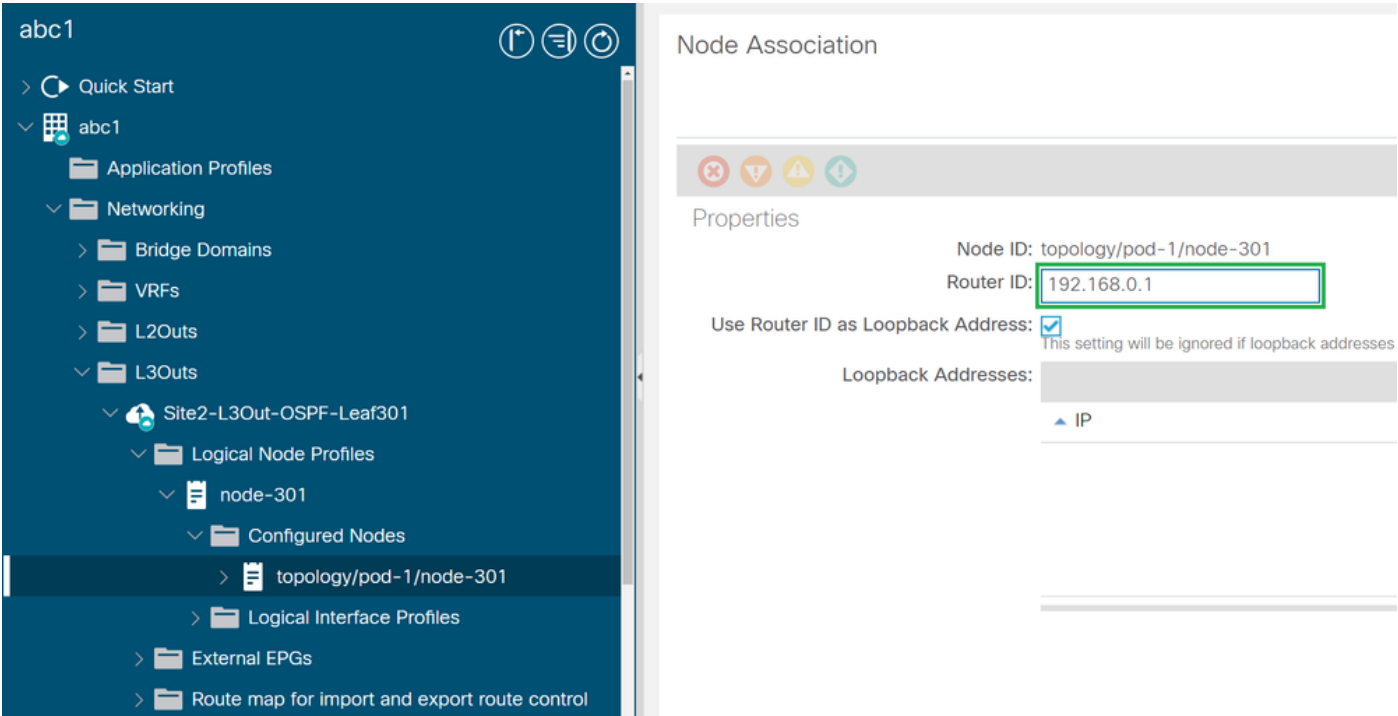
172.16.0.1

, Backbone Area, Authentication Type: none (0)
Options [External]
Hello Timer 10s, Dead Timer 40s, Mask 255.255.255.0, Priority 1

从外部设备

NX-OS# show logging log | tail -n 100 | grep ospf-bootcamp
2024 Jan 4 13:55:36 NX-OS %OSPF-4-DUPRID: ospf-bootcamp [22263] (301-13-abc1) Router 192.0.2.1 on int

解决方案：在两个设备上使用不同的路由器ID。



两台设备上使用不同的路由器ID

排除OSPF邻接故障：MTU不匹配

在两个OSPF相邻路由器建立双向通信并完成（广播网络上的）指定路由器(DR)/BDR选举后，路由器会转换到Exstart状态。在此状态

下，相邻路由器将建立active/standby关系，并确定在交换DBD数据包时使用的初始数据库描述符(DBD)序列号。

协商active/standby关系之后(具有最高路由器ID的路由器变为active)，邻居路由器将转换到exchange状态。在此状态下，路由器将交换DBD数据包，这些数据包描述了其整个链路状态数据库。路由器还会发送链路状态请求数据包，这些数据包从邻居请求更新的链路状态通告(LSA)。

