

排除ACI管理和核心服务故障 — 带内和带外管理

目录

[简介](#)

[背景信息](#)

[带内管理与带外管理](#)

[APIC连接首选项](#)

[场景:无法访问管理网络](#)

[带外管理访问](#)

[带外配置验证](#)

[静态节点管理地址GUI验证](#)

[带外EPG — 默认](#)

[带外合同](#)

[外部管理网络实例配置文件](#)

[带内管理配置](#)

[将充当带内管理网关的网桥域子网](#)

[故障F0467 — 内部EPG](#)

[带内EPG](#)

[外部EPG实例配置文件](#)

[静态节点管理地址](#)

简介

本文档介绍对ACI带外(OOB)和带内(INB)管理进行故障排除的步骤。

背景信息

本文档中的资料摘自[思科以应用为中心的基础设施故障排除，第二版](#)书，具体来说是“管理和核心服务 — 带内和带外管理”一章。

带内管理与带外管理

ACI交换矩阵节点有两种管理连接选项；带外(OOB) (管理设备背面的专用物理管理端口) 或带内(INB)(使用管理租户中的特定EPG/BD/VRF调配带内(INB)，具有一定程度的可配置参数)。管理 (“mgmt”)租户中存在OOB EPG，但默认情况下存在，且无法修改。它仅允许配置提供的OOB合同。在APIC上，在“ifconfig”命令输出中观察到OOB接口为“oobmgmt”，带内接口将由“bond.x”接口表示，其中是为带内EPG配置的封装VLAN。

```
apic1# ifconfig oobmgmt
oobmgmt: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.4.20 netmask 255.255.255.0 broadcast 192.168.4.255
    inet6 fe80::7269:5aff:feca:2986 prefixlen 64 scopeid 0x20
    ether 70:69:5a:ca:29:86 txqueuelen 1000 (Ethernet)
    RX packets 495815 bytes 852703636 (813.2 MiB)
```

```
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 432927 bytes 110333594 (105.2 MiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

```
apic1# ifconfig bond0.300
bond0.300: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1496
  inet 10.30.30.254 netmask 255.255.255.0 broadcast 10.30.30.255
  inet6 fe80::25d:73ff:fec1:8d9e prefixlen 64 scopeid 0x20
  ether 00:5d:73:c1:8d:9e txqueuelen 1000 (Ethernet)
  RX packets 545 bytes 25298 (24.7 KiB)
  RX errors 0 dropped 0 overruns 0 frame 0
  TX packets 6996 bytes 535314 (522.7 KiB)
  TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

在枝叶上，在“ifconfig”命令输出中，OOB接口被视为“eth0”，INB被视作专用SVI。用户可以通过“ifconfig”或“show ip interface vrf mgmt :”查看接口，其中是为带内VRF选择的名称。

```
leaf101# show interface mgmt 0
mgmt0 is up
admin state is up,
  Hardware: GigabitEthernet, address: 00fc.baa8.2760 (bia 00fc.baa8.2760)
  Internet Address is 192.168.4.23/24
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec
  reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, medium is broadcast
  Port mode is routed
  full-duplex, 1000 Mb/s
  Beacon is turned off
  Auto-Negotiation is turned on
  Input flow-control is off, output flow-control is off
  Auto-mdix is turned off
  EtherType is 0x0000
  30 seconds input rate 3664 bits/sec, 4 packets/sec
  30 seconds output rate 4192 bits/sec, 4 packets/sec
  Rx
    14114 input packets 8580 unicast packets 5058 multicast packets
    476 broadcast packets 2494768 bytes
  Tx
    9701 output packets 9686 unicast packets 8 multicast packets
    7 broadcast packets 1648081 bytes
```

```
leaf101# show ip interface vrf mgmt:inb
IP Interface Status for VRF "mgmt:inb-vrf"
vlan16, Interface status: protocol-up/link-up/admin-up, iod: 4, mode: pervasive
  IP address: 10.30.30.1, IP subnet: 10.30.30.0/24
  secondary IP address: 10.30.30.3, IP subnet: 10.30.30.0/24
  IP broadcast address: 255.255.255.255
  IP primary address route-preference: 0, tag: 0
```

“show ip interface vrf mgmt :”将显示带内管理BD子网IP作为辅助IP地址；这是预期输出。

在主干交换机上，带内管理IP地址被添加为“mgmt :”VRF中的专用环回接口。因此，此实施与枝叶交换机上的带内管理IP实施不同。观察主干交换机上下面的“show ip int vrf mgmt :”命令输出

```
spine201# show ip interface vrf mgmt:inb
```

```

IP Interface Status for VRF "mgmt:inb"
lo10, Interface status: protocol-up/link-up/admin-up, iod: 98, mode: pervasive
  IP address: 10.30.30.12, IP subnet: 10.30.30.12/32
  IP broadcast address: 255.255.255.255
IP primary address route-preference: 0, tag: 0

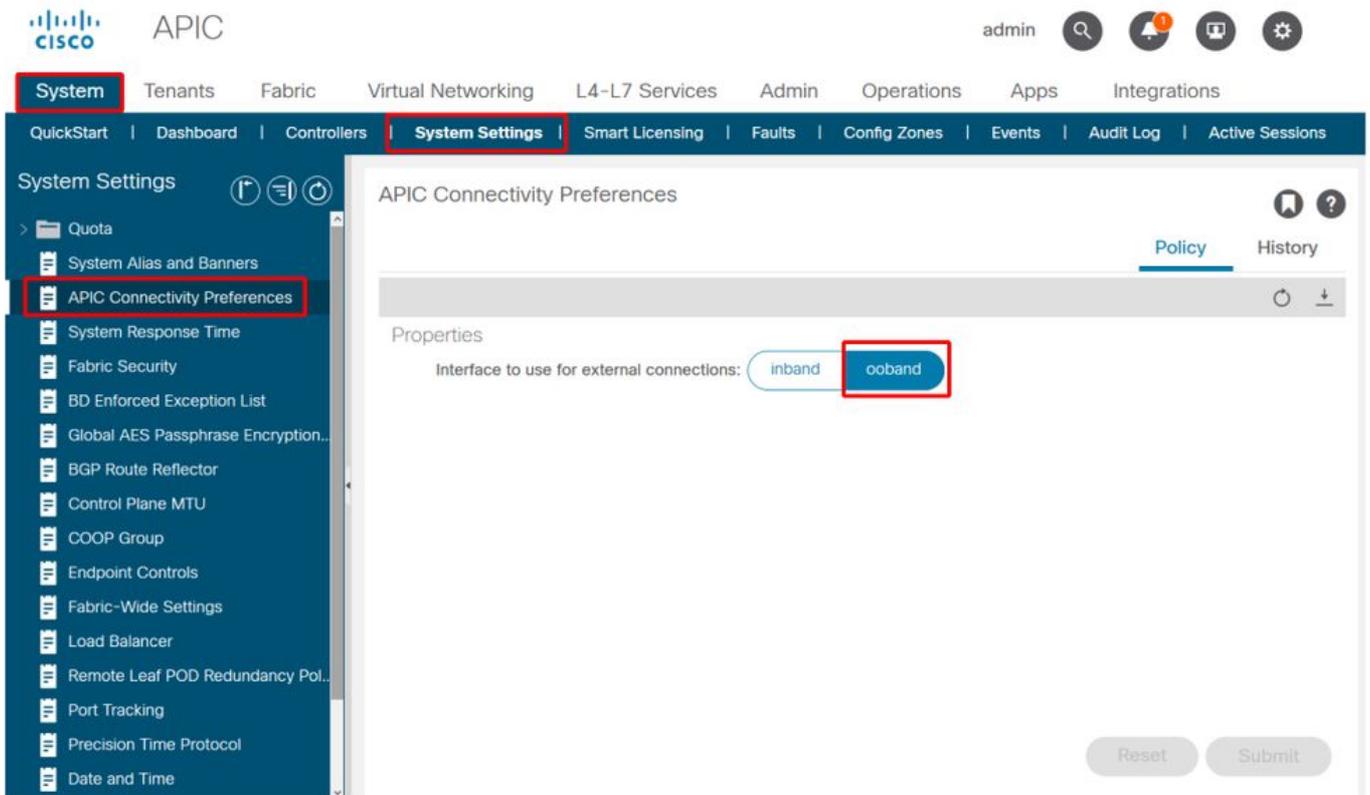
```

