使用IP定向广播功能配置SD-Access静默主机

目录

简介

描述

拓扑

- 硬件和软件

要求

- 要求

Catalyst Center配置

网络设备配置

IP定向广播转发

边界 — 入口CPU分支和子网广播转换

边缘 — 入口广播

未知单播转发

在身份验证模板中启用LAN唤醒

身份验证前为主机手动分配VLAN

访问控制方向

替代方案

- 边缘节点和相同VLAN — 第2层泛洪
- 边缘节点和不同VLAN — 未知单播
- SD访问传输 — 未知单播
- SD访问传输 — IP定向广播

简介

本文档介绍如何使用L2泛洪和IP定向广播在SD-Access中管理无声主机，从而解决连接难题。

描述

大多数终端及其网络接口会定期传输流量，尤其是与控制相关的消息，例如ARP或DHCP。但是，某些终端仅在出现提示时响应，而不是按固定间隔发送数据包。这些设备仅按需发送控制数据包。在网络中，此类终端通常称为静默主机。在SD-Access环境中，静默主机必须停止所有流量或通过阻止控制平面数据包来限制其通信。

在SDA交换矩阵中，可在每个边缘节点抑制广播，或使用L2泛洪将广播转发到所有边缘 — 此过程通常限于边缘节点和L2边界。将广播转发到VLAN上的每个端口会模仿传统第2层网络的行为，从而显着帮助静默主机保持活动状态。但是，管理交换矩阵环境中的静默主机带来了挑战，因为缺乏常

规通信可能会中断身份验证机制、控制平面注册和转发。

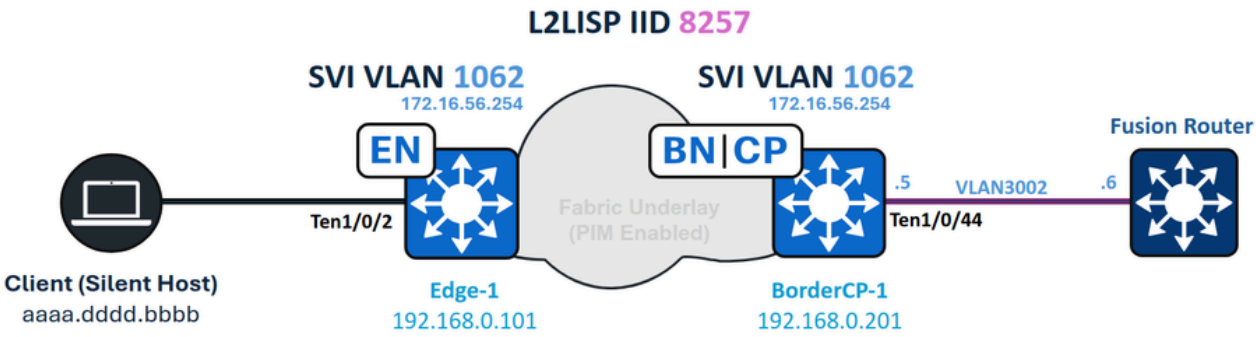
启用L2泛洪只能解决部分问题。静默主机只有在其他设备生成广播数据包时，才能从交换矩阵内的相同VLAN或交换矩阵边界接收广播数据包。IP定向广播是指目的地址设置为子网广播地址的IP数据包，源自该子网外部的主机。此功能需要在底层提供组播支持。在交换矩阵中启用IP定向广播时，所有子网广播数据包都会到达该子网内的每台主机。此功能还可以使用标准单播数据包唤醒设备，有效模拟传统网络中的“未知单播”行为。

拓扑

硬件和软件

- Catalyst 9000 系列交换机
- Catalyst Center版本2.3.7.9
- Cisco IOS® XE 17.15.03及更高版本(Border/CP & Edge)

拓扑：



网络图

要求

Cisco 建议您了解以下主题：

- Internet协议(IP)转发
- 定位器/ID分离协议(LISP)

- 独立于协议的多播 (PIM)
- SD-Access中的第2层泛洪

要求

- 此功能需要Cisco Catalyst Center 1.3或更高版本
- Cisco IOS XE 17.3和Cisco DNA Advantage许可证*
- 对于ASR和ISR边界，需要Cisco IOS XE 17.3.1或更高版本
- 不支持Catalyst 3000、4000、6000系列交换机或Nexus 7000