如果相邻路由器接口的MTU设置不匹配，则路由器停滞在Exstart/Exchange状态。这是因为MTU较大的路由器会发送一个大于邻居路由器上设置的MTU的数据包，因此邻居路由器会忽略该数据包。

从使用默认继承配置的APIC GUI配置，导航至Fabric > Tenants > Networking > L3Outs > "L3outName" > "Node-X" > Logical Interface Profiles > OSPF Interface Profile。



默认情况下，ACI交换矩阵将第3层接口MTU设置为9000而不是1500

默认情况下，ACI交换矩阵将第3层接口MTU设置为9000而不是1500。由于ACI具有更高的MTU，因此它继续接受来自外部路由器的DBD数据包并尝试确认这些数据包。

如果外部路由器具有较低或较高的MTU，则它会忽略来自ACI的DBD数据包和ACK，继续重新传输初始DBD数据包，并保持Exstart/Exchange状态。

从边界枝叶：

<#root>

[+]From the border Leaf we can identify the state of the neighborhood relation

```
BL-301# show ip ospf neighbors vrf abc1:vrf-1
OSPF Process ID default VRF abc1:vrf-1
Total number of neighbors: 1
Neighbor ID   Pri State      Up Time  Address      Interface
172.16.0.1    1
```

EXCHANGE

```
/ -          01:10:05 192.0.2.50
```

Vlan1

[+] You can check the associated faults to the Tenant:VRF / OSPF interface
BL-301# moquery -c faultInst -x 'query-target-filter=wcard(faultInst.dn,"

abc1:vrf-1

\if-\[

vlan1

```
\])' | egrep "code|rule|dn|descr|lastTransition"  
code :
```

F1385

descr :

OSPF adjacency is not full, current state Exchange

```
dn : topology/pod-1/node-301/sys/ospf/inst-default/dom-abc1:vrf-1/if-[vlan1]/adj-172.16.0  
lastTransition : 2023-12-28T12:26:23.369-05:00  
rule : ospf-adj-ep-failed  
title : OSPF Adjacency Down
```

code :

F3592

descr :

OSPF interface vlan1 mtu is different than neighbor mtu

```
dn : topology/pod-1/node-301/sys/ospf/inst-default/dom-abc1:vrf-1/if-[vlan1]/fault-F3592  
lastTransition : 2023-12-28T12:26:23.369-05:00  
rule : ospf-if-mtu-config-mismatch-err
```

[+] Identify the MTU applied on the OSPF interface
BL-301# show int vlan 1 | egrep "MTU"

MTU

9000

bytes, BW 10000000 Kbit, DLY 1 usec

[+] If the default configuration is on place there will be a mismatch with the 1500 default
BL-301# show ip ospf event-history adjacency | grep "neighbor mtu"

2023-12-28T12:24:31.986149000-05:00 ospf default [20751]: TID 21885:ospfv2_check_ddesc_for_nbr_state:49

neighbor mtu [

1500] is smaller than if mtu 9000

[+] Or if the locally configured MTU is lower than external router

[2023-12-28T14:05:48.495659000-05:00:T:ospfv2_check_ddesc_for_nbr_state:478] abc1:vrf-1DBD from 192.0.2

mtu [1500] is large than if mtu 1200

可能的解决方案：

- 匹配两台设备上的MTU

当更改任一端的MTU时，由于已建立成员资格，因此在下次协商之前会保持该状态，并且可能出于多种原因触发。例如，关闭物理接口、策略重新部署、枝叶重新加载、升级等。

导航至Fabric > Tenants > Networking > L3Outs > "L3outName" > "Node-X" > Logical Interface Profiles > OSPF Interface Profile 如图所示。



