Dépannage des contiguïtés OSPF ACI

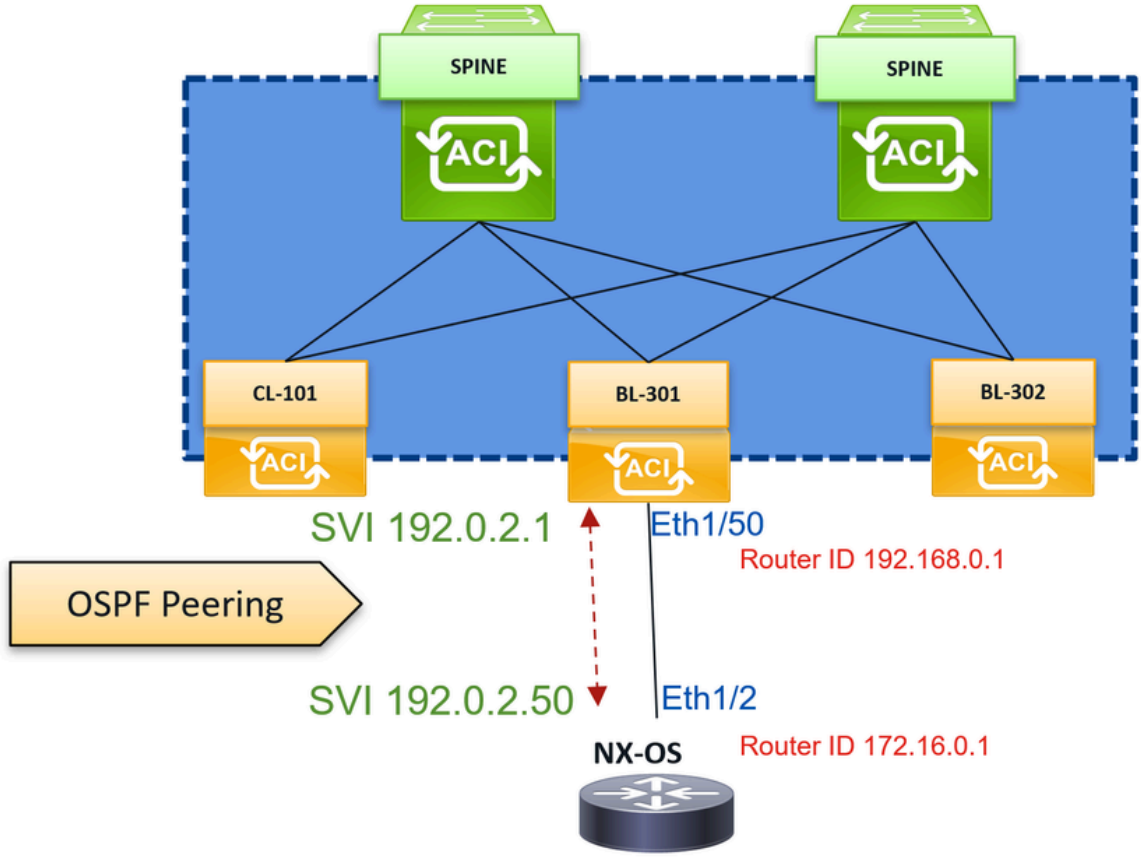
Table des matières

- Introduction
- Topologie
- Configuration requise pour l'appairage OSPF
- Dépannage de la contiguïté OSPF - Liste de contrôle générale
- Dépannage de la contiguïté OSPF - Défauts
- Capture du trafic du plan de contrôle sur le noeud
  - Vérification Wireshark
- Scénarios de dépannage
  - Dépannage de la contiguïté OSPF : incompatibilité des ID de zone
  - dépannage de la contiguïté OSPF:incompatibilité de type de zone
  - Dépannage de la contiguïté OSPF:ID de routeur dupliqué
  - Dépannage de la contiguïté OSPF:non-concordance MTU
  - dépannage de la contiguïté OSPF:non-concordance d'authentification
  - Dépannage de la contiguïté OSPF : incompatibilité des minuteurs Hello/Dead
  - dépannage de la contiguïté OSPF:incompatibilité des types d'interface
    - Diffusion
    - Point à point
- Fiche de commande de vérification
- Informations connexes

Introduction

Ce document décrit le dépannage des contiguïtés OSPF (Open Shortest Path First) de l'infrastructure axée sur les applications (ACI).

Topologie



Topologie

Configuration requise pour l'appairage OSPF

OSPF est l'un des protocoles que vous pouvez activer entre l'ACI Cisco et un routeur externe. L'ACI Cisco prend en charge toutes les options courantes, telles que la zone OSPF, y compris le réseau fédérateur, diverses options de stub, l'authentification de voisin et d'autres options similaires.

Un L3Out inclut les options de protocole de routage, la configuration spécifique au commutateur (un profil de noeud) et les paramètres spécifiques à l'interface (un profil d'interface). Les paramètres liés au protocole OSPF peuvent être configurés principalement à deux endroits, tout comme un routeur normal. La première est une configuration VRF (Virtual Routing and Forwarding) ou Node-wide, telle que l'ID de zone et le type de zone qui peuvent être configurés sur L3Out lui-même. Le deuxième est celui des paramètres de niveau interface, tels que l'intervalle Hello OSPF ou le type d'interface (diffusion, point à point (P2P)).

Voici les conditions requises pour l'établissement de la contiguïté OSPF entre le leaf de périphérie ACI et le routeur externe :

1. L'ID et le type de zone OSPF doivent correspondre
2. L'ID de routeur OSPF doit être unique
3. L'unité de transmission maximale (MTU) doit correspondre (par défaut, le fabric le définit sur 9 000 et la plupart des systèmes Cisco IOS®/NXOS le définissent sur 1 500)

4. La clé et le type d'authentification OSPF doivent correspondre (le cas échéant)
5. Les intervalles Hello et Dead OSPF doivent correspondre
6. Le type de réseau OSPF doit correspondre

Le livre blanc fournit une explication détaillée des concepts et des options de conception liés à l'ACI L3Out pour les protocoles de routage pris en charge.

Référez-vous au livre blanc si vous ne connaissez pas la configuration de L3Out ni les autres exigences de base.

Dépannage de la contiguïté OSPF - Liste de contrôle générale

Que la contiguïté OSPF ait été activée avant ou n'ait jamais été activée, il est préférable de valider d'abord les exigences de base.

Étape 1. Envoyez une requête ping à l'interface distante. Cela vous aide à confirmer si vous disposez d'une accessibilité IP à l'extrémité distante, qui est une exigence principale pour l'activation du protocole OSPF.