在System Settings下，有一个设置用于选择APIC的带内连接首选项或带外连接首选项。

只有从APIC发送的流量将使用“APIC连接首选项”中选择的管理首选项。APIC仍然可以在带内或带外接收流量（假设已配置其中之一）。APIC使用以下转发逻辑：

- 进入接口并流出同一接口的数据包。
- 从APIC发往直连网络的数据包通过直连接口。
- 根据APIC连接首选项，源自APIC、发往远程网络的数据包首选带内或带外。

APIC连接首选项



已选择OOB的APIC路由表。观察oobmgmt接口的度量值16，该值低于bond0.300带内管理接口度量32。这意味着带外管理接口将用于传出管理流量。

```

apic1# bash
admin@apic1:~> route -n
Kernel IP routing table
Destination      Gateway         Genmask        Flags Metric Ref    Use Iface
0.0.0.0          192.168.4.1    0.0.0.0        UG    16     0      0 oobmgmt
0.0.0.0          10.30.30.1     0.0.0.0        UG    32     0      0 bond0.300

```

选择带内的APIC路由表。观察带bond0.300管理接口的度量（如果为8，现在该度量低于oobmgmt接口度量16）。这意味着带bond0.300管理接口将用于传出管理流量。

```

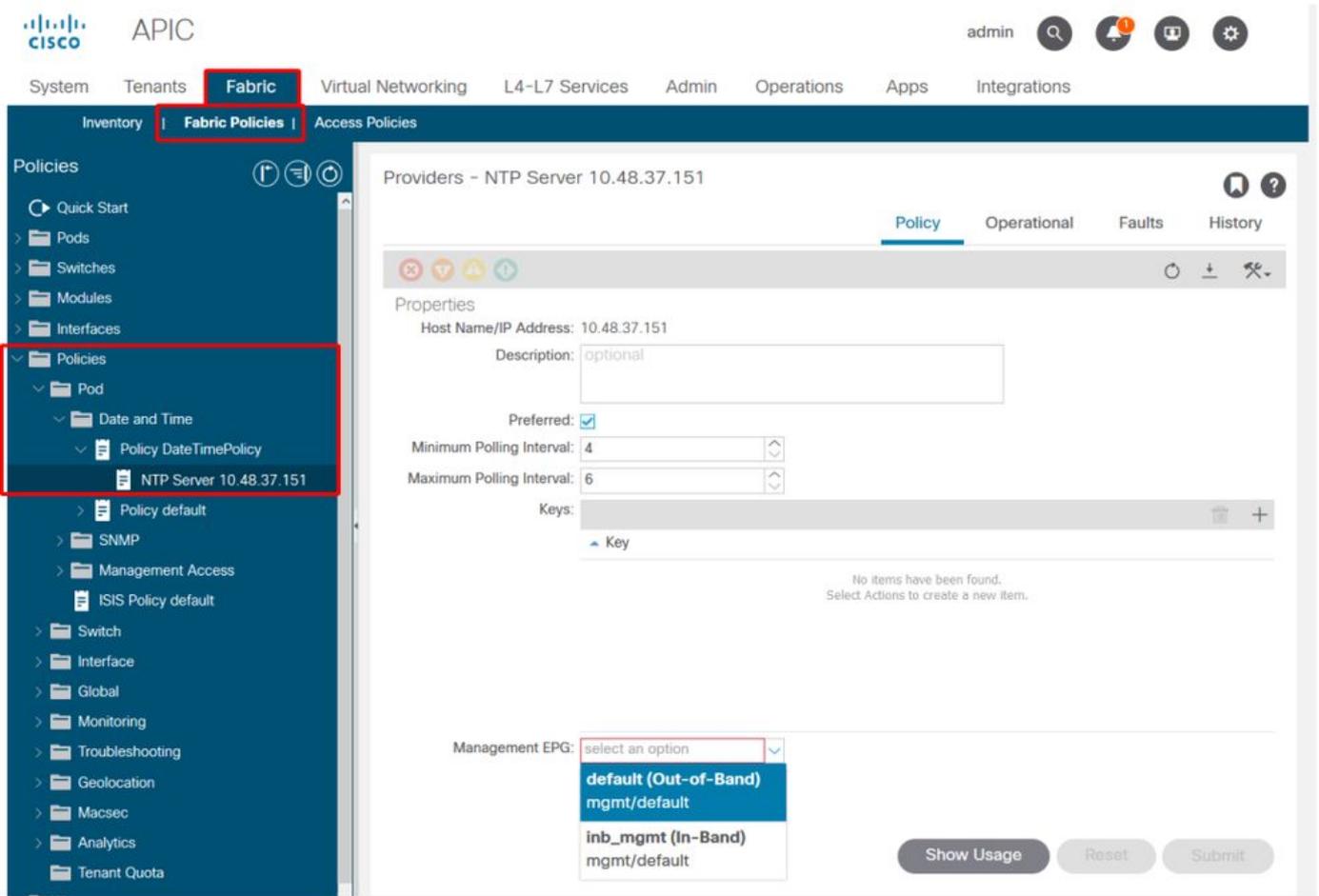
admin@apic1:~> route -n