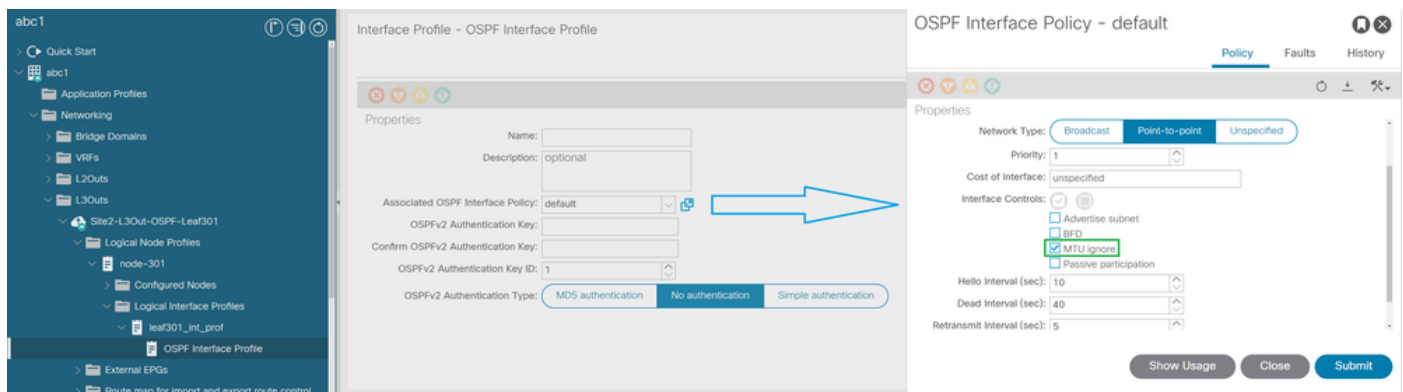
MTU配置为1500

- 关联OSPF接口策略中的MTU忽略将重新建立连接。

当OSPF数据库增长时，会出现MTU忽略问题。当MTU仅相差几个字节时，设置会持续很长时间，直到您碰巧遇到了生成DBD的正确LSA组合，或者更新了正好合适的数据包。

小型实验室中的测试运行良好，但生产网络可能会遇到意外行为。

导航至Fabric > Tenants > Networking > L3Outs > "L3outName" > "Node-X" > Logical Interface Profiles > OSPF Interface Profile > Associated OSPF Interface Policy 如图所示。



MTU忽略配置

排除OSPF邻接故障：身份验证不匹配

您可以在OSPF中启用身份验证，以便安全地交换路由更新信息。OSPF 身份验证可以是“无”（或“空”）、“简单”或“MD5”。身份验证方

法“none”表示OSPF不使用身份验证，它是默认方法。使用简单身份验证时，口令通过网络以明文形式传输。如果使用 MD5 身份验证，则口令不会通过网络传递。

下面是 OSPF 支持的三种不同类型的身份验证。

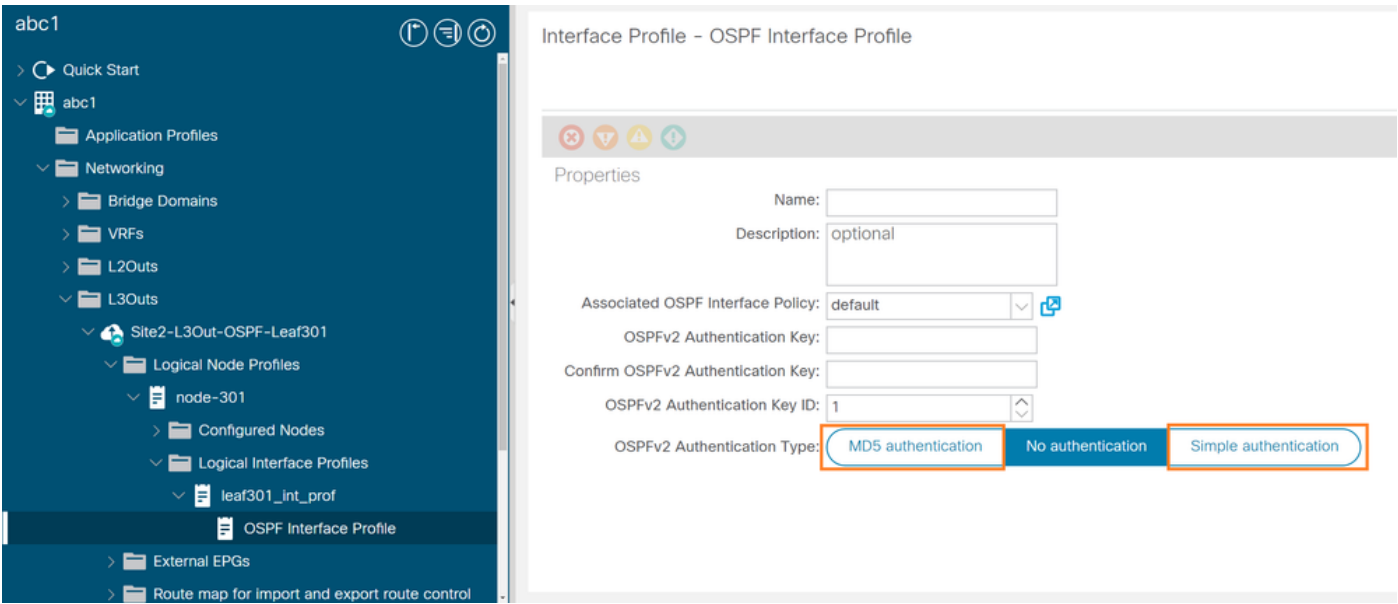
空身份验证 — 又称为类型 0，表示不在数据包报头中包含身份验证信息。这种模式是默认模式。