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

Étape 2. Validez les paramètres de configuration de base :

1. L'ID et le type de zone OSPF doivent correspondre
2. L'ID de routeur OSPF doit être unique
3. MTU doit correspondre (par défaut, le fabric le définit sur 9 000 et la plupart des systèmes Cisco IOS/NXOS le définissent sur 1 500)
4. La clé et le type d'authentification OSPF doivent correspondre (le cas échéant)
5. Les intervalles Hello et Dead OSPF doivent correspondre
6. Le type de réseau OSPF doit correspondre

Les résultats de la commande montrent les attributs de configuration poussés vers le leaf.

<#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
```

Notez tous les détails mis en surbrillance et confirmez que les paramètres d'extrémité distante correspondants sont synchronisés.

Dépannage de la contiguïté OSPF - Défauts

<#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>>

Il y a quelques scénarios sans défaut actif dans l'environnement, mais il peut y avoir un enregistrement de défaut F1385 (protocol-ospf-adjacency-down) sur le leaf qui nous indique la dernière fois que ce voisinage était actif ou s'il n'a jamais été en état complet.
Vous pouvez l'identifier à l'aide de la commandemoquery -c faultRecord -f 'fault.Inst.code=="F1385"' -x 'query-target-filter=wcard(faultRecord.dn,"abc1:vrf-1")' | grep dn.

Vérifiez le nombre d'enregistrements d'erreurs pour une date spécifique à l'aide de la commandemoquery -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.

Vous devez identifier l'interface OSPF et les adresses IP configurées localement et à distance.

<#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,"

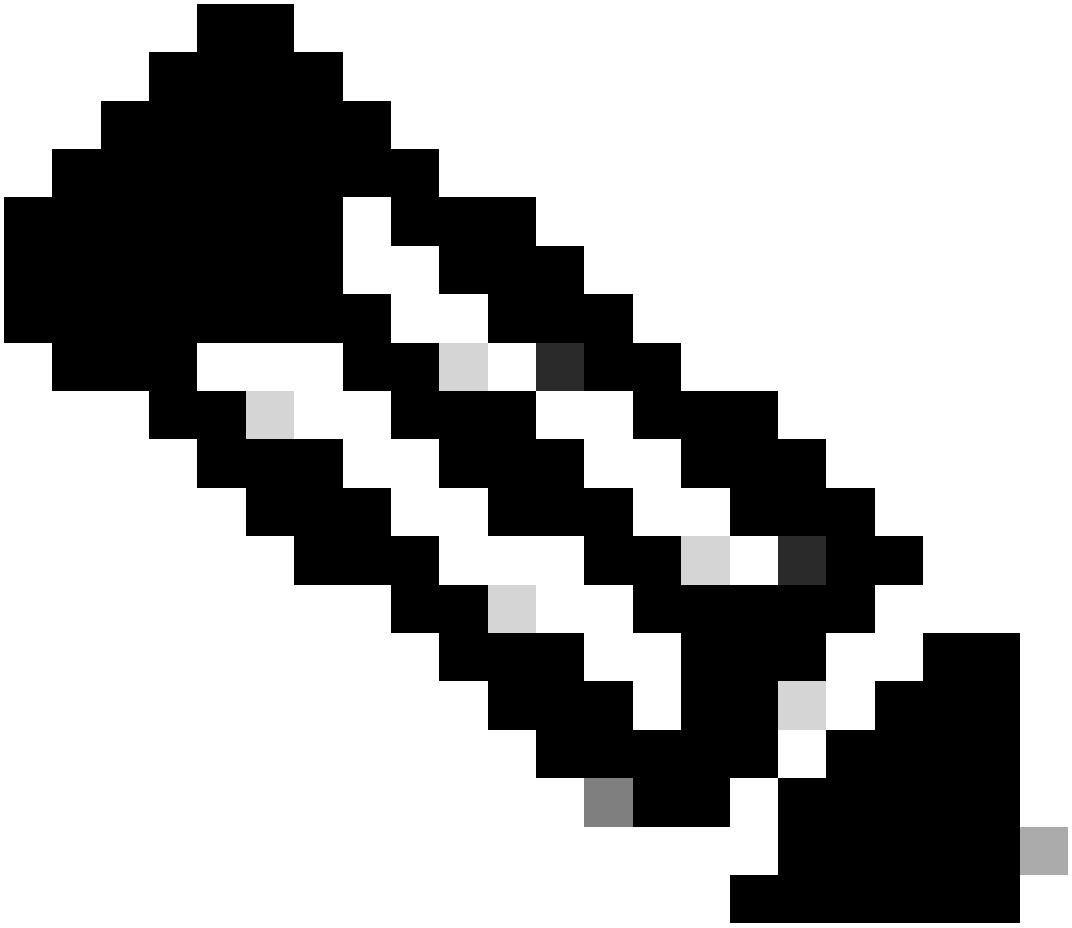
vlan1

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

192.0.2.50

Capture du trafic du plan de contrôle sur le noeud

Avec l'interface virtuelle de commutateur source et de destination (SVI) attendue à partir du leaf de bordure, vous pouvez utiliser l'utilitaire tcpdump pour vérifier.



> **Remarque** : pour cela, l'interface kpm_inb qui vous permet de voir tout le trafic réseau du plan de contrôle intrabande du processeur est utilisée.

<#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

Vérification Wireshark

Vous pouvez capturer le trafic OSPF et spécifique à l'HÔTE afin de l'analyser sur Wireshark.

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

Pour les captures pcap, vous pouvez utiliser les filtres Wireshark en recherchant et en utilisant **Analyze > Apply as a Column**.

ospf.area_id = afin d'identifier AreaID

ospf.auth.type = afin de vérifier que le type d'authentification configuré correspond

ospf.hello.hello_interval = afin de vérifier les différents MTU

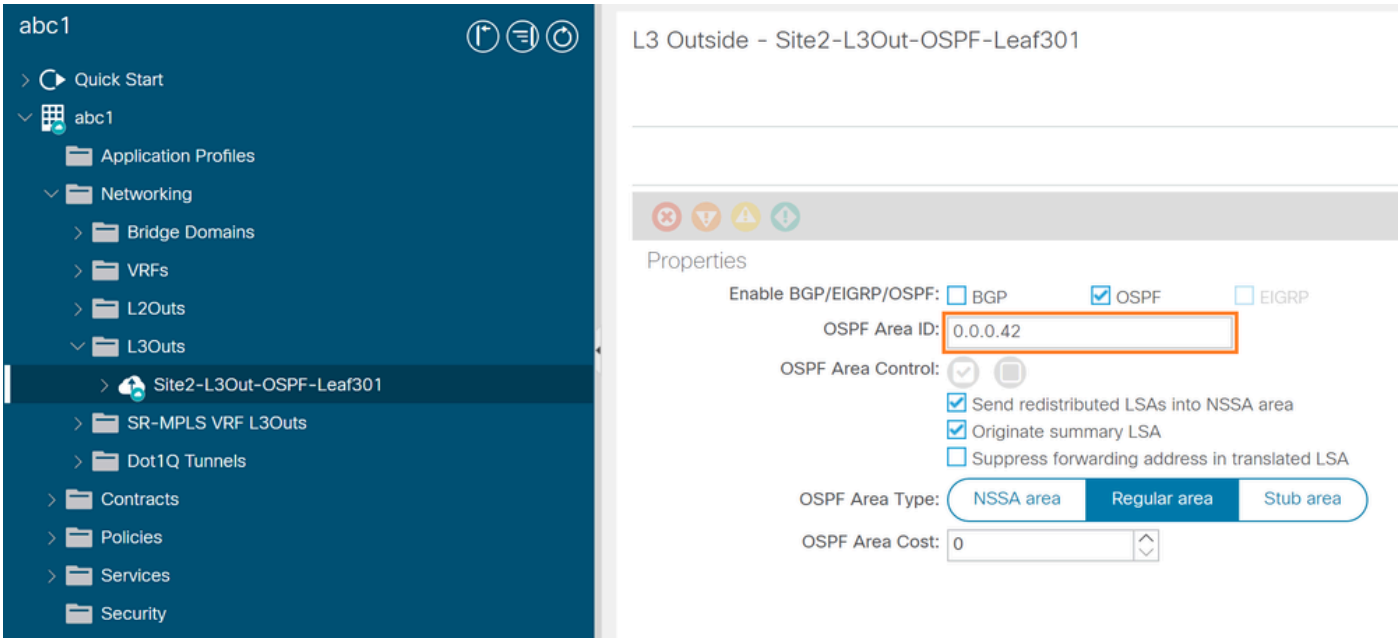
ospf.hello.router_dead_interval = afin de vérifier la présence de différentes configurations d'intervalle d'arrêt

ospf.srcrouter = IDrouteur

Scénarios de dépannage

Dépannage de la contiguïté OSPF : incompatibilité des ID de zone

Dans la configuration APIC avec l'ID de zone 0.0.0.42, accédez à **Fabric > Tenants > Networking > L3Out > <<L3outName>> > Policy > Main**.



ID de zone OSPF incorrect configuré 0.0.0.42

À partir de la feuille de bordure :

<#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
```

