

Risoluzione dei problemi relativi alle adiacenze ACI OSPF

Sommario

[Introduzione](#)

[Topologia](#)

[Requisiti di configurazione peer OSPF](#)

[Risoluzione dei problemi relativi all'adiacenza OSPF - Elenco di controllo generale](#)

[Risoluzione dei problemi relativi all'adiacenza OSPF - Errori](#)

[Acquisizione del traffico del Control Plane sul nodo](#)

[Verifica Wireshark](#)

[Risoluzione dei problemi](#)

[Risoluzione dei problemi relativi all'adiacenza OSPF: mancata corrispondenza dell'ID area](#)

[Risoluzione dei problemi relativi all'adiacenza OSPF: mancata corrispondenza del tipo di area](#)

[Risoluzione dei problemi adiacenza OSPF: ID router duplicato](#)

[Risoluzione dei problemi relativi all'adiacenza OSPF: MTU non corrispondente](#)

[Risoluzione dei problemi adiacenza OSPF: mancata corrispondenza autenticazione](#)

[Risoluzione dei problemi relativi all'adiacenza OSPF: mancata corrispondenza tra Hello/Dead Timers](#)

[Risoluzione dei problemi adiacenza OSPF: tipo di interfaccia non corrispondente](#)

[Trasmissione](#)

[Point-to-point](#)

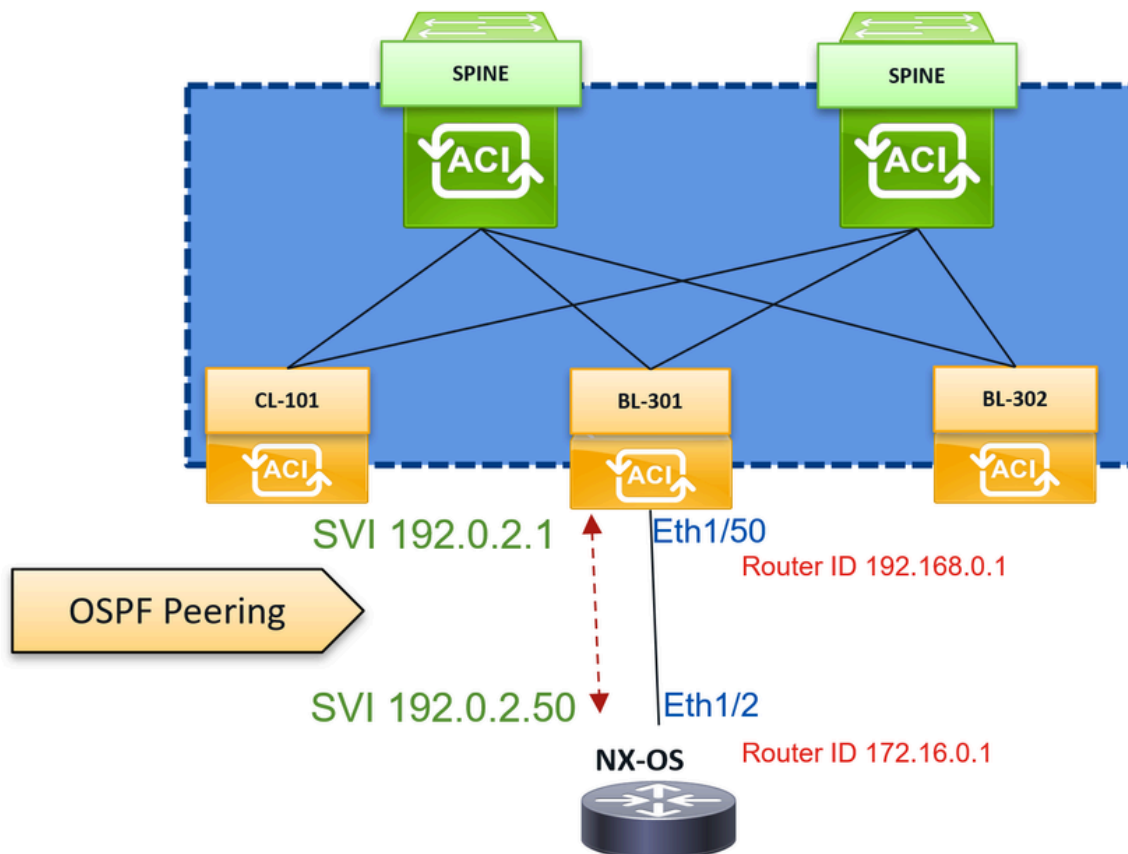
[Scheda grafica del comando di verifica](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritto come risolvere i problemi relativi alle adiacenze ACI (Application Centric Infrastructure) e OSPF (Open Shortest Path First).

Topologia



Topologia

Requisiti di configurazione peer OSPF

OSPF è uno dei protocolli che è possibile abilitare tra Cisco ACI e un router esterno. Cisco ACI supporta tutte le opzioni comuni, ad esempio l'area OSPF, inclusa la backbone, varie opzioni stub, l'autenticazione dei router adiacenti e altre opzioni simili.

L3Out include le opzioni del protocollo di routing, la configurazione specifica dello switch (un profilo di nodo) e le impostazioni specifiche dell'interfaccia (un profilo di interfaccia). I parametri relativi al protocollo OSPF possono essere configurati principalmente in due posizioni, come se si trattasse di un router normale. La prima è la configurazione a livello di VRF (Virtual Routing and Forwarding) o di nodo, ad esempio l'ID dell'area e il tipo di area, che può essere configurata nello stesso L3Out. Il secondo è costituito da parametri a livello di interfaccia, ad esempio Intervallo hello OSPF o tipo di interfaccia (Broadcast, Point-to-Point(P2P)).