简单身份验证-也称为类型1，它使用简单的明文密码。

MD5 身份验证 — 又称为类型 2，它使用 MD5 加密口令。

身份验证无需设置。但是，如果已设置，则相同网段上的所有对等路由器必须使用相同的口令和身份验证方法。

从ACI GUI导航至Fabric > Tenants > Networking > L3Outs > "L3outName" > "Node-X" > Logical Interface Profiles > OSPF Interface Profile 如图所示。



已配置MD5或简单身份验证

从CLI：

```
<#root>
```

```
[+] Check Authentication type configured
APIC# moquery -c ospfIfP -x 'query-target-filter=wcard(ospfIfP.dn,"tn-abc1/out-Site2-L30ut-OSPF-BL-301
authType      :
```

simple

```
[+] Capture a single packet TCPDUMP for local BL OSPF IP
BL-301# tcpdump src host 192.0.2.1 -vv -e -i kpm_inb -c 1
192.0.2.1 > ospf-all.mcast.net: OSPFv2, Hello, length 44
Router-ID 192.168.0.1, Backbone Area, Authentication Type:
```

simple (

1)

```
Simple text password: cisco
Options [External]
Hello Timer 10s, Dead Timer 40s, Mask 255.255.255.0, Priority 1
```

or

[+] Check Authentication type configured

```
APIC# moquery -c ospfIfP -x 'query-target-filter=wcard(ospfIfP.dn,"tn-abc1/out-Site2-L30ut-OSPF-BL-301
authType      :
```

md5

[+] Capture a single packet TCPDUMP for local BL OSPF IP

```
BL-301# tcpdump src host 192.0.2.1 -vv -e -i kpm_inb -c 1
```

```
192.0.2.1 > ospf-all.mcast.net: OSPFv2, Hello, length 44
Router-ID 192.168.0.1, Backbone Area, Authentication Type:
```

MD5 (2)

```
Key-ID: 1, Auth-Length: 16, Crypto Sequence Number: 0x026c0a34
Options [External]
Hello Timer 10s, Dead Timer 40s, Mask 255.255.255.0, Priority 1
```

```
[+] Capture a single OSPF hello packet using TCPDUMP coming from external device OSPF IP
BL-301# tcpdump src host 192.0.2.50 -vv -e -i kpm_inb -c 1
192.0.2.50 > ospf-all.mcast.net: OSPFv2, Hello, length 48
Router-ID 172.16.0.1, Backbone Area, Authentication Type:
```

none (0)

```
Options [External]
Hello Timer 10s, Dead Timer 40s, Mask 255.255.255.0, Priority 1
```

```
[+] Live OSPF trace Decode for VRF
BL-301# log_trace_bl_print_tool /var/sysmgr/tmp_logs/ospfv2_1_trace.bl | tail -n 250 | grep abc1:vrf-1
[2024-01-04T16:23:29.650806000-05:00:T:ospfv2_set_authentication:70] abc1:vrf-1out pkt on Vlan1:
```

auth simple text: key cisco

```
or
[2024-01-04T16:24:22.794682000-05:00:T:ospfv2_set_authentication:96] abc1:vrf-1out pkt on Vlan1:
```

auth md5: key cisco

, key id 1 Seq 40635829 (time 1704403462)