À partir du périphérique externe :

<#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 are

0.0.0.42

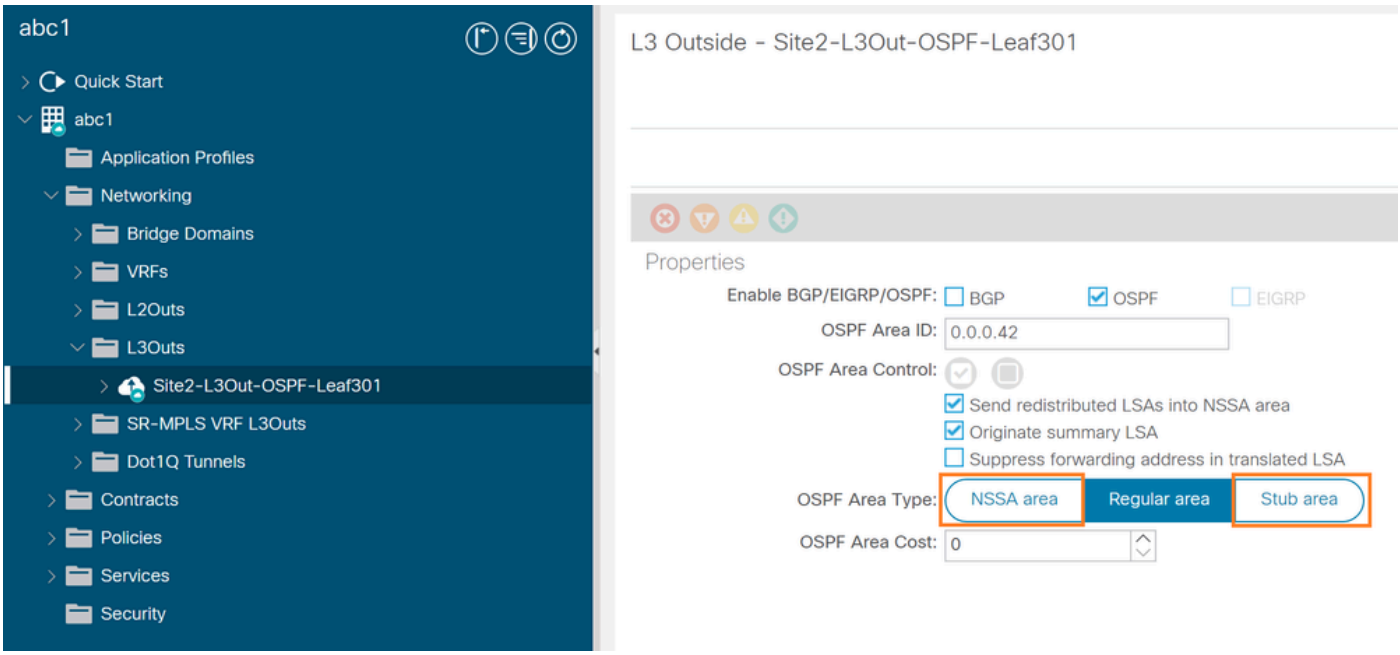
```
NX-OS# show ip ospf interface Ethernet1/2 | grep area
    Process ID bootcamp VRF 301-l3-abc1,
```

area 0.0.0.0

Solution : associez la zone OSPF à 0.0.0.0 ou backbone sur BL ou à 0.0.0.42 sur le périphérique externe.

Dépannage de la contiguïté OSPF : incompatibilité de type de zone

À partir de l'interface graphique utilisateur de l'ACI, dans la configuration avec le type de zone NSSA ou Stub, accédez à **Fabric** > **Tenants** > **Networking** > **L3Out** > **"L3outName"** > **Policy** > **Main**.



Configuration NSSA ou zone de stub.