```

Kernel IP routing table

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
0.0.0.0	10.30.30.1	0.0.0.0	UG	8	0	0	bond0.300
0.0.0.0	192.168.4.1	0.0.0.0	UG	16	0	0	oobmgmt

枝叶和主干节点管理首选项不受此设置的影响。这些连接首选项在协议策略下选择。以下是NTP的示例。



如果在“APIC连接首选项”下选择带内，但在协议下选择带外，则使用协议数据包的哪个接口？

- APIC连接首选项将始终优先于APIC上的协议选择。
- 枝叶节点则相反，它们只引用协议下的选择。

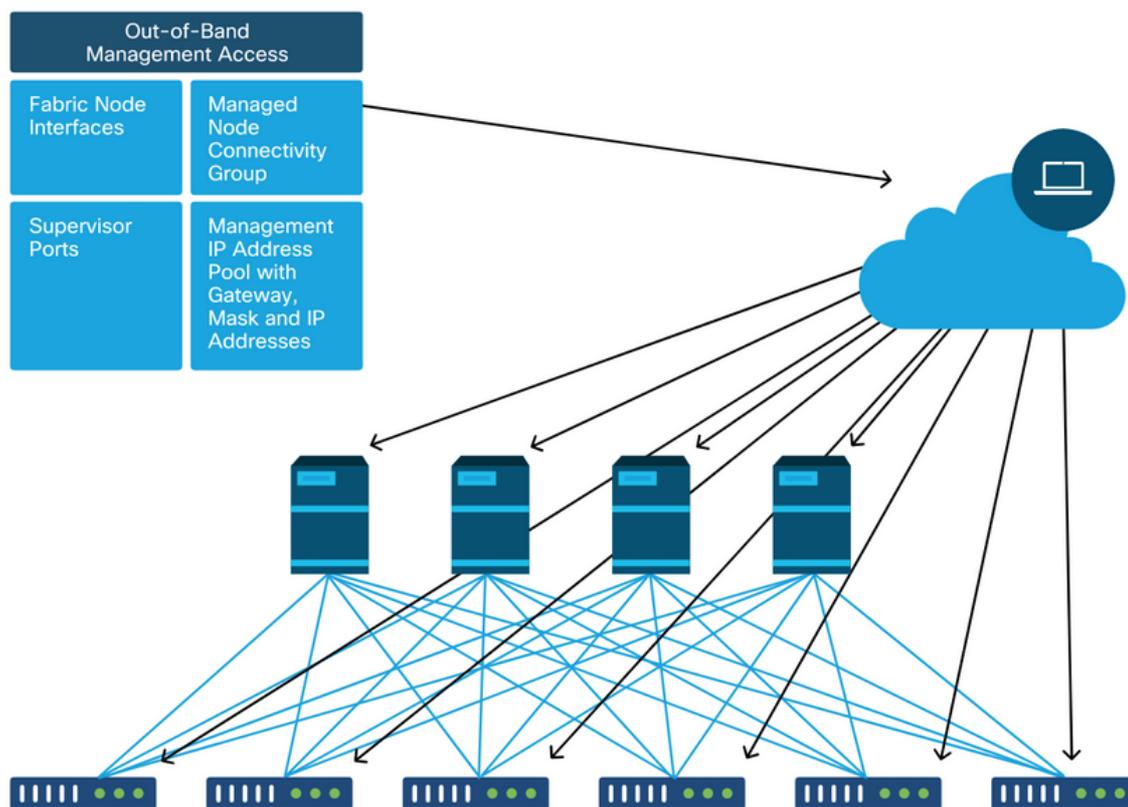
场景:无法访问管理网络

如果用户无法访问管理网络，可能是由于许多不同的问题，但他们始终可以使用相同的方法隔离问题。此场景中的假设是用户不能从其L3Out后面访问管理网络中的任何设备。

- 检验APIC连接首选项。图“APIC连接首选项”中对此进行了概述，选项为OOB或带内。
- 根据所选的首选项，验证配置是否正确、接口是否启用、默认网关是否可通过所选接口访问，以及数据包的路径上无丢弃。

不要忘记在GUI的每个配置部分中检查故障。但是，某些配置错误可能会表现为意外状态，但在其他部分中可能会生成错误，而不是用户最初认为的错误。

带外管理访问



带外配置验证

对于带外配置，在名为“mgmt”的特殊租户下有四个文件夹要验证：

- 节点管理地址。
- 节点管理EPG。
- 带外合同（根据合同）。
- 外部网络实例配置文件。

节点管理地址可以静态分配，也可以从池中分配。以下是静态地址分配的示例。验证已分配带外IP地址类型以及默认网关是否正确。

静态节点管理地址GUI验证

The screenshot shows the Cisco APIC interface for the 'mgmt' tenant. The left sidebar highlights the 'Node Management Addresses' folder. The main content area displays a table of static node management addresses.