从外部设备：

```
NX-OS# show logging log | tail -n 100 | grep ospf-bootcamp
2024 Jan  4 16:55:01 NX-OS %OSPF-4-AUTH_ERR: ospf-bootcamp [22263] (301-13-abc1) Received packet from
or
2024 Jan  4 16:55:20 NX-OS %OSPF-4-AUTH_ERR: ospf-bootcamp [22263] (301-13-abc1) Received packet from
```

解决方案：匹配身份验证。

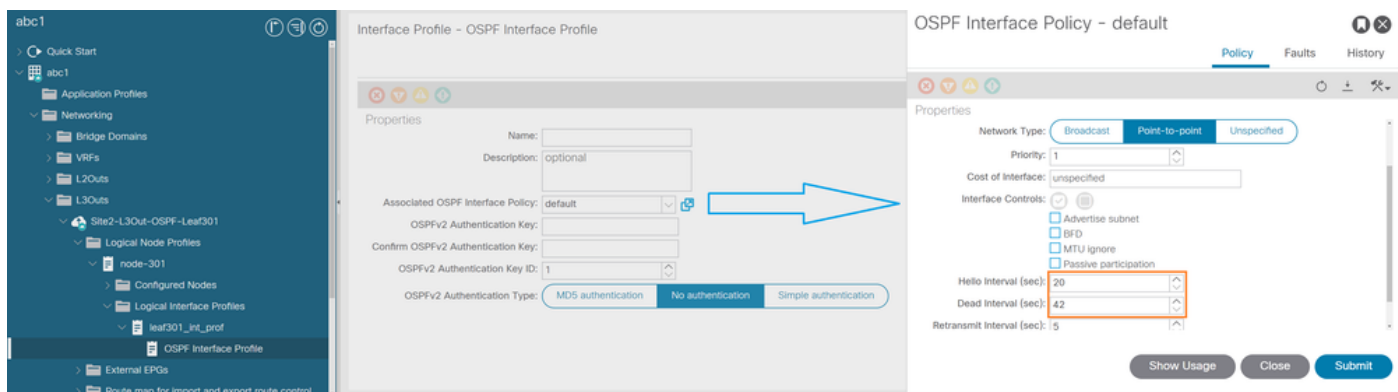
排除OSPF邻接故障：Hello/Dead计时器不匹配

OSPF hello数据包是OSPF进程为保持与这些邻居的连接而发送到其OSPF邻居的数据包。Hello数据包按可配置的时间间隔（以秒为单位）发送。以太网链路的默认值为10秒（P2P和广播网络类型）。Hello数据包包括已在dead间隔内收到hello数据包的所有邻居的列表。dead间隔也可以配置（以秒为单位），默认为hello间隔值的四倍。网络中所有hello间隔的值必须相同。同样，网络中所有停顿间隔的值必须相同。

这两个间隔协同工作，以便通过指示链路运行状态来保持连接。如果路由器在dead间隔内没有收到来自邻居的hello数据包，则会声明该邻居已关闭。

如果在ACI交换矩阵上修改了默认OSPF Hello和Dead计时器，它们必须与外部路由器匹配。

从ACI GUI导航至Fabric > Tenants > Networking > L3Outs > "L3outName" > "Node-X" > Logical Interface Profiles > OSPF Interface Profile > Associated OSPF Interface Policy 如图所示。



自定义Hello/Dead计时器

从边界枝叶：

<#root>

```
[+] Check OSPF interface configuration
BL-301# show ip ospf interface vlan 1 | egrep "Timer|Network"
State P2P, Network type P2P, cost 4
Timer intervals: Hello
```