À partir de la feuille de bordure :

```
    <#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
```

À partir du périphérique externe :

<#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,
```

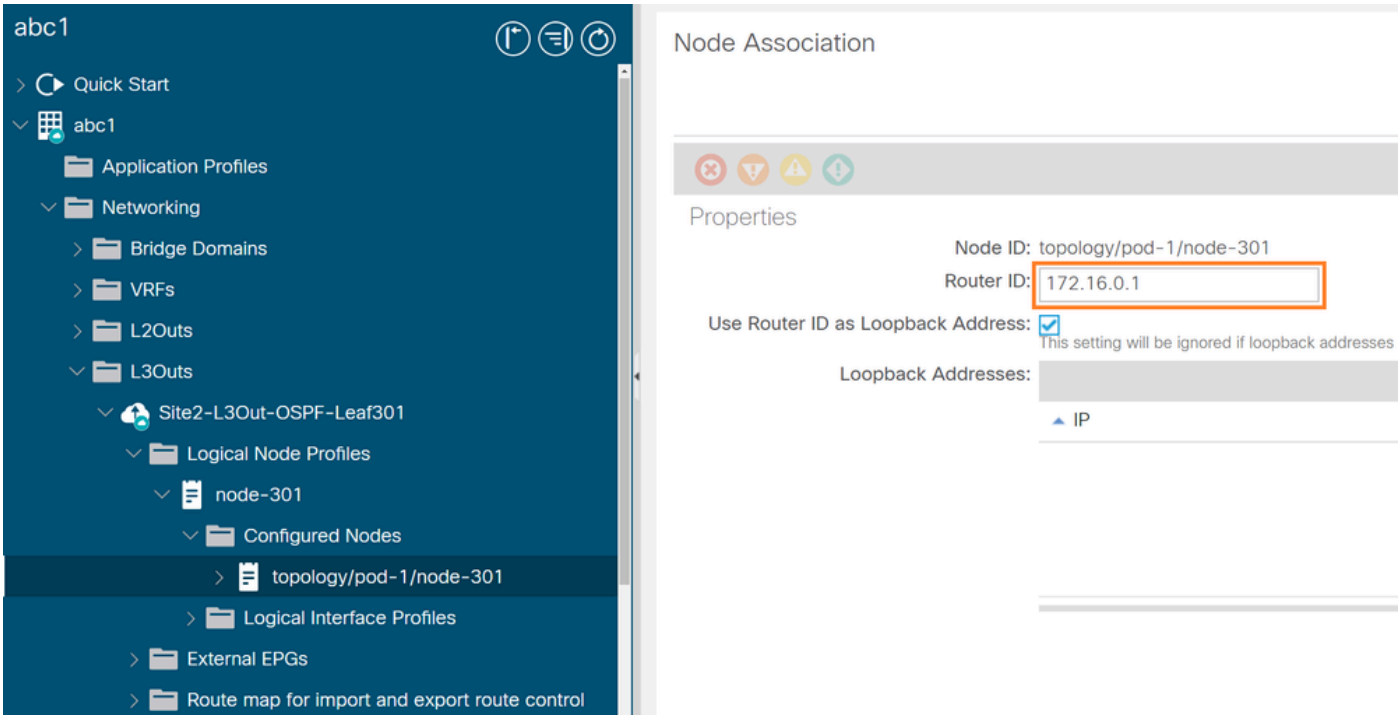
area 0.0.0.0

Solution : faites correspondre régulièrement le type de zone OSPF sur L3Out ou sur le périphérique externe.

Dépannage de la contiguïté OSPF : ID de routeur dupliqué

Un ID de routeur dupliqué empêche la formation de contiguïté OSPF. Dans le fabric ACI, après la configuration de l'ID de routeur OSPF, le leaf crée une boucle avec l'adresse IP de l'ID de routeur. Comme cette adresse est utilisée pour le bouclage, vous ne pouvez pas la faire chevaucher avec l'adresse IP de l'interface utilisée en cas d'échec.
Dans cet exemple, vous pouvez confirmer qu'il a été mal configuré avec l'ID de routeur du périphérique voisin.

Dans l'interface utilisateur graphique ACI, accédez à Fabric > Tenants > Networking > L3Outs > "L3outName" > "Node-X" > Configured Nodes > topology/pod-Y/node-X.



mal configuré avec l'ID de routeur du périphérique voisin.

À partir de la feuille de bordure :

```
    <#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

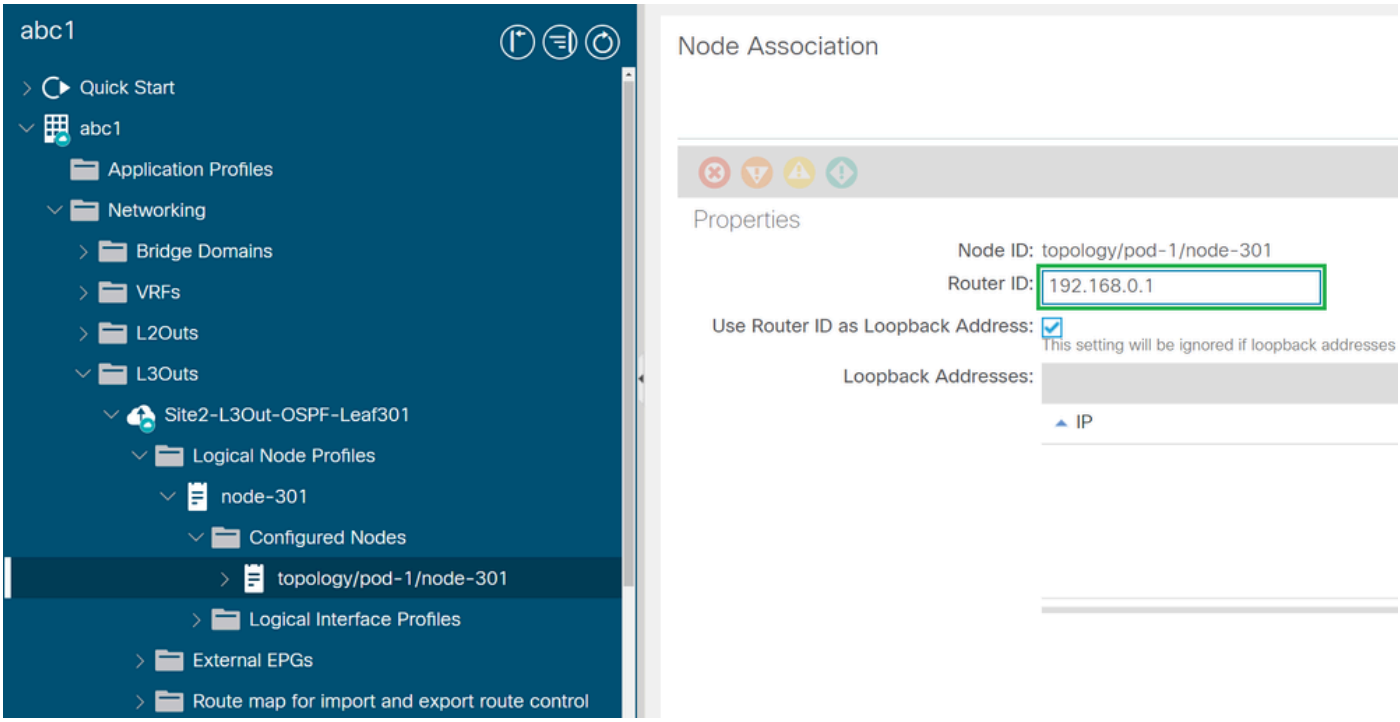
172.16.0.1

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

À partir du périphérique externe

```
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-l3-abc1) Router 192.0.2.1 on int
```