Node ID	Name	Type	EPG	IPv4 Address	IPv4 Gateway	IPv6 Address	IPv6 Gateway
pod-1/node-1	bdsol-aci37-apic1	Out-Of-Band	default	10.48.176.57/24	10.48.176.1	::	::
pod-1/node-101	S1P1-Leaf101	Out-Of-Band	default	10.48.176.70/24	10.48.176.1	::	::
pod-1/node-102	S1P1-Leaf102	Out-Of-Band	default	10.48.176.71/24	10.48.176.1	::	::
pod-1/node-2	bdsol-aci37-apic2	Out-Of-Band	default	10.48.176.58/24	10.48.176.1	::	::
pod-1/node-201	S1P1-Spine201	Out-Of-Band	default	10.48.176.74/24	10.48.176.1	::	::
pod-1/node-202	S1P1-Spine202	Out-Of-Band	default	10.48.176.75/24	10.48.176.1	::	::
pod-1/node-301	S1P2-Leaf301	Out-Of-Band	default	10.48.176.72/24	10.48.176.1	::	::
pod-1/node-302	S1P2-Leaf302	Out-Of-Band	default	10.48.176.73/24	10.48.176.1	::	::
pod-1/node-401	S1P2-Spine401	Out-Of-Band	default	10.48.176.76/24	10.48.176.1	::	::
pod-1/node-402	S1P2-Spine402	Out-Of-Band	default	10.48.176.77/24	10.48.176.1	::	::
pod-2/node-3	bdsol-aci37-apic3	Out-Of-Band	default	10.48.176.59/24	10.48.176.1	::	::

带外EPG应出现在节点管理EPG文件夹下。

带外EPG — 默认

The screenshot shows the configuration page for the 'Out-of-Band EPG - default' policy. The left sidebar highlights the 'Out-of-Band EPG - default' folder. The main content area displays the configuration details for the policy.

Properties

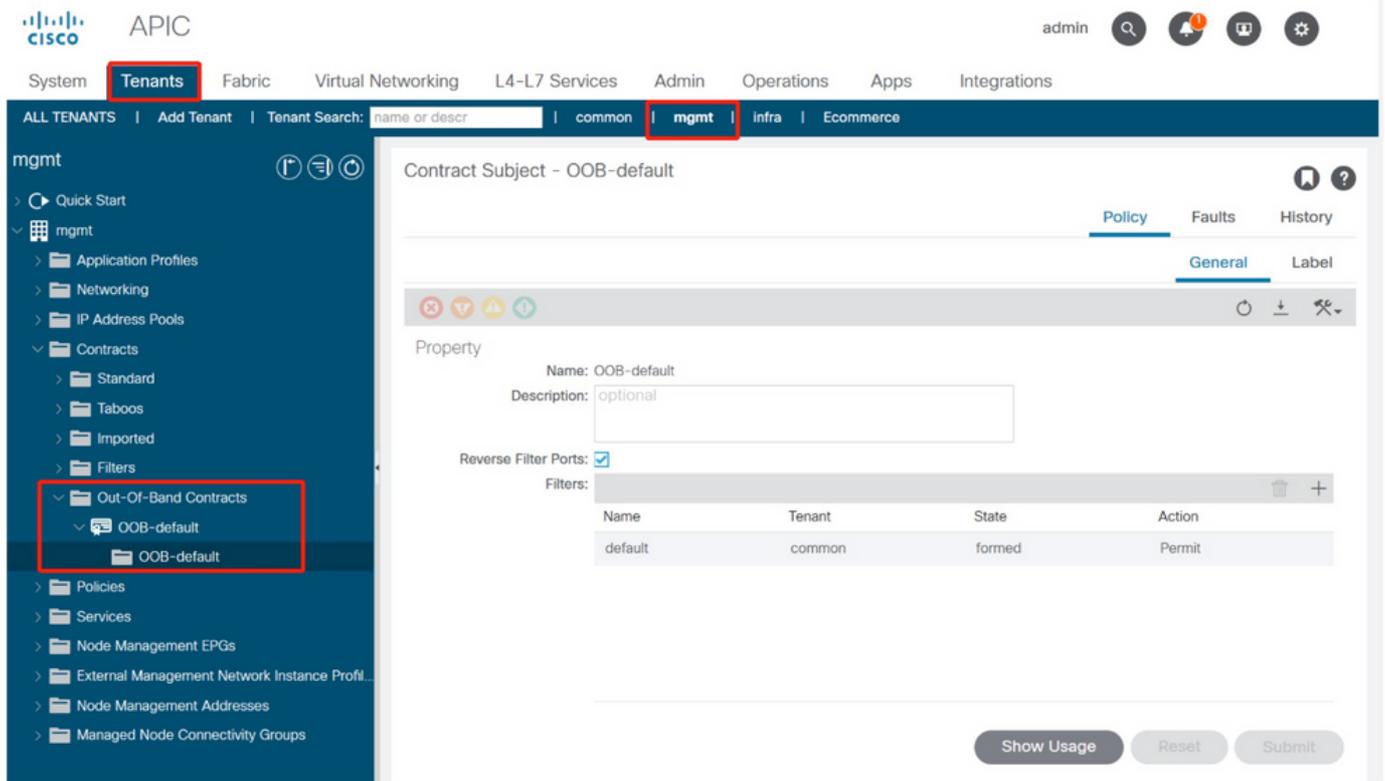
- Name: default
- Tags:
- Configuration Issues: Configuration State: applied
- Class ID: 16387
- QoS Class: Unspecified

Provided Out-of-Band Contracts:

OOB Contract	Tenant	Type	QoS Class	State
OOB-default	mgmt	oobrc-OOB-default	Unspecified	formed