20

, Dead

42

, Wait 42, Retransmit 5

Or

```
BL-301# moquery -c ospfIf -x 'query-target-filter=wcard(ospfIf.id,"vlan1")' | egrep "deadIntvl|helloIntvl"
```

deadIntvl : 42

helloIntvl : 20

nwT : p2p

Or

```
APIC# moquery -c ospfRsIfPol -x 'query-target-filter=wcard(ospfIfP.dn,"abc1\out-Site2-L3Out-OSPF-BL-301")
tnOspfIfPolName : Custom_OSPF_Interface_Policy
```

```
APIC# moquery -c ospfIfPol -x 'query-target-filter=wcard(ospfIfPol.name,"Custom_OSPF_Interface_Policy")
deadIntvl :
```

42

helloIntvl :

2

0

nwT : p2p

```
[+] Capture a single packet TCPDUMP for local BL OSPF IP
BL-301# tcpdump src host 192.0.2.1 -vv -e -i kpm_inb -c 1
192.0.2.1 > ospf-all.mcast.net: OSPFv2, Hello, length 44
    Router-ID 192.168.0.1, Backbone Area, Authentication Type: none (0)
    Options [External]
```

Hello Timer 20s

,

Dead Timer 42s

, Mask 255.255.255.0, Priority 1

```
[+] Capture a single OSPF hello packet using TCPDUMP coming from external device OSPF IP
BL-301# tcpdump src host 192.0.2.50 -vv -e -i kpm_inb -c 1
192.0.2.50 > ospf-all.mcast.net: OSPFv2, Hello, length 44
      Router-ID 172.16.0.1, Backbone Area, Authentication Type: none (0)
      Options [External]
```

Hello Timer 10s

,

Dead Timer 40s

, Mask 255.255.255.0, Priority 1

从外部设备：

<#root>

[+] Check OSPF interfaces con vrf

NX-OS# show ip int bri vrf 301-l3-abc1

IP Interface Status for VRF "301-l3-abc1"(21)

Interface	IP Address	Interface Status
Lo1001	110.1.0.1	protocol-up/link-up/admin-up
Eth1/2.1120	192.0.2.50	protocol-up/link-up/admin-up

[+] Check OSPF configuration by default Dead timer on NX-OS devices is 4 times hello interval

NX-OS# show run ospf all | section Ethernet1/2.1120 | grep hello

ip ospf hello-interval

10

[+] Check OSPF interface advertized parameters

NX-OS# show ip ospf interface Ethernet1/2.1120 | grep Timer
Timer intervals:

Hello

10

,

Dead

, Wait 40, Retransmit 5

解决方案：匹配OSPF计时器。

排除OSPF邻接故障：接口类型不匹配

本部分介绍在ACI上配置广播或未指定且外部设备为P2P时的故障排除。

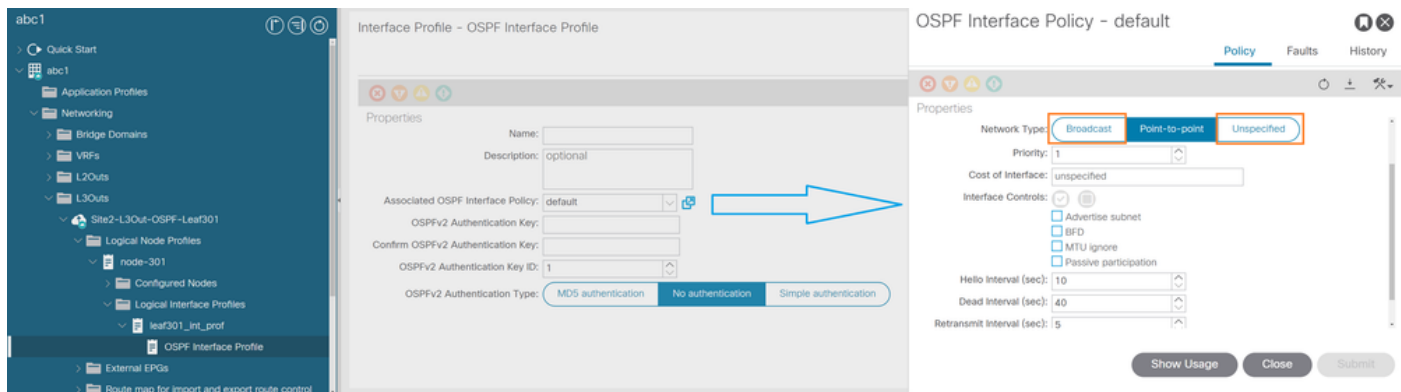
广播

- 广播网络类型是启用了OSPF的以太网接口的默认类型
- 广播网络类型要求链路支持第2层广播功能
- 广播网络类型有一个10秒hello和40秒dead计时器（与P2P相同）
- OSPF广播网络类型需要使用DR/BDR。