Solution : utilisez des ID de routeur différents sur les deux périphériques.



utiliser des ID de routeur différents sur les deux périphériques

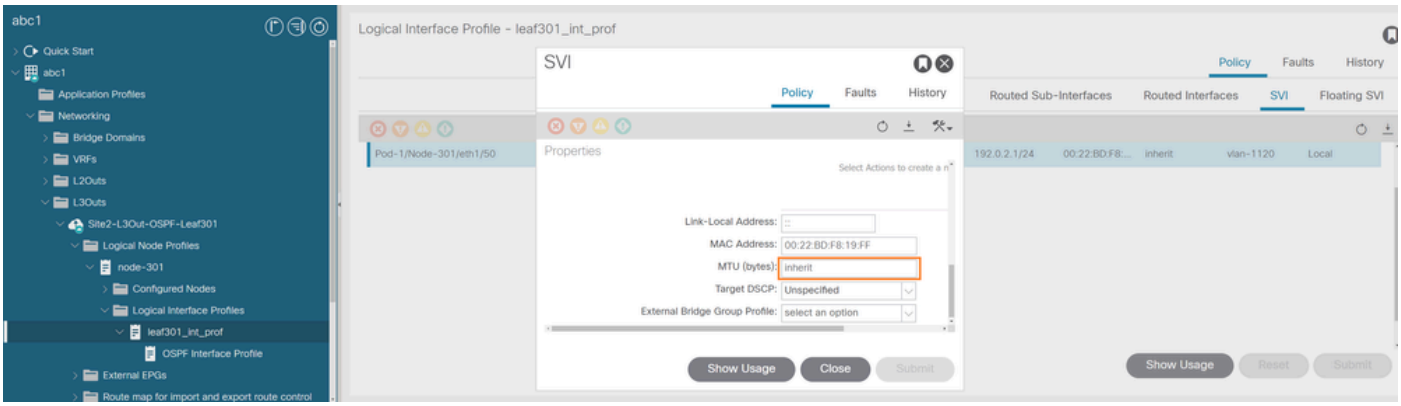
Dépannage de la contiguïté OSPF : non-concordance MTU

Une fois que deux routeurs voisins OSPF ont établi une communication bidirectionnelle et terminé la sélection DR/BDR (sur les réseaux de diffusion), les routeurs passent à l'état Exstart. Dans cet état, les routeurs voisins établissent une relation active/standby et déterminent le numéro de séquence du descripteur de base de données (DBD) initial à utiliser lors de l'échange de paquets DBD.

Une fois que la relation active/standby a été négociée (le routeur avec l'ID de routeur le plus élevé devient le routeur actif), les routeurs voisins passent à l'état d'échange. Dans cet état, les routeurs échangent des paquets DBD, qui décrivent l'intégralité de leur base de données d'état des liaisons. Les routeurs envoient également des paquets de requête d'état de liens, qui demandent des LSA (Link-State Advertisements) plus récentes aux voisins.

Si les paramètres MTU des interfaces de routeur voisines ne correspondent pas, les routeurs sont bloqués dans l'état Exstart/Exchange. En effet, le routeur dont la MTU est supérieure envoie un paquet plus grand que la MTU définie sur le routeur voisin, de sorte que ce dernier ignore le paquet.

Dans la configuration de l'interface graphique APIC avec configuration d'héritage par défaut, accédez à Fabric > Tenants > Networking > L3Outs > "L3outName" > "Node-X" > Logical Interface Profiles > OSPF Interface Profile.



Par défaut, le fabric ACI définit le MTU de l'interface de couche 3 sur 9 000 au lieu de 1 500

Par défaut, le fabric ACI définit le MTU de l'interface de couche 3 sur 9 000 au lieu de 1 500. Comme l'ACI a un MTU plus élevé, elle continue d'accepter les paquets DBD du routeur externe et tente de les accuser réception.

Si le routeur externe a un MTU inférieur ou supérieur, il ignore les paquets DBD avec ACK de l'ACI, continue à retransmettre le paquet DBD initial et reste dans l'état Exstart/Exchange.

À partir de la feuille de bordure :

<#root>

[+]From the border Leaf we can identify the state of the neighborship 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 missmatch 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 tham 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

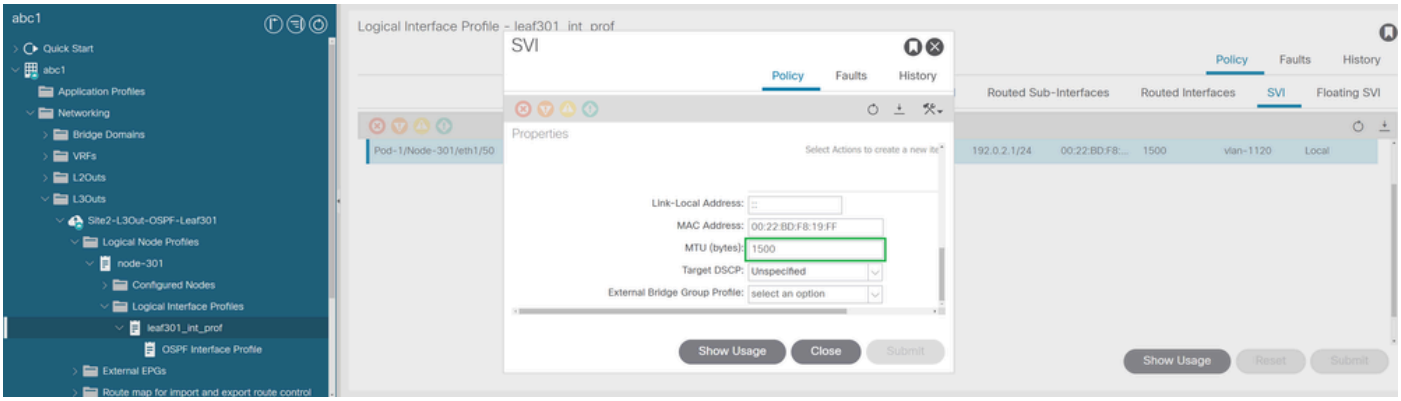
mtu [1500] is large than if mtu 1200

Solutions possibles :

- Correspondance du MTU sur les deux périphériques

Lorsqu'un MTU est modifié de part et d'autre, puisque l'appartenance est déjà établie, il le reste jusqu'à la négociation suivante et peut être déclenché pour plusieurs raisons. Par exemple, arrêt de l'interface physique, redéploiement de stratégie, rechargement de leaf, mise à niveau, etc.