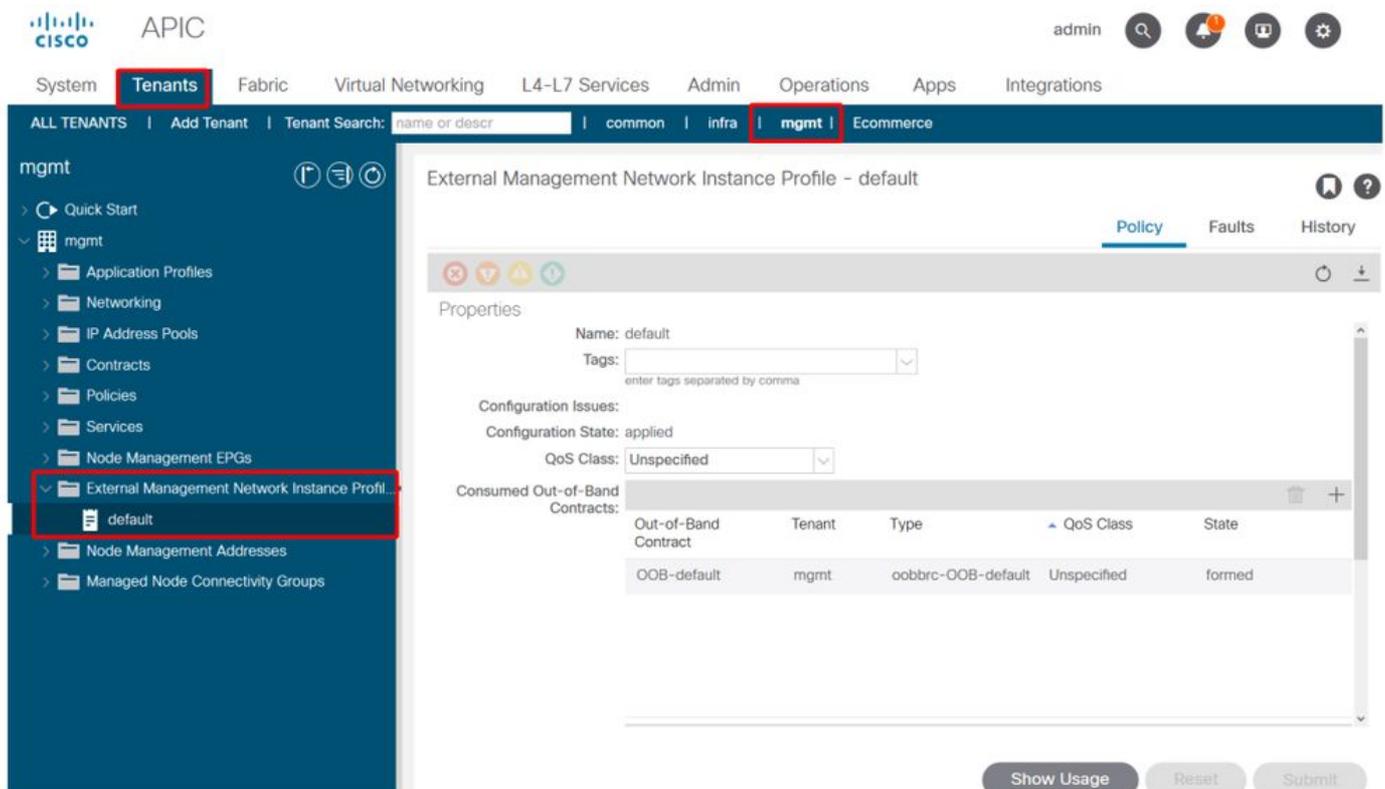
管理哪些管理服务由带外EPG提供的合同是带外合同文件夹中配置的特殊合同。

带外合同



接下来，验证已创建外部管理网络实例配置文件，并且已将正确的带外合同配置为“消耗的带外合同”。

外部管理网络实例配置文件



接下来要检验的项目是接口状态和布线，然后是到网关的连接。

- 要检查oobmgmt接口是否启用，请在APIC CLI上输入“ifconfig oobmgmt”。确认接口标志为“UP”和“RUNNING”，配置了正确的IP地址，并且数据包在RX和TX计数器中增加。如果缺少任

何检查，请验证使用的电缆是否正确，以及它们是否连接到APIC上正确的物理管理端口。管理端口将被标记为Eth1-1和Eth1-2，最近的硬件带有带外接口的oobmgmt标签。有关APIC背面的物理带外管理端口的详细信息，请参阅“交换矩阵发现”一章中的“初始交换矩阵设置”部分。

```
apic1# ifconfig oobmgmt
oobmgmt: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.4.20 netmask 255.255.255.0 broadcast 192.168.4.255
inet6 fe80::7269:5aff:feca:2986 prefixlen 64 scopeid 0x20
ether 70:69:5a:ca:29:86 txqueuelen 1000 (Ethernet)
RX packets 295605 bytes 766226440 (730.7 MiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 253310 bytes 38954978 (37.1 MiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

- 要通过OOB检查网络连接，请使用ping测试数据包通过带外网络的路径。