Di seguito sono riportati i requisiti per stabilire l'adiacenza OSPF tra la foglia di confine ACI e il router esterno:

1. L'ID e il tipo dell'area OSPF devono corrispondere
2. L'ID del router OSPF deve essere univoco
3. La MTU (Maximum Transmission Unit) deve corrispondere (per impostazione predefinita, la struttura la imposta su 9000 e la maggior parte dei Cisco IOS®/NXOS su 1500)
4. Il tipo e la chiave di autenticazione OSPF devono corrispondere (se utilizzata)

5. Gli intervalli Hello e Dead di OSPF devono corrispondere
6. Il tipo di rete OSPF deve corrispondere

Il [white paper](#) ha fornito una spiegazione dettagliata dei concetti e delle opzioni di progettazione relativi all'ACI L3Out per i protocolli di routing di supporto.

Fare riferimento al white paper se non si ha familiarità con l'impostazione L3Out e con altri requisiti di base.

Risoluzione dei problemi relativi all'adiacenza OSPF - Elenco di controllo generale

Indipendentemente dal fatto che l'adiacenza OSPF sia stata rilevata in precedenza o non sia mai stata rilevata, è consigliabile convalidare prima i requisiti di base.

Passaggio 1. Eseguire il ping dell'interfaccia dell'estremità remota. Ciò consente di verificare se si dispone di raggiungibilità IP all'estremità remota, che è un requisito principale per l'arrivo di OSPF.

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

Passaggio 2. Convalidare i parametri di configurazione di base:

1. L'ID e il tipo dell'area OSPF devono corrispondere
2. L'ID del router OSPF deve essere univoco
3. L'MTU deve corrispondere (per impostazione predefinita, l'MTU viene impostata su 9000 e la maggior parte dei Cisco IOS/NXOS su 1500)
4. Il tipo e la chiave di autenticazione OSPF devono corrispondere (se utilizzata)
5. Gli intervalli Hello e Dead di OSPF devono corrispondere
6. Il tipo di rete OSPF deve corrispondere

Gli output del comando mostrano gli attributi di configurazione sottoposti a push nella foglia.

<#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

Prendere nota di tutti i dettagli evidenziati e verificare che i corrispondenti parametri dell'estremità remota siano sincronizzati.

Risoluzione dei problemi relativi all'adiacenza OSPF - Errori

<#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>>

Ci sono alcuni scenari senza errori attivi nell'ambiente, ma può esserci un errore Record F1385 (protocollo-ospf-adiacenza-giù) sulla foglia che ci indica l'ultima volta che questo quartiere è stato attivo o se non è mai stato in pieno stato.

È possibile identificare questa condizione con il comando `moquery -c faultRecord -f 'fault.Inst.code=="F1385"' -x 'query-target-filter=wcard(faultRecord.dn,"abc1:vrf-1")' | grep dn`.

Controllare il numero di record di errore per una data specifica con il comando `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` comando.

È necessario identificare l'interfaccia OSPF e gli IP configurati in locale e in remoto.

<#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

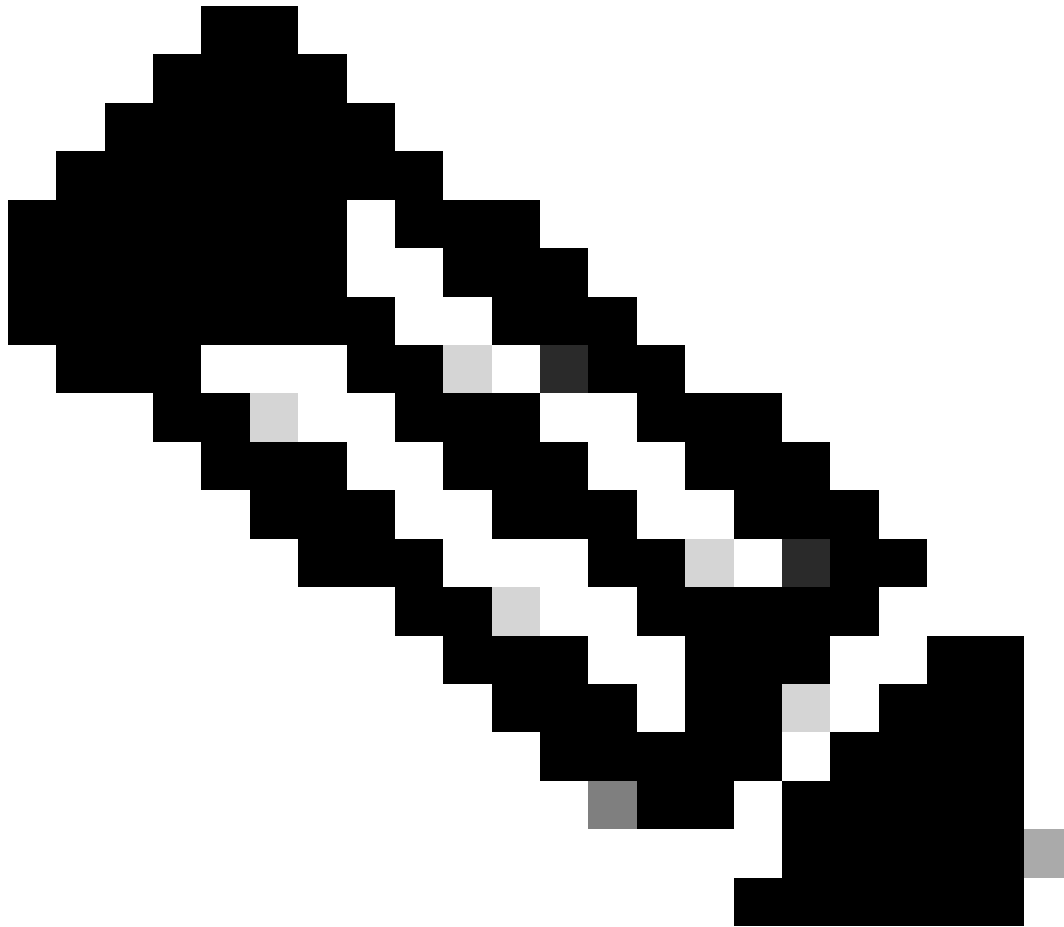
")' | grep "ip "
ip :

192.0.2.50

Acquisizione del traffico del Control Plane sul nodo

Usando l'interfaccia virtuale dello switch di origine e destinazione (SVI) prevista dalla foglia del bordo, è possibile usare l'utility tcpdump per

controllare.