点对点

- P2P OSPF网络类型不维护DR/BDR关系
- P2P网络类型有一个10秒hello和40秒dead计时器
- P2P网络类型适用于两台直接相连的路由器

从ACI GUI导航至Fabric > Tenants > Networking > L3Outs > "L3outName" > "Node-X" > Logical Interface Profiles > OSPF Interface Profile > Associated OSPF Interface Policy 如图所示。



已配置广播或未指定的网络类型

从边界枝叶：

<#root>

[+] Check OSPF neighborhood relation

BL-301# show ip ospf neighbors vrf abc1:vrf-1

OSPF Process ID default VRF abc1:vrf-1

Total number of neighbors: 1

Neighbor ID	Pri	State	Up Time	Address	Interface
172.16.0.1	1				

INITIALIZING/DROTHER

00:06:42 192.0.2.50 Vlan1

[+] Check OSPF interface configuration

BL-301# moquery -c ospfIf -x 'query-target-filter=wcard(ospfIf.id,"vlan1")' | egrep "deadIntvl|helloIntvl"

deadIntvl : 40

helloIntvl : 10

nwT :

bcast

or

BL-301# moquery -c ospfIf -x 'query-target-filter=wcard(ospfIf.id,"vlan1")' | egrep "deadIntvl|helloIntvl"

deadIntvl : 40

```
helloIntvl    : 10
nwT           :
```

unspecified

Or

```
APIC# moquery -c ospfRsIfPol -x 'query-target-filter=wcard(ospfIfP.dn,"abc1\out-Site2-L30ut-OSPF-BL-30
tnOspfIfPolName : Custom_OSPF_Interface_Policy
```

```
APIC# moquery -c ospfIfPol -x 'query-target-filter=wcard(ospfIfPol.name,"Custom_OSPF_Interface_Policy")
deadIntvl     : 40
helloIntvl    : 10
nwT           :
```

bcast

```
APIC# moquery -c ospfIfPol -x 'query-target-filter=wcard(ospfIfPol.name,"Custom_OSPF_Interface_Policy")
deadIntvl     : 40
helloIntvl    : 10
nwT           :
```

unspecified

[+] Whether it is bcast or unspecified the interface will show as Broadcast
BL-301# show ip ospf interface vlan 1 | egrep "Timer|Network"
State DR, Network type

BROADCAST

```
, cost 4
  Timer intervals: Hello 10, Dead 40, Wait 40, Retransmit 5

[+] Capture a single packet TCPDUMP for local BL OSPF IP
BL-301# tcpdump src host 192.0.2.1 -vv -e -i kpm_inb -c 1
192.0.2.1 > ospf-all.mcast.net: OSPFv2, Hello, length 48
  Router-ID 192.168.0.1, Backbone Area, Authentication Type: none (0)
  Options [External]
  Hello Timer 10s, Dead Timer 40s, Mask 255.255.255.0, Priority 1
```

Designated Router

192.0.2.1

```
Neighbor List:
  172.16.0.1
```

```
[+] Capture a single OSPF hello packet using TCPDUMP coming from external device OSPF IP
BL-301# tcpdump src host 192.0.2.50 -vv -e -i kpm_inb -c 1
192.0.2.50 > ospf-all.mcast.net: OSPFv2, Hello, length 44
  Router-ID 172.16.0.1, Backbone Area, Authentication Type: none (0)
  Options [External]
  Hello Timer 10s, Dead Timer 40s, Mask 255.255.255.0, Priority 1
```