```
apic1# ping 192.168.4.1
PING 192.168.4.1 (192.168.4.1) 56(84) bytes of data.
64 bytes from 192.168.4.1: icmp_seq=1 ttl=255 time=0.409 ms
64 bytes from 192.168.4.1: icmp_seq=2 ttl=255 time=0.393 ms
64 bytes from 192.168.4.1: icmp_seq=3 ttl=255 time=0.354 ms
```

在APIC的bash shell中使用traceroute，跟踪与最终用户的连接。如果traceroute不完整，请登录此设备（如果可访问），ping oobmgmt接口并ping主机。根据故障方向，将问题作为传统网络问题进行故障排除。

Traceroute的工作方式是，从1开始，以不断增加的TTL发送UDP数据包。如果路由器收到包含TTL 1的数据包并需要对其进行路由，它会丢弃该帧并向发送方发送一条ICMP不可达消息。每跳在当前TTL发送3个UDP数据包，星号表示未收到ICMP不可达/TTL已超出的数据包的尝试。由于某些路由设备禁用了ICMP不可达/超出TTL消息，因此当它们收到需要路由的TTL 1数据包时，它们只会丢弃该数据包，并且不会将该消息发送回发送方，因此在大多数网络中都预期存在这3个星号块。

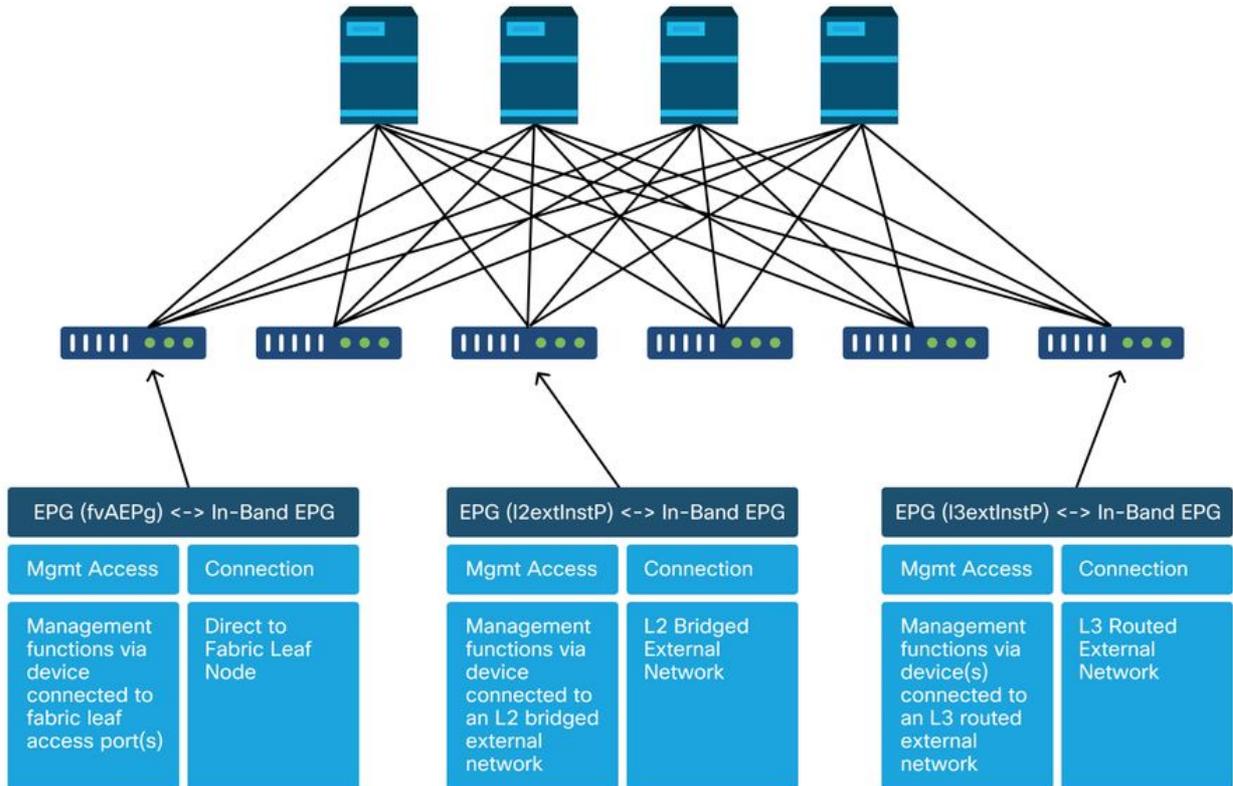
```
apic1# bash
admin@apic1:~> traceroute 10.55.0.16
traceroute to 10.55.0.16 (10.55.0.16), 30 hops max, 60 byte packets
 1  192.168.4.1 (192.168.4.1)  0.368 ms  0.355 ms  0.396 ms
 2  * * *
 3  * * *
 4  10.0.255.221 (10.0.255.221)  6.419 ms  10.0.255.225 (10.0.255.225)  6.447 ms *
 5  * * *
 6  * * *
 7  10.55.0.16 (10.55.0.16)  8.652 ms  8.676 ms  8.694 ms
```

枝叶交换机可以访问tcpdump命令，该命令可用于验证哪些数据包通过oobmgmt接口。以下示例捕获在枝叶和主干交换机上使用的oobmgmt接口“eth0”，并使用“— n”选项为tcpdump提供使用的IP地址而不是DNS名称，然后特别针对NTP数据包（UDP端口123）进行过滤。回想一下，在上一个示例中，枝叶正在轮询NTP服务器172.18.108.14。下面，用户可以验证NTP数据包是否通过带外接口传输，以及枝叶是否正在接收来自服务器的响应。