Nota: per questa operazione viene utilizzata l'interfaccia kpm_inb che consente di visualizzare tutto il traffico di rete del control plane in banda della CPU.

<#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

Verifica Wireshark

È possibile acquisire il traffico OSPF e quello specifico dell'HOST per analizzarlo su 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
```

Per le acquisizioni pcap, potete utilizzare i filtri Wireshark eseguendo una ricerca e selezionando **Analizza (Analyze) > Applica come colonna (Apply as a Column)**.

ospf.area_id = per identificare AreaID

ospf.auth.type = per verificare che il tipo di autenticazione configurato corrisponda

ospf.hello.hello_interval = per verificare la presenza di MTU diverse

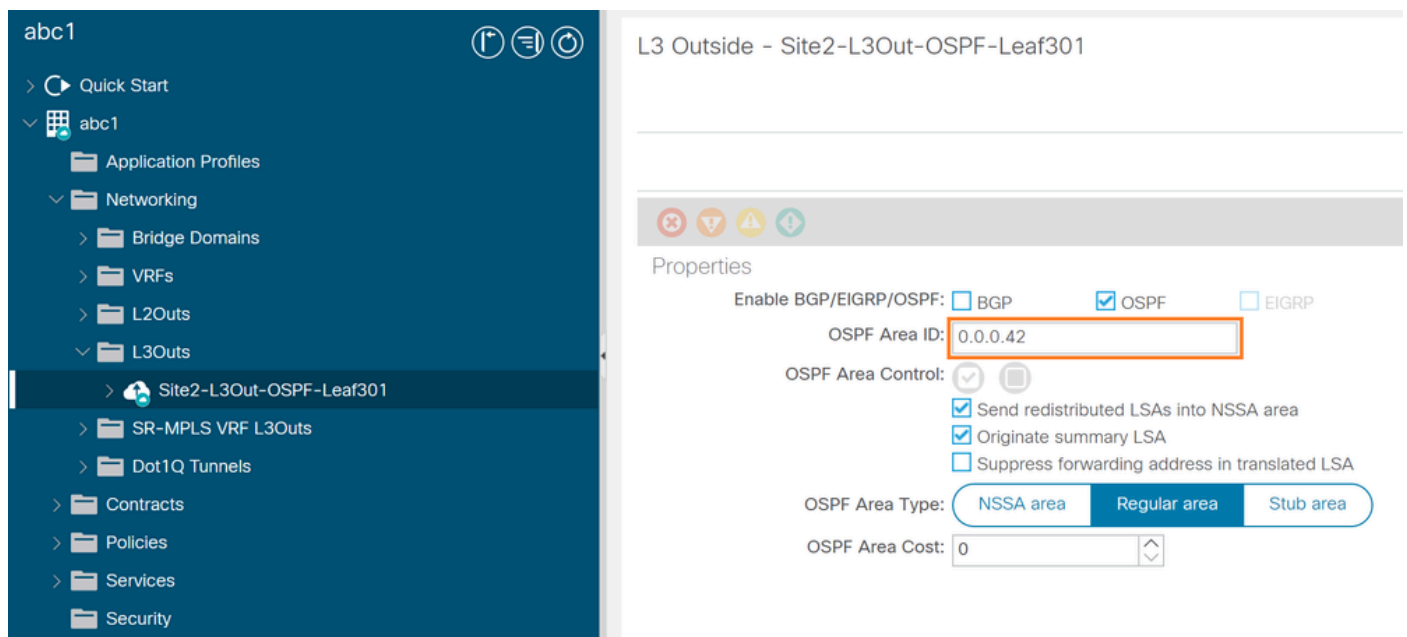
ospf.hello.router_dead_interval = per controllare la configurazione di un intervallo inattivo diverso

ospf.srcrouter = ID router

Risoluzione dei problemi

Risoluzione dei problemi relativi all'adiacenza OSPF: mancata corrispondenza dell'ID area

Dalla configurazione APIC con ID area 0.0.0.42, selezionare **Fabric > Tenant > Networking > L3Outs > <<L3outName>> > Policy > Main** (Infrastruttura > Tenant > Rete > L3Outs > <<L3outName>> Criteri > Principale).



ID area OSPF errato configurato 0.0.0.42

Dalla foglia di confine:

<#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
```

Dalla periferica esterna:

<#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

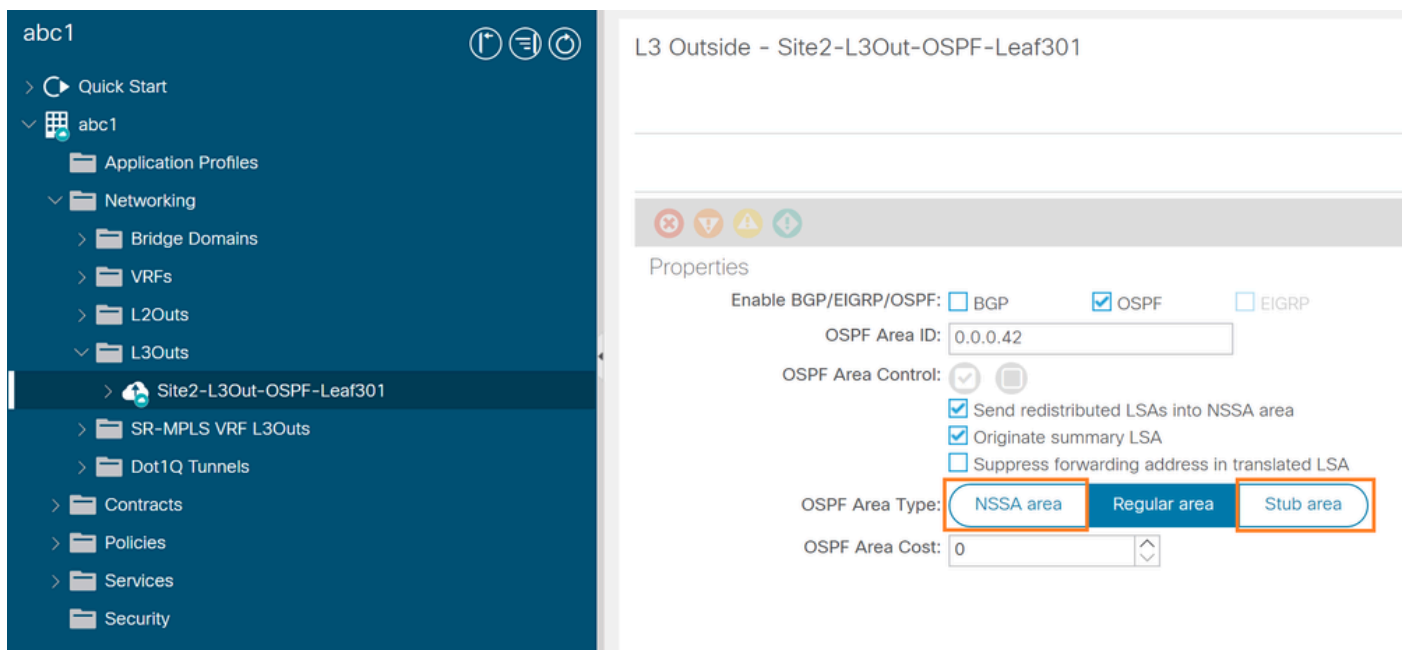
```
NX-OS# show ip ospf interface Ethernet1/2 | grep area
Process ID bootcamp VRF 301-l3-abc1,
```

area 0.0.0.0

Soluzione: associare l'area OSPF a 0.0.0.0 o alla backbone su BL o 0.0.0.42 sul dispositivo esterno.

Risoluzione dei problemi relativi all'adiacenza OSPF: mancata corrispondenza del tipo di area

Dalla GUI ACI, configurare con il tipo Area NSSA o Stub, selezionare **Fabric > Tenants > Networking > L3Outs > "L3outName" > Policy > Main** (Policy > Principale).



Configurazione NSSA o area stub.

Dalla foglia di confine:

```
<#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
```

Dalla periferica esterna:

<#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

Soluzione: verificare che il tipo di area OSPF corrisponda a intervalli regolari su L3Out o che corrisponda su dal dispositivo esterno.

Risoluzione dei problemi relativi all'adiacenza OSPF: ID router duplicato

Un ID di router duplicato impedisce la formazione dell'adiacenza OSPF. Nell'infrastruttura ACI, dopo aver configurato l'ID router OSPF, la foglia crea un loopback con l'indirizzo IP dell'ID router. Poiché questo indirizzo viene utilizzato per il loopback, non è possibile sovrapporlo all'IP dell'interfaccia utilizzato in caso di errore.

Nell'esempio, è possibile verificare che non sia stato configurato correttamente con l'ID del router del dispositivo adiacente.

Dalla GUI ACI, selezionare Fabric > Tenants > Networking > L3Outs > "L3outName" > "Node-X" > Configured Nodes > topology/pod-Y/node-X.

The screenshot displays the ACI GUI configuration for a Node Association. On the left, the navigation pane shows the hierarchy: Fabric > Tenants > Networking > L3Outs > Site2-L3Out-OSPF-Leaf301 > Logical Node Profiles > node-301 > Configured Nodes > topology/pod-1/node-301. The main configuration area is titled 'Node Association' and shows the following details:

- Node ID:** topology/pod-1/node-301
- Router ID:** 172.16.0.1 (highlighted with an orange box)
- Use Router ID as Loopback Address:** ☒ (with a note: 'This setting will be ignored if loopback addresses')
- Loopback Addresses:** A section with a plus icon and the label 'IP', currently empty.

configurazione errata con l'ID router del dispositivo adiacente.

Dalla foglia di confine:

<#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
```

Da periferica esterna