从外部设备：

<#root>

```
[+] Check OSPF interfaces con vrf
NX-OS# show ip int bri vrf 301-l3-abc1
IP Interface Status for VRF "301-l3-abc1"(21)
Interface          IP Address      Interface Status
Lo1001             110.1.0.1      protocol-up/link-up/admin-up
Eth1/2.1120        192.0.2.50     protocol-up/link-up/admin-up
```

```
[+] Check OSPF configuration by default Dead timer on NX-OS devices is 4 times hello interval
NX-OS# show run ospf all | section Ethernet1/2 | grep network
  ip ospf network
```

point-to-point

```
[+] Check OSPF interface advertized parameters
NX-OS# show ip ospf interface Ethernet1/2 | grep type
      State P2P, Network type
```

P2P

, cost 1

验证命令清单

本文中引用了这些命令，以便对不同场景进行故障排除。

节点	命令	目的
ACI交换机	show ip ospf neighbors vrf <<TNT:VRF>>	检查VRF上的邻居关系
	show ip ospf interface brief vrf <<TNT:VRF>>	检查与VRF关联的OSPF接口
	moquery -c faultInst -x 'query-target-filter=wcard(faultInst.dn,"<<TNT:VRF>>")'	您可以检查VRF的相关故障
	moquery -c ospflf -x 'query-target-filter=wcard(ospflf.dn,"<<TNT:VRF>>")'	检查与VRF关联的所有OSPF接口详细信息
	moquery -c ospflf -x 'query-target-filter=wcard(ospflf.id,"<<vlanX>>")'	检查OSPF接口配置

	moquery -c arpAdjEp -x 'query-target-filter=wcard(arpAdjEp.ifId,"<<vlanX>>")' grep ip	从与接口关联的ARP检查应用于外部设备的IP
	log_trace_bl_print_tool /var/sysmgr/tmp_logs/ospfv2_1_trace.bl tail -n 250 grep <<TNT:VRF>>	VRF的实时OSPF跟踪解码
	tcpdump -i kpm_inb proto ospf -vv -e -w - tee /data/techsupport/Node-XXX_OSPF.pcap tcpdump -r - host any	捕获要在Wireshark上分析的OSPF流量
	tcpdump -i kpm_inb proto ospf -vv -e -w - tee /data/techsupport/Node-XXX_OSPF_HOST.pcap tcpdump -r - host <<X.X.X.X>>	捕获HOST的特定流量，以便在Wireshark上进行分析
	tcpdump -xxxvi kpm_inb 'proto ospf and (host <<X.X.X.X>> or host <<Y.Y.Y.Y>>)' -w /data/techsupport/Node-XXX_OSPF_HOST.pcap	捕获HOST的SRC和DST特定流量，以便在Wireshark上分析
	tcpdump src host <<X.X.X.X>> -vv -e -i kpm_inb -c 1	为和特定主机捕获单个带内控制平面
ACI APIC	moquery -c ospfIfP -x 'query-target-filter=wcard(ospfIfP.dn,"<<TNT>>\out-<<L3outName>>")'	检查配置的身份验证类型
	moquery -c l3ext.RsPathL3OutAtt -x 'query-target-filter=wcard(l3extRsPathL3OutAtt.dn,"<<TNT>>\out-<<L3outName>>")'	检查L3out路径配置
	moquery -c faultRecord -f 'fault.Inst.code=="F1385"' -x 'query-target-filter=wcard(faultRecord.dn,"<<TNT:VRF>>")'	检查故障F1385 protocol-ospf-adjacency-down的故障历史记录
	moquery -c ospfRsIfPol -x 'query-target-filter=wcard(ospfIfP.dn,"<<TNT>>\out-<<L3outName>>")' grep tnOspfIfPolName	检查L3out以获取自定义的关联OSPF接口策略

	moquery -c ospflfPol -x 'query-target-filter=wcard(ospflfPol.name,"Custom_OSPF_Interface_Policy")'	检查自定义关联OSPF接口策略详细信息
NXOS交换机	show ip int bri vrf <<VRF>>	检查OSPF接口con vrf
	show run ospf all section EthernetX/Y	检查OSPF配置
	show ip ospf interface EthernetX/Y	检查OSPF接口通告参数

相关信息

- [排除ACI外部转发故障](#)
- [思科技术支持和下载](#)

关于此翻译

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

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

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