```
fab1-leaf101# tcpdump -n -i eth0 dst port 123
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
16:49:01.431624 IP 192.168.4.23.123 > 172.18.108.14.123: NTPv4, Client, length 48
16:49:01.440303 IP 172.18.108.14.123 > 192.168.4.23.123: NTPv4, Server, length 48
```

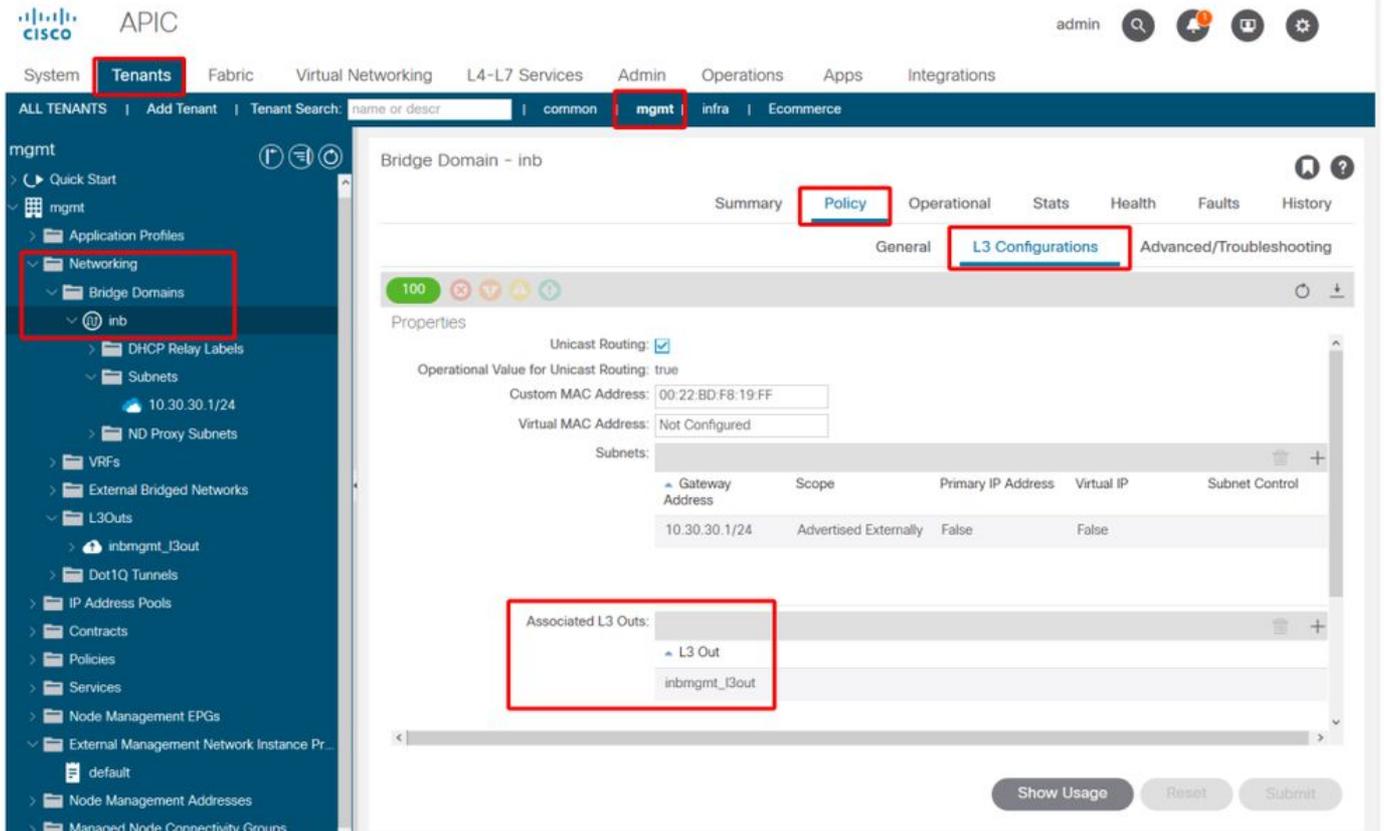
带内管理配置需要第2层或第3层部署的特定注意事项。本示例仅介绍第3层部署和故障排除。

带内管理配置



验证具有子网的管理租户中有一个BD，带内节点管理地址将从该BD分配给交换矩阵节点以实现带内连接，并确保L3Out在带内管理BD下相关联。

将充当带内管理网关的网桥域子网



验证带内节点管理EPG是否存在。根据下面的屏幕截图，带内EPG名称在GUI中以前缀“inb —”表示。验证带内EPG封装VLAN是否与VLAN池正确关联。

接入策略需要允许带内管理EPG中配置的封装VLAN: 'inb mgmt EPG encap VLAN > VLAN Pool > Domain > AEP > Interface Policy Group > Leaf Interface Profile > Switch Profile'。如果未配置支持访问策略，则会根据以下屏幕截图引发代码为F0467的故障。

故障F0467 — 内部EPG

8589935303

ID: 8589935303

Description: Fault delegate: Configuration failed for uni/tn-mgmt/mgmt-default/inb-inbmgmt due to Invalid VLAN Configuration, debug message: i
vlan-300STP Segment Id not present for Encap. Either the EpG is not associated with a domain or the domain does not have this vlan i

Severity: minor

Affected Object: [uni/tn-mgmt/mgmt-default/inb-inbmgmt](#)

Reported From: topology/pod-1/node-101/local/svc-policyelem-id-0/uni/epp/inb-[uni/tn-mgmt/mgmt-default/inb-inbmgmt]/nwissues

Created: 2019-10-03T02:23:04.637+00:00

Code: F0467

Type: Config

Cause: configuration-failed

Change Set:

Action: deletion

Domain: Tenant

Life Cycle:

Time Occurred: 1

Event Status: false

验证网桥域与上面为带内子网创建的域相同。最后，验证带内管理EPG上是否配置了由外部EPG使用的提供的合同。

带内EPG

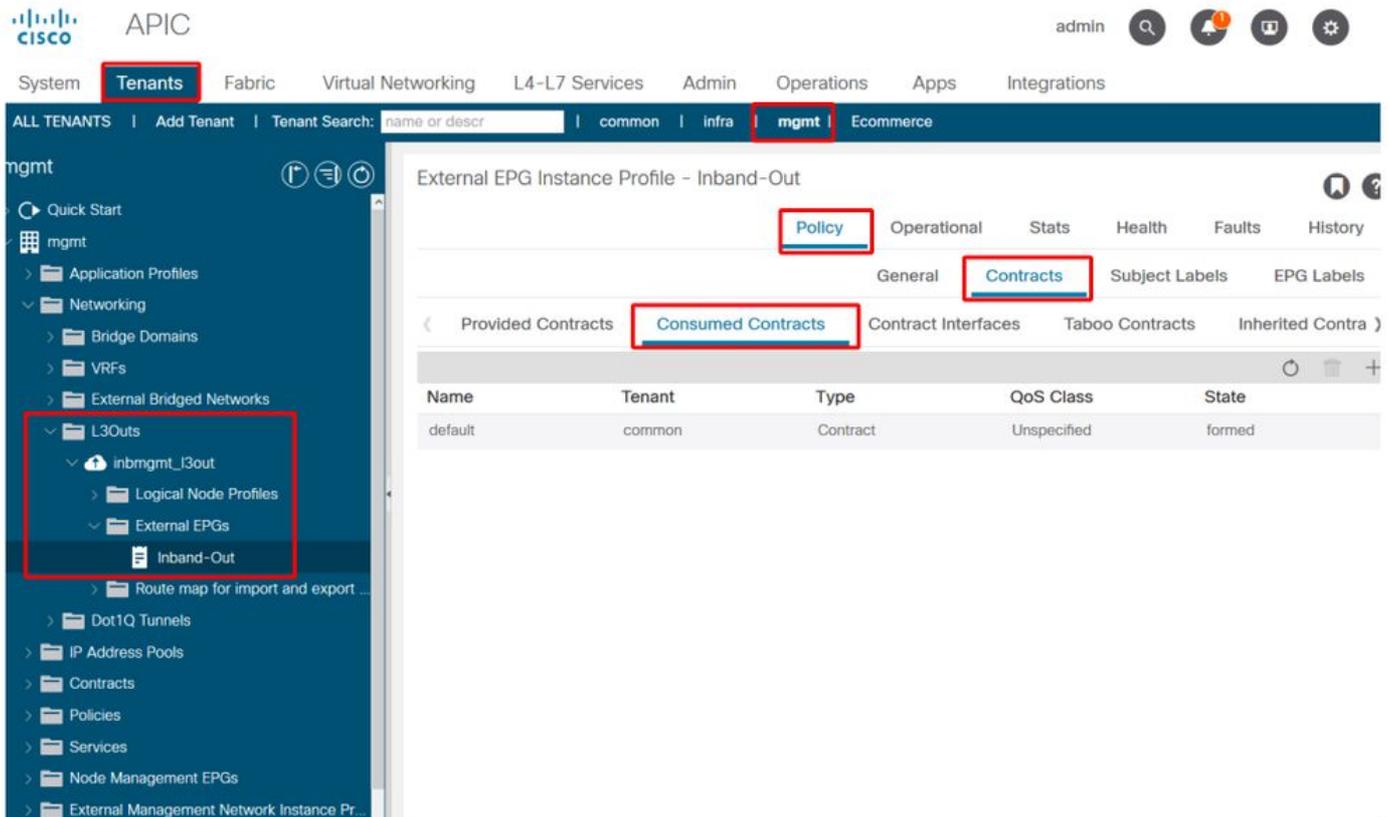
The screenshot shows the Cisco APIC interface. The 'Tenants' menu is highlighted, and the 'mgmt' tenant is selected. In the left-hand navigation pane, 'Node Management EPGs' is expanded, and 'In-Band EPG - inb_mgmt' is selected. The main content area displays the configuration for 'In-Band EPG - inb_mgmt' under the 'Policy' tab. The configuration includes the following details:

- Name: inb_mgmt
- Tags: (empty field)
- Encap: vlan-300 (with a note: e.g., vlan-1)
- Configuration Issues: (empty)
- Configuration State: applied
- Class ID: 32770
- QoS Class: Unspecified
- Bridge Domain: inb
- Resolved Bridge Domain: inb
- Provided Contracts: A table showing one contract named 'default' from the 'common' tenant, with a type of 'Contract', QoS Class 'Unspecified', Match Type 'AtleastOne', and State 'formed'.

Name	Tenant	Type	QoS Class	Match Type	State
default	common	Contract	Unspecified	AtleastOne	formed

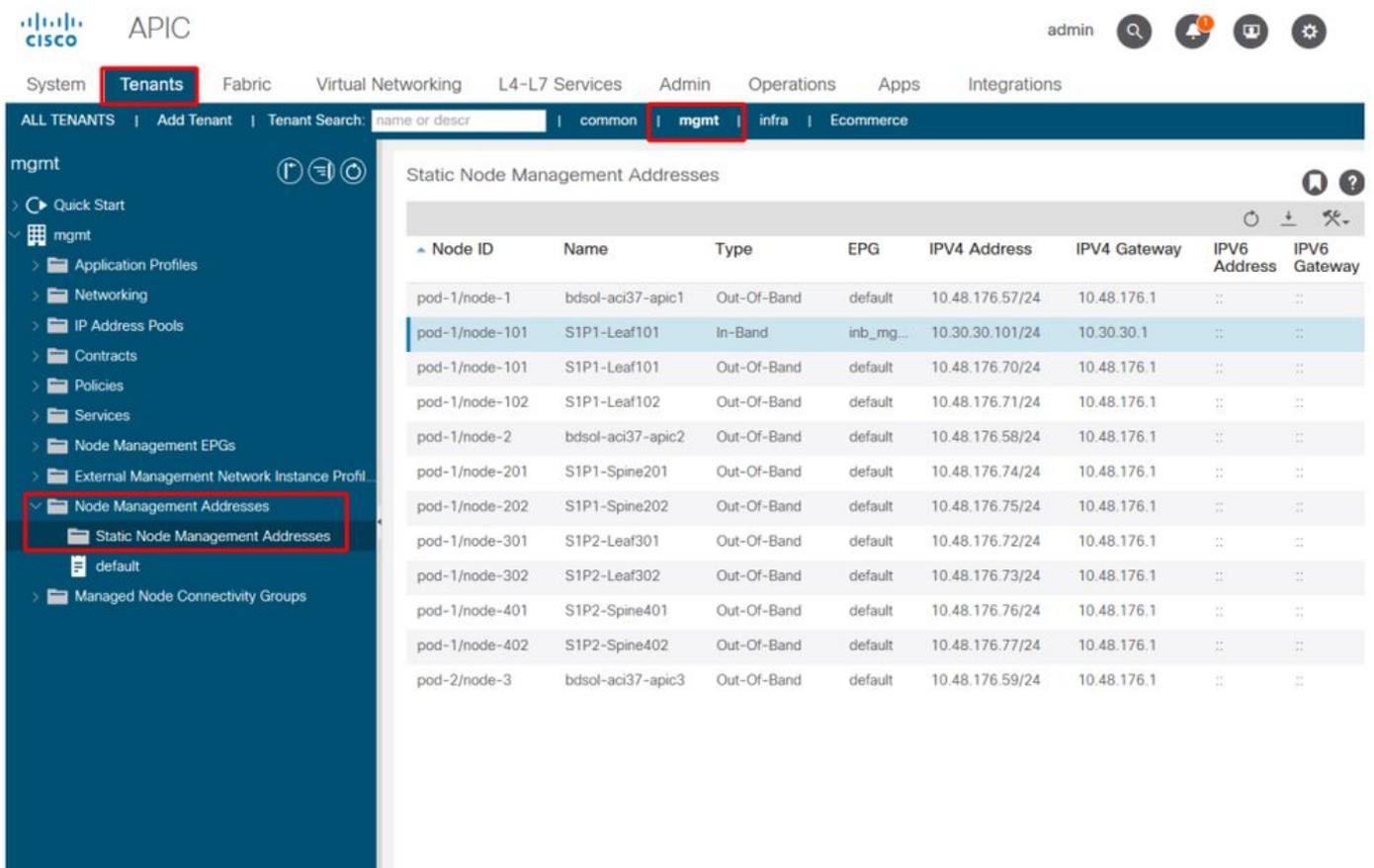
At the bottom of the configuration page, there are buttons for 'Show Usage', 'Reset', and 'Submit'.

外部EPG实例配置文件



与带外类似，交换矩阵节点的带内管理IP地址可以静态分配，也可以从预先选择的范围动态分配。验证应用于带内类型的地址是否与之前配置的BD子网匹配。还要验证默认网关是否正确。

静态节点管理地址



如果所有配置都正确，并且上述任何部分均没有故障，则下一步是在交换机和/或APIC之间执行

ping操作以验证带内连接在ACI中是否正常工作。

主干节点不会响应带内上的ping，因为它们使用环回接口进行连接，而环回接口不响应ARP。

枝叶交换机上使用的带内接口是kpm_inb。使用类似的tcpdump捕获，检验数据包是否从带内CPU接口发出。

```
fab2-leaf101# tcpdump -n -i kpm_inb dst port 123
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on kpm_inb, link-type EN10MB (Ethernet), capture size 65535 bytes
16:46:50.431647 IP 10.30.30.3.123 > 172.18.108.14.123: NTPv4, Client, length 48
16:47:19.431650 IP 10.30.30.3.123 > 172.18.108.15.123: NTPv4, Client, length 48
```

验证用于带内的SVI是“protocol-up/link-up/admin-up”。

```
fab1-leaf101# show ip interface vrf mgmt:inb-vrf
IP Interface Status for VRF "mgmt:inb-vrf"
vlan16, Interface status: protocol-up/link-up/admin-up, iod: 4, mode: pervasive
  IP address: 10.30.30.1, IP subnet: 10.30.30.0/24 secondary
  IP address: 10.30.30.3, IP subnet: 10.30.30.0/24
  IP broadcast address: 255.255.255.255
  IP primary address route-preference: 0, tag: 0
```

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）。