```
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
```

Soluzione: utilizzare ID router diversi su entrambi i dispositivi.

The screenshot displays the Cisco NX-OS configuration interface. On the left, a 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 main panel is titled **Node Association** and contains a **Properties** section. In the **Properties** section, the **Router ID** is set to **192.168.0.1**, which is highlighted with a green box. Below this, the checkbox **Use Router ID as Loopback Address** is checked, with a note: "This setting will be ignored if loopback addresses". The **Loopback Addresses** section is currently empty, with an **IP** button visible.

usa ID router diversi su entrambi i dispositivi

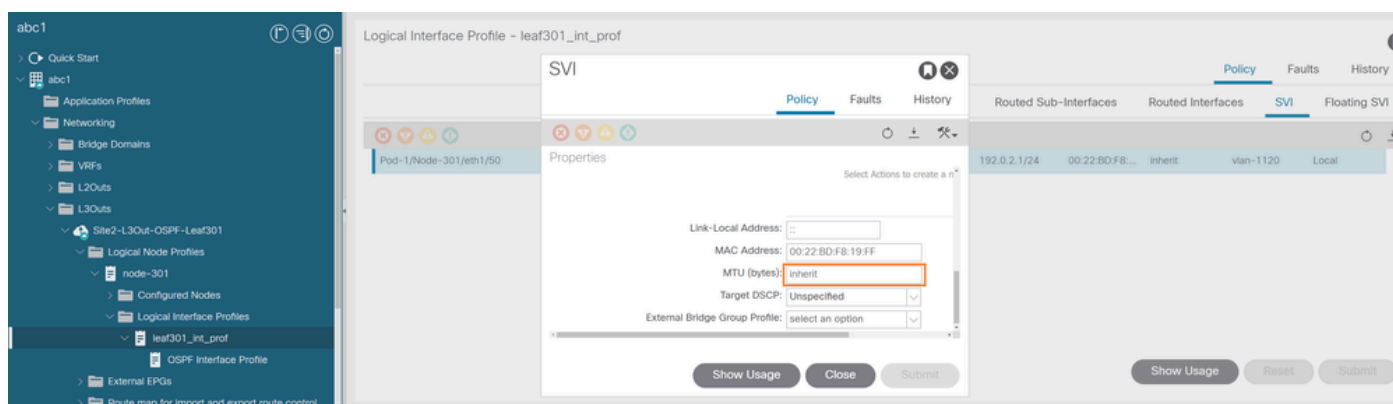
Risoluzione dei problemi relativi all'adiacenza OSPF: MTU non corrispondente

Dopo che due router adiacenti OSPF hanno stabilito la comunicazione bidirezionale e completato l'elezione di un router designato (DR) o di un BDR (su reti broadcast), i router passano allo stato Exstart. In questo stato, i router adiacenti stabiliscono una relazione attiva/standby e determinano il numero di sequenza del descrittore di database iniziale (DBD) da utilizzare nello scambio di pacchetti DBD.

Dopo aver negoziato la relazione attivo/standby (il router con l'ID più alto diventa il router attivo), i router adiacenti passano allo stato di scambio. In questo stato, i router si scambiano i pacchetti DBD che descrivono l'intero database dello stato del collegamento. I router inviano anche pacchetti di richieste allo stato del collegamento, che richiedono annunci allo stato del collegamento (LSA) più recenti dai router adiacenti.

Se le impostazioni MTU delle interfacce dei router adiacenti non corrispondono, i router sono bloccati nello stato Exstart/Exchange. Infatti, il router con l'MTU più alta invia un pacchetto più grande dell'MTU impostata sul router adiacente, in modo che quest'ultimo ignori il pacchetto.

Dalla configurazione GUI APIC con la configurazione di ereditarietà predefinita, passare a Fabric > Tenants > Networking > L3Outs > "L3outName" > "Node-X" > Logical Interface Profiles > OSPF Interface Profile.



Per impostazione predefinita, ACI fabric imposta l'MTU dell'interfaccia di layer 3 su 9000 anziché su 1500

Per impostazione predefinita, l'MTU dell'interfaccia di layer 3 viene impostata su 9000 anziché su 1500. Poiché l'ACI ha una MTU più alta, continua ad accettare i pacchetti DBD dal router esterno e cerca di confermarli.

Se l'MTU del router esterno è inferiore o superiore, i pacchetti DBD vengono ignorati insieme all'ACK inviato dall'ACI, il router continua a trasmettere il pacchetto DBD iniziale e rimane nello stato Exstart/Exchange.

Dalla foglia di confine:

<#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

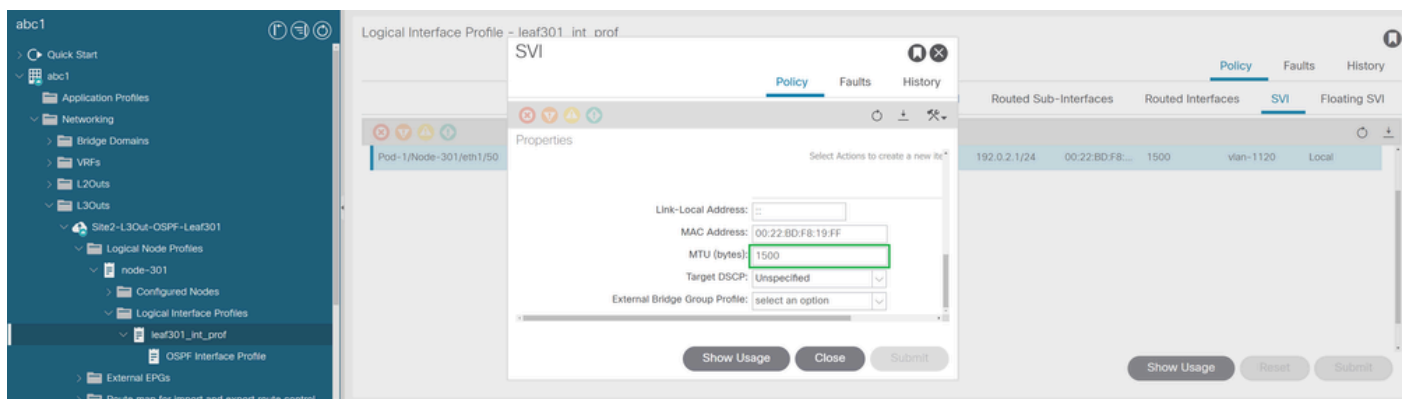
mtu [1500] is large than if mtu 1200

Soluzioni possibili:

- Trova la corrispondenza con l'MTU su entrambi i dispositivi

Quando un'MTU viene modificata su entrambi i lati, poiché l'appartenenza è già stabilita, rimane tale fino alla negoziazione successiva e può essere attivata per diversi motivi. ad esempio l'interfaccia fisica inattiva, la redistribuzione delle policy, il ricaricamento delle foglie, l'aggiornamento e così via.

Passare a Fabric > Tenants > Networking > L3Outs > "L3outName" > "Node-X" > Logical Interface Profiles > OSPF Interface Profile come mostrato nell'immagine.



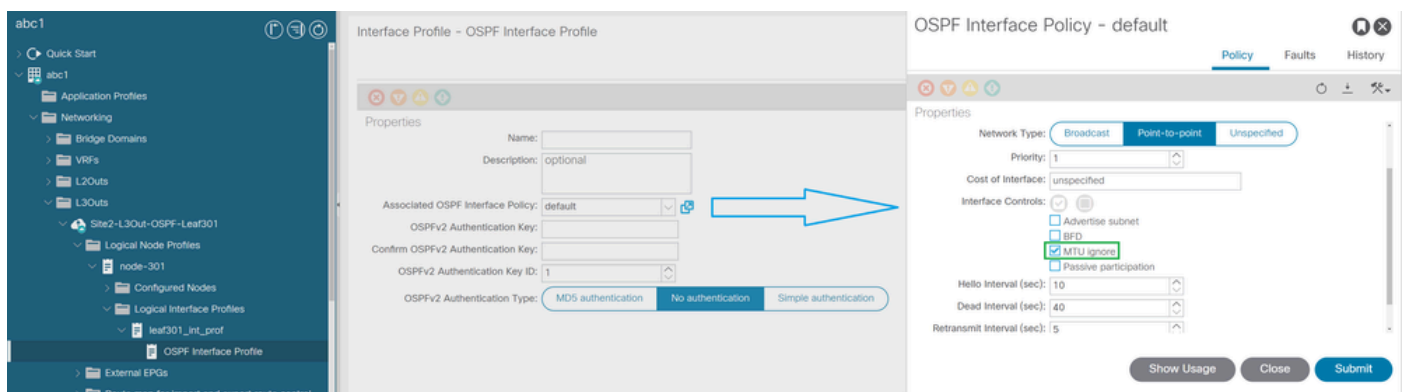
MTU configurata su 1500

- L'MTU ignorata nel criterio dell'interfaccia OSPF associata ristabilisce la connettività.

Il problema con MTU ignorata può apparire quando il database OSPF cresce. Quando le MTU differiscono solo di alcuni byte, la configurazione può funzionare per molto tempo finché non ci si imbatte nella combinazione corretta di LSA che generano il DBD o aggiornano il pacchetto solo delle dimensioni corrette.

I test in un piccolo laboratorio funzionano bene, ma la rete di produzione può incontrare comportamenti imprevisti.

Passare a Fabric > Tenants > Networking > L3Outs > "L3outName" > "Node-X" > Logical Interface Profiles > OSPF Interface Profile > Associated OSPF Interface Policy come mostrato nell'immagine.



MTU che ignora la configurazione

Risoluzione dei problemi relativi all'adiacenza OSPF: mancata corrispondenza dell'autenticazione

È possibile abilitare l'autenticazione in OSPF per scambiare in modo sicuro le informazioni di aggiornamento del routing. L'autenticazione OSPF può essere none (o null), simple o MD5. Il metodo di autenticazione 'none' indica che non viene utilizzata alcuna autenticazione per OSPF ed è il metodo predefinito. Con l'autenticazione semplice, la password passa in testo non crittografato attraverso la rete. Con l'autenticazione MD5, la password non passa attraverso la rete.

Si tratta dei tre diversi tipi di autenticazione supportati da OSPF.

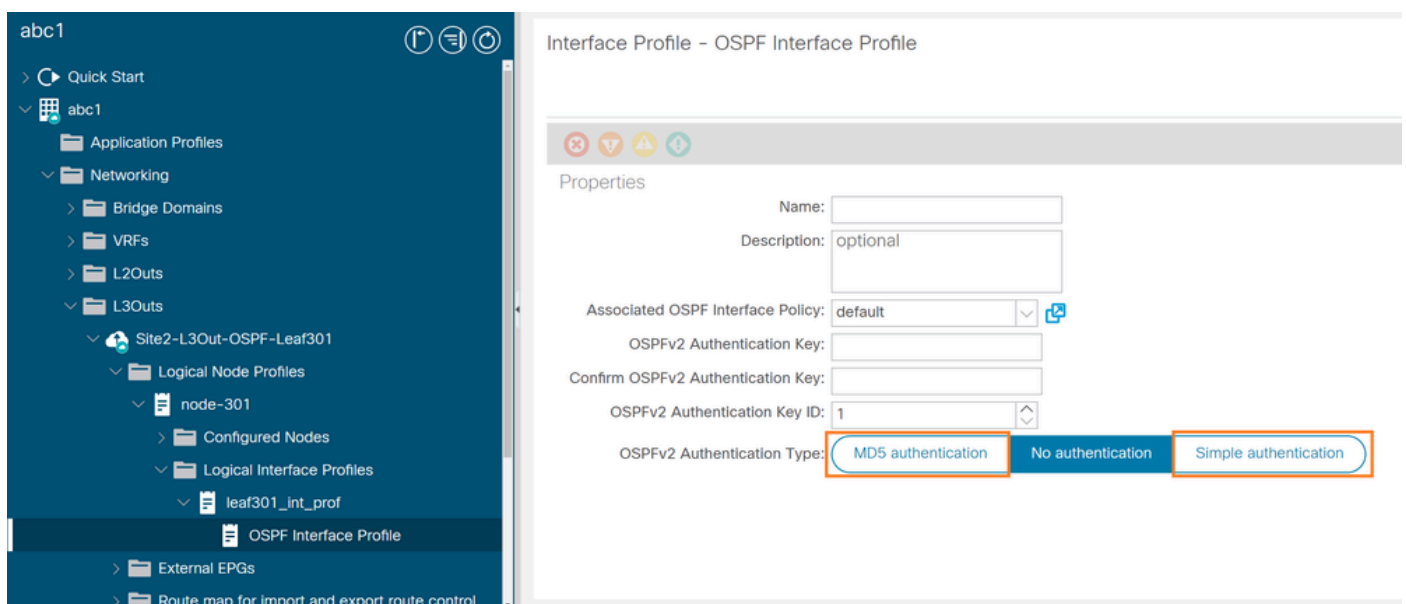
Autenticazione null: viene chiamata anche Type 0 e indica che nell'intestazione del pacchetto non sono incluse informazioni di autenticazione. È l'impostazione predefinita.

Autenticazione semplice - Viene anche denominata Tipo 1 e utilizza semplici password non crittografate.

Autenticazione MD5 - Viene chiamata anche Tipo 2 e utilizza password crittografiche MD5.

Non è necessario impostare l'autenticazione. Tuttavia, se impostato, tutti i router peer sullo stesso segmento devono avere la stessa password e lo stesso metodo di autenticazione.

Dalla GUI ACI, selezionare Fabric > Tenants > Networking > L3Outs > "L3outName" > "Node-X" > Logical Interface Profiles > OSPF Interface Profile come mostrato nell'immagine.



Configurazione di MD5 o delle autenticazioni semplici

Dalla 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-lout pkt on Vlan1:
```

```
auth md5: key cisco
```

```
, key id 1 Seq 40635829 (time 1704403462)
```