Naviguez jusqu'à Fabric > Tenants > Networking > L3Outs > "L3outName" > "Node-X" > Logical Interface Profiles > OSPF Interface Profile comme indiqué dans l'image.



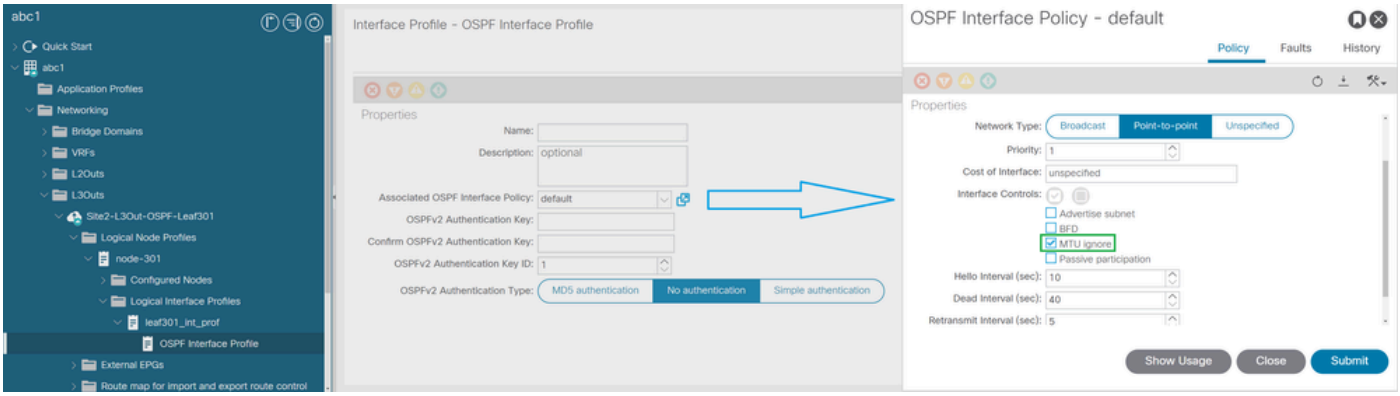
MTU configuré sur 1500

- MTU ignore dans la stratégie d'interface OSPF associée rétablit la connectivité.

Le problème avec MTU ignore peut apparaître lorsque la base de données OSPF se développe. Lorsque les MTU ne diffèrent que de quelques octets, la configuration peut fonctionner pendant longtemps jusqu'à ce que vous tombiez sur la bonne combinaison de LSA qui génèrent le DBD ou le paquet de mise à jour de la bonne taille.

Les tests effectués dans un petit laboratoire fonctionnent bien, mais le réseau de production peut rencontrer des comportements inattendus.

Naviguez jusqu'à Fabric > Tenants > Networking > L3Outs > "L3outName" > "Node-X" > Logical Interface Profiles > OSPF Interface Profile > Associated OSPF Interface Policy comme indiqué dans l'image.



MTU ignore la configuration

Dépannage de la contiguïté OSPF : non-concordance d'authentification

Vous pouvez activer l'authentification dans OSPF afin d'échanger des informations de mise à jour de routage en toute sécurité. L'authentification OSPF peut être de type « none » (ou null), « simple » ou « MD5 ». La méthode d'authentification « none » signifie qu'aucune authentification n'est utilisée pour OSPF et qu'il s'agit de la méthode par défaut. Avec une authentification simple, le mot de passe passe en texte clair sur le réseau. Avec l'authentification MD5, le mot de passe n'est pas transmis sur le réseau.

Voici les trois types d'authentifications pris en charge par OSPF.

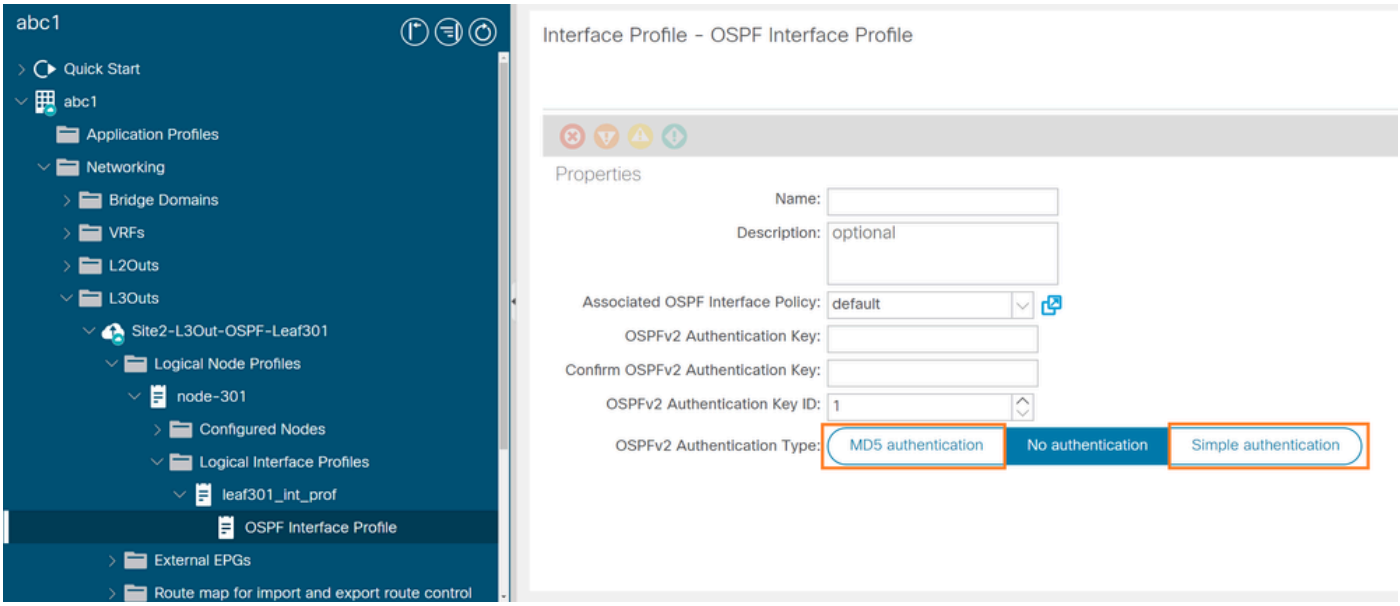
Authentification nulle : également appelée Type 0, cette authentification signifie qu'aucune information d'authentification n'est incluse dans l'en-tête de paquet. Il s'agit de la valeur par défaut.