Dalla periferica esterna:

```
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
```

Soluzione: associare le autenticazioni.

Risoluzione dei problemi relativi all'adiacenza OSPF: mancata corrispondenza tra Hello/Dead Timers

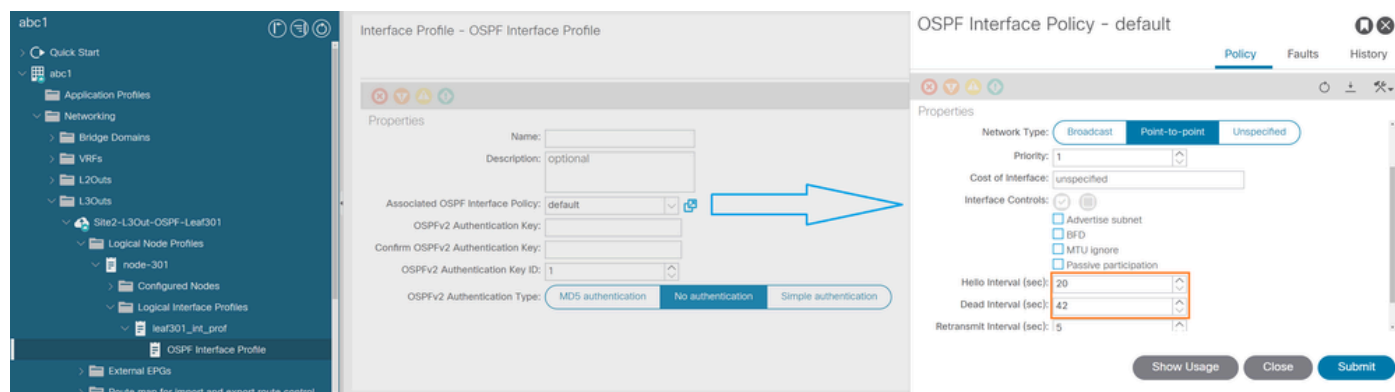
I pacchetti hello OSPF sono pacchetti che un processo OSPF invia ai propri vicini OSPF per mantenere la connettività con tali vicini. I pacchetti hello vengono inviati a intervalli configurabili (in secondi). L'impostazione predefinita è 10 secondi per un collegamento Ethernet (per il tipo di rete P2P e broadcast). I pacchetti Hello includono un elenco di tutti i router adiacenti per i quali è stato ricevuto un pacchetto hello entro l'intervallo di inattività. Anche l'intervallo inattivo è configurabile (in secondi) e per impostazione predefinita è quattro volte il valore dell'intervallo hello. Il valore di tutti gli intervalli hello deve essere lo stesso all'interno di una rete. Analogamente, il valore di tutti gli intervalli inattivi deve essere lo stesso all'interno di una rete.

Questi due intervalli funzionano insieme per mantenere la connettività indicando che il collegamento è operativo. Se un router non riceve un pacchetto hello da un router adiacente entro l'intervallo di inattività, dichiara tale router inattivo.

Se i timer hello e inattivi OSPF predefiniti vengono modificati sull'infrastruttura ACI, devono corrispondere al router esterno.

Dalla GUI ACI, selezionare Fabric > Tenants > Networking > L3Outs > "L3outName" > "Node-X" > Logical Interface Profiles > OSPF

Interface Profile > Associated OSPF Interface Policy come mostrato nell'immagine.



Timer Hello/Dead personalizzati

Dalla foglia di confine:

<#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

Dalla periferica esterna:

<#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

Soluzione: abbinare i timer OSPF.

Risoluzione dei problemi relativi all'adiacenza OSPF: mancata corrispondenza del tipo di interfaccia

In questa sezione viene descritta la risoluzione dei problemi quando in ACI è configurato Broadcast o unspecified (Trasmissione non specificata) e la periferica esterna è P2P.