Authentification simple : également appelée Type 1, elle utilise des mots de passe en texte clair simples.

Authentification MD5 : également appelée Type 2, cette authentification utilise des mots de passe MD5 chiffrés.

L'authentification n'a pas besoin d'être définie. Cependant, si elle est définie, tous les routeurs homologues du même segment doivent avoir le même mot de passe et la même méthode d'authentification.

À partir de l'interface utilisateur graphique de l'ACI, accédez à Fabric > Tenants > Networking > L3Outs > "L3outName" > "Node-X" > Logical Interface Profiles > OSPF Interface Profile comme indiqué dans l'image.



Authentifications MD5 ou simples configurées

À partir de CLI :

<#root>

```
[+] Check Authentication type configured
APIC# moquery -c ospfIfP -x 'query-target-filter=wcard(ospfIfP.dn,"tn-abc1\/out-Site2-L3Out-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-L3Out-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)
```

À partir du périphérique externe :

```
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-l3-abc1) Received packet from
or
2024 Jan  4 16:55:20 NX-OS %OSPF-4-AUTH_ERR:  ospf-bootcamp [22263] (301-l3-abc1) Received packet from
```

Solution : faites correspondre les authentifications.

Dépannage de la contiguïté OSPF : incompatibilité des minuteurs Hello/Dead

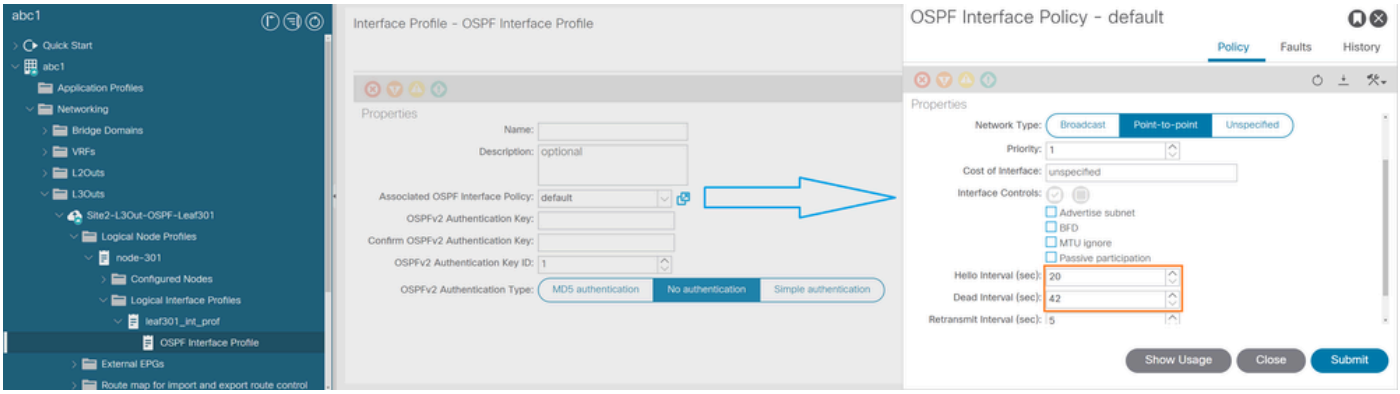
Les paquets Hello OSPF sont des paquets qu'un processus OSPF envoie à ses voisins OSPF afin de maintenir la connectivité avec ces voisins. Les paquets Hello sont envoyés à un intervalle configurable (en secondes). Les valeurs par défaut sont de 10 secondes pour une liaison Ethernet (P2P et Broadcast Network Type). Les paquets Hello incluent une liste de tous les voisins pour lesquels un paquet Hello a été reçu au cours de l'intervalle Dead. L'intervalle Dead est également configurable (en secondes) et correspond par défaut à quatre fois la valeur de l'intervalle Hello. La valeur de tous les intervalles HELLO doit être identique sur un réseau. De même, la valeur de tous les intervalles Dead doit être identique au sein d’un réseau.

Ces deux intervalles fonctionnent ensemble afin de maintenir la connectivité en indiquant que la liaison est opérationnelle. Si un routeur ne reçoit pas de paquet Hello d’un voisin au cours de l’intervalle Dead, il déclare ce voisin comme inactif.

Si les minuteurs Hello et Dead OSPF par défaut sont modifiés sur le fabric ACI, ils doivent correspondre au routeur externe.

À partir de l'interface utilisateur graphique de l'ACI, accédez à Fabric > Tenants > Networking > L3Outs > "L3outName" > "Node-X" > Logical

Interface Profiles > OSPF Interface Profile > Associated OSPF Interface Policy comme indiqué dans l'image.



Minuteurs Hello/Dead personnalisés

À partir de la feuille de bordure :

<#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|helloInt
```

deadIntvl   : 42

helloIntvl   : 20

nwT   : p2p

Or

```
APIC# moquery -c ospfRsIfPol -x 'query-target-filter=wcard(ospfIfP.dn,"abc1\/out-Site2-L3Out-OSPF-BL-30
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

À partir du périphérique externe :

<#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

40

, Wait 40, Retransmit 5

Solution : faites correspondre les minuteurs OSPF.

Dépannage de la contiguïté OSPF : incompatibilité des types d'interface

Cette section décrit le dépannage lorsque la diffusion ou non spécifiée est configurée sur l'ACI et que le périphérique externe est P2P.

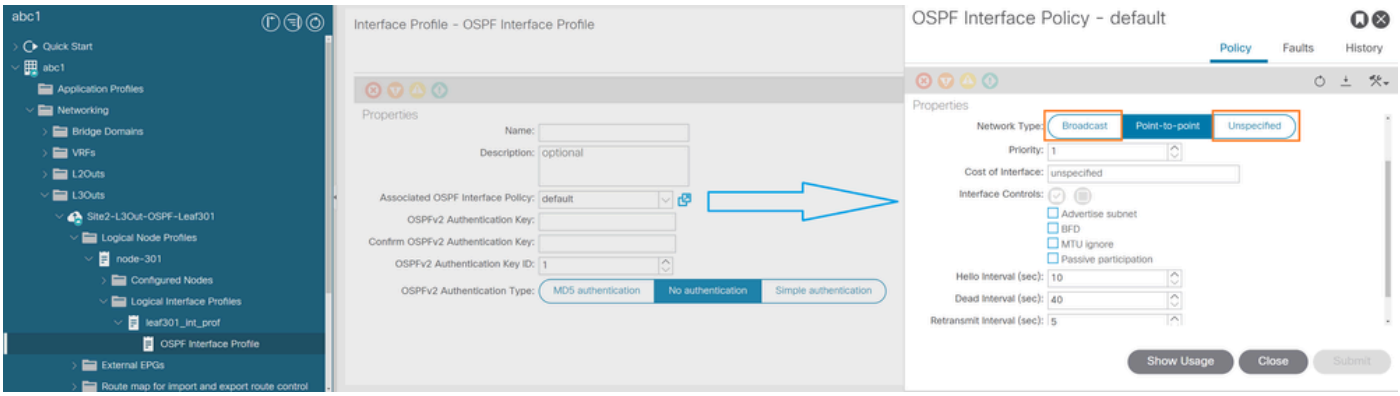
Diffusion

- Le type de réseau de diffusion est le type par défaut pour une interface Ethernet compatible OSPF
- Le type de réseau de diffusion nécessite qu'une liaison prenne en charge les fonctionnalités de diffusion de couche 2
- Le type de réseau de diffusion dispose d'un Hello de 10 secondes et d'un minuteur d'arrêt de 40 secondes (identique à P2P)
- Un type de réseau de diffusion OSPF nécessite l'utilisation d'un DR/BDR.

Point à point

- Un type de réseau OSPF P2P ne gère pas de relation DR/BDR
- Le type de réseau P2P dispose d'un minuteur Hello de 10 secondes et d'un minuteur d'arrêt de 40 secondes
- Les types de réseau P2P sont destinés à être utilisés entre deux routeurs connectés directement

À partir de l'interface utilisateur graphique de l'ACI, accédez à Fabric > Tenants > Networking > L3Outs > "L3outName" > "Node-X" > Logical Interface Profiles > OSPF Interface Profile > Associated OSPF Interface Policy comme indiqué dans l'image.



Type de diffusion ou de réseau non spécifié configuré

À partir de la feuille de bordure :

```
    <#root>


[+] Check OSPF neighborship 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|helloInt
deadIntvl     : 40
helloIntvl    : 10
nwT           :


bcast



or

BL-301# moquery -c ospfIf -x 'query-target-filter=wcard(ospfIf.id,"vlan1")' | egrep "deadIntvl|helloInt
deadIntvl     : 40
```

```
helloIntvl   : 10
nwT          :
```

unspecified

Or

```
APIC# moquery -c ospfRsIfPol -x 'query-target-filter=wcard(ospfIfP.dn,"abc1\/out-Site2-L3Out-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
```

À partir du périphérique externe :

```
    <#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
```

Fiche de commande de vérification

Ces commandes ont été référencées tout au long de ce document afin de dépanner les différents scénarios.

Noeud	Commandes	Objectif
Commutateur ACI	show ip ospf neighbors vrf <<TNT:VRF>>	Vérifier la relation de voisinage sur VRF
	show ip ospf interface brief vrf <<TNT:VRF>>	Vérifier les interfaces OSPF associées au VRF
	moquery -c faultInst -x 'query-target-filter=wcard(faultInst.dn,"<<TNT:VRF>>")'	Vous pouvez vérifier les défaillances associées au VRF
	moquery -c ospfIf -x 'query-target-filter=wcard(ospfIf.dn,"<<TNT:VRF>>")'	Vérifiez tous les détails de l'interface OSPF associée au VRF

	moquery -c ospfIf -x 'query-target-filter=wcard(ospfIf.id,"<<vlanX>>")'	Vérifier la configuration de l'interface OSPF
	moquery -c arpAdjEp -x 'query-target-filter=wcard(arpAdjEp.ifId,"<<vlanX>>")' | grep ip	Vérifiez l'adresse IP appliquée sur le périphérique externe à partir du protocole ARP associé à l'interface
	log_trace_bl_print_tool /var/sysmgr/tmp_logs/ospfv2_1_trace.bl | tail -n 250 | grep <<TNT:VRF>>	Décodage de trace OSPF en direct pour VRF
	tcpdump -i kpm_inb proto ospf -vv -e -w - | tee /data/techsupport/Node-XXX_OSPF.pcap | tcpdump -r - host any	Capturer le trafic OSPF à analyser sur Wireshark
	tcpdump -i kpm_inb proto ospf -vv -e -w - | tee /data/techsupport/Node-XXX_OSPF_HOST.pcap | tcpdump -r - host <<X.X.X.X>>	Capturer le trafic spécifique de HOST afin d'analyser sur Wireshark
	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	Capturer le trafic spécifique à SRC et DST de HOST afin d'analyser sur Wireshark
	tcpdump src host <<X.X.X.X>> -vv -e -i kpm_inb -c 1	Capturer un seul plan de contrôle intrabande pour un hôte spécifique
ACI APIC	moquery -c ospfIfP -x 'query-target-filter=wcard(ospfIfP.dn,"<<TNT>>\/out-<<L3outName>>")'	Vérifiez le type d'authentification configuré
	moquery -c l3ext.RsPathL3OutAtt -x 'query-target-filter=wcard(l3extRsPathL3OutAtt.dn,"<<TNT>>\/out-<<L3outName>>")'	Vérifier la configuration du chemin L3out
	moquery -c faultRecord -f 'fault.Inst.code=="F1385"' -x 'query-target-filter=wcard(faultRecord.dn,"<<TNT:VRF>>")'	Vérifiez les enregistrements historiques de panne pour le

		protocole F1385 protocol-ospf-adjacency-down
	moquery -c ospfRsIfPol -x 'query-target-filter=wcard(ospfIfP.dn,"<<TNT>>\/out-<<L3outName>>")' | grep tnOspfIfPolName	Recherchez la politique d'interface OSPF associée personnalisée dans L3out
	moquery -c ospfIfPol -x 'query-target-filter=wcard(ospfIfPol.name,"Custom_OSPF_Interface_Policy")'	Vérifiez les détails de la stratégie d'interface OSPF associée personnalisée
Commutateur NXOS	show ip int bri vrf <<VRF>>	Vérifier les interfaces OSPF avec vrf
	show run ospf all | section EthernetX/Y	Vérifier la configuration OSPF
	show ip ospf interface EthernetX/Y	Vérifier les paramètres annoncés de l'interface OSPF

Informations connexes

- Dépannage du transfert externe ACI
- Assistance technique de Cisco et téléchargements

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.