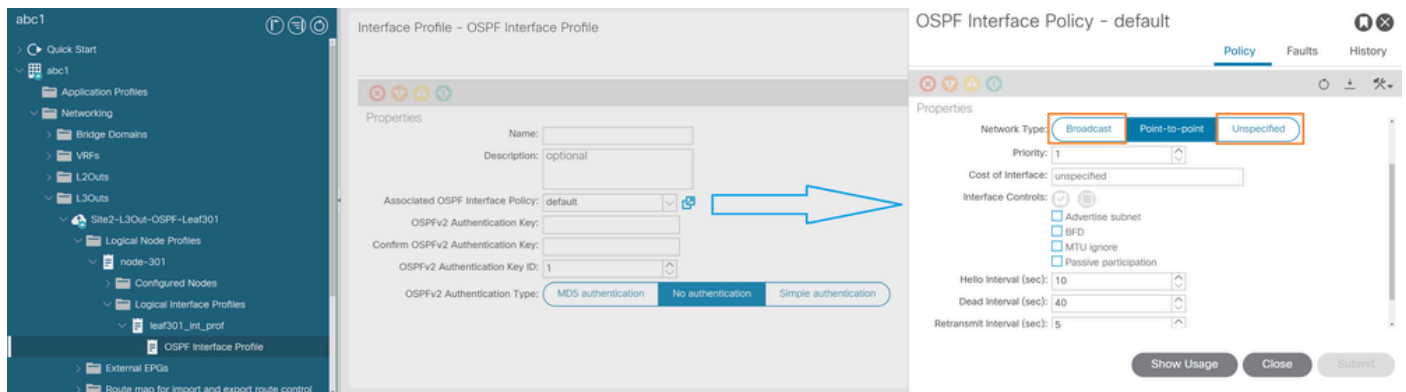
Trasmissione

- Il tipo di rete Broadcast è il tipo predefinito per un'interfaccia Ethernet abilitata per OSPF
- Il tipo di rete Broadcast richiede che un collegamento supporti le funzionalità di trasmissione di layer 2
- Il tipo di rete Broadcast dispone di un hello di 10 secondi e di un timer inattivo di 40 secondi (come P2P)
- Un tipo di rete broadcast OSPF richiede l'utilizzo di un DR/BDR.

Point-to-point

- Un tipo di rete OSPF P2P non mantiene una relazione DR/BDR
- Il tipo di rete P2P ha un hello di 10 secondi e un timer inattivo di 40 secondi
- I tipi di rete P2P sono progettati per essere utilizzati tra due router collegati direttamente

Dalla GUI ACI, selezionare Fabric > Tenants > Networking > L3Outs > "L3outName" > "Node-X" > Logical Interface Profiles > OSPF Interface Profile > Associated OSPF Interface Policy come mostrato nell'immagine.



Tipo di rete broadcast o non specificato configurato

Dalla foglia di confine:

<#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|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

Dalla periferica esterna:

<#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

Scheda grafica del comando di verifica

In questo documento è stato fatto riferimento a questi comandi per risolvere i problemi relativi ai diversi scenari.

Nodo	Comandi	Scopo
ACI Switch	show ip ospf neighbors vrf <<TNT:VRF>>	Controllare la relazione di vicinato in VRF
	show ip ospf interface brief vrf <<TNT:VRF>>	Controllare le interfacce OSPF associate al VRF
	moquery -c faultInst -x 'query-target-filter=wcard(faultInst.dn,"<<TNT:VRF>>")'	È possibile controllare i guasti associati al VRF
	moquery -c ospfIf -x 'query-target-filter=wcard(ospfIf.dn,"<<TNT:VRF>>")'	Controllare tutti i dettagli dell'interfaccia OSPF associata al VRF
	moquery -c ospfIf -x 'query-target-filter=wcard(ospfIf.id,"<<vlanX>>")'	Controllare la configurazione

		dell'interfaccia OSPF
	moquery -c arpAdjEp -x 'query-target-filter=wcard(arpAdjEp.ifId,"<<vlanX>>")' grep ip	Controllare l'indirizzo IP applicato sul dispositivo esterno dall'ARP associato all'interfaccia
	log_trace_bl_print_tool /var/sysmgr/tmp_logs/ospfv2_1_trace.bl tail -n 250 grep <<TNT:VRF>>	Decodifica traccia OSPF in tempo reale per VRF
	tcpdump -i kpm_inb proto ospf -vv -e -w - tee /data/techsupport/Node-XXX_OSPF.pcap tcpdump -r - host any	Acquisire il traffico OSPF da analizzare su 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>>	Acquisire il traffico specifico dell'host per analizzarlo su 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	Acquisire il traffico SRC e DST specifico dell'HOST per analizzarlo su Wireshark
	tcpdump src host <<X.X.X.X>> -vv -e -i kpm_inb -c 1	Acquisire un singolo control plane in banda per un host specifico
ACI APIC	moquery -c ospfIfP -x 'query-target-filter=wcard(ospfIfP.dn,"<<TNT>>\out-<<L3outName>>")'	Controllare il tipo di autenticazione configurato
	moquery -c l3ext.RsPathL3OutAtt -x 'query-target-filter=wcard(l3extRsPathL3OutAtt.dn,"<<TNT>>\out-<<L3outName>>")'	Verifica configurazione percorso L3out
	moquery -c faultRecord -f 'fault.Inst.code=="F1385"' -x 'query-target-filter=wcard(faultRecord.dn,"<<TNT:VRF>>")'	Verifica record cronologici errori per errore F1385 protocollo-adiacenza-OSPF-inattivo

	moquery -c ospfRsIfPol -x 'query-target-filter=wcard(ospfIfP.dn,"<<TNT>>\out-<<L3outName>>")' grep tnOspfIfPolName	Controllo L3out per i criteri dell'interfaccia OSPF associata personalizzata
	moquery -c ospfIfPol -x 'query-target-filter=wcard(ospfIfPol.name,"Custom_OSPF_Interface_Policy")'	Verificare i dettagli personalizzati dei criteri dell'interfaccia OSPF associata
Switch NXOS	show ip int bri vrf <<VRF>>	Controllare le interfacce OSPF con vrf
	show run ospf all section EthernetX/Y	Verifica configurazione OSPF
	show ip ospf interface EthernetX/Y	Controllare i parametri annunciati dell'interfaccia OSPF

Informazioni correlate

- [Risoluzione dei problemi relativi all'inoltro esterno ACI](#)
- [Supporto tecnico Cisco e download](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).