⚠ 警告：启用IP定向广播功能会自动激活L2泛洪。启用此功能之前，请确保衬底中的组播功能正常运行。

创建IP池后，您可以启用或禁用IP定向广播，类似于管理无线池或L2泛洪设置。

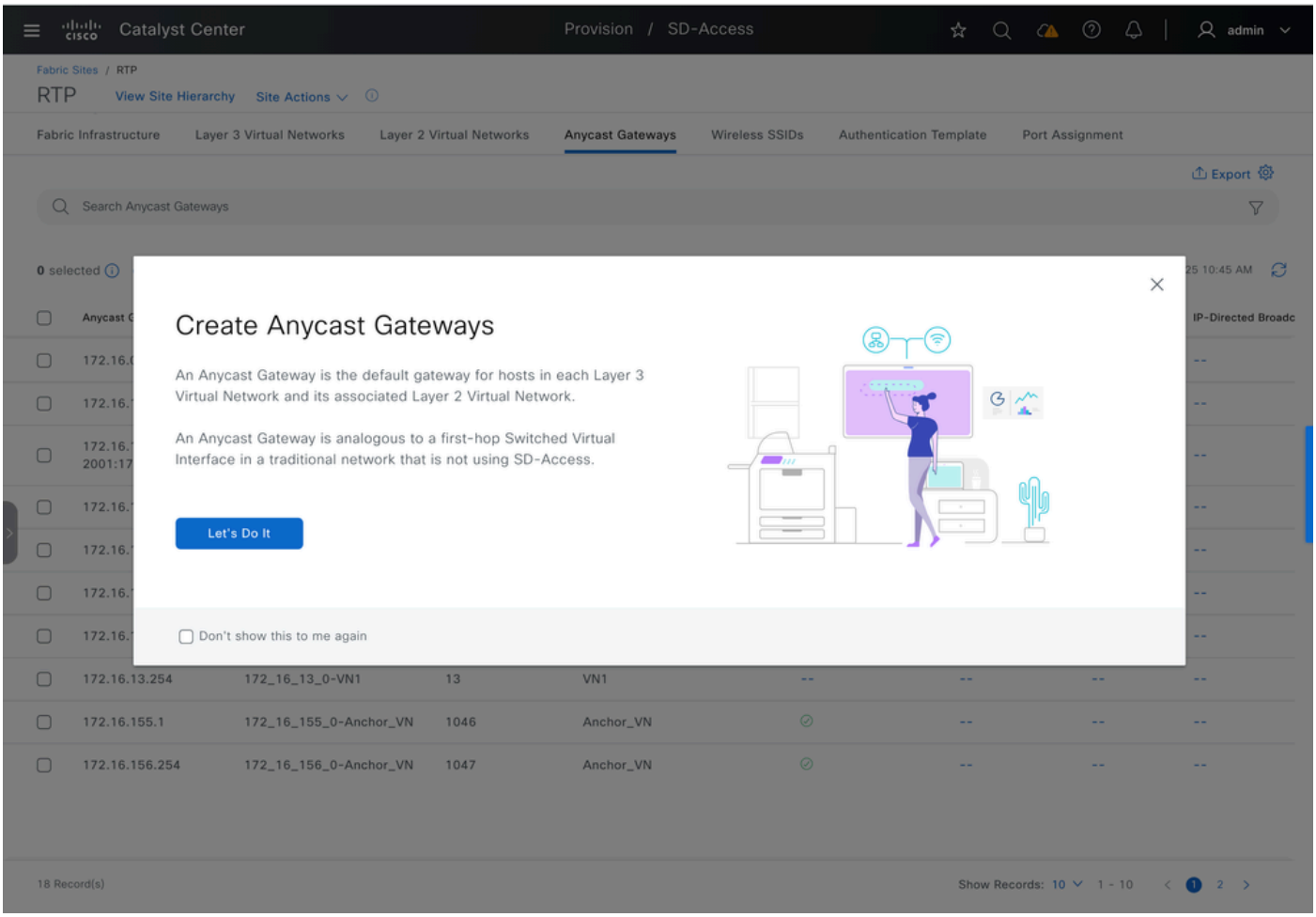
Catalyst Center配置

启用IP定向广播时，Catalyst Center会启动交换矩阵范围的调配任务。所有边缘节点、L2边界以及具有L3切换的边界都包含在此调配过程中。

在UI中触发IP定向广播工作流的步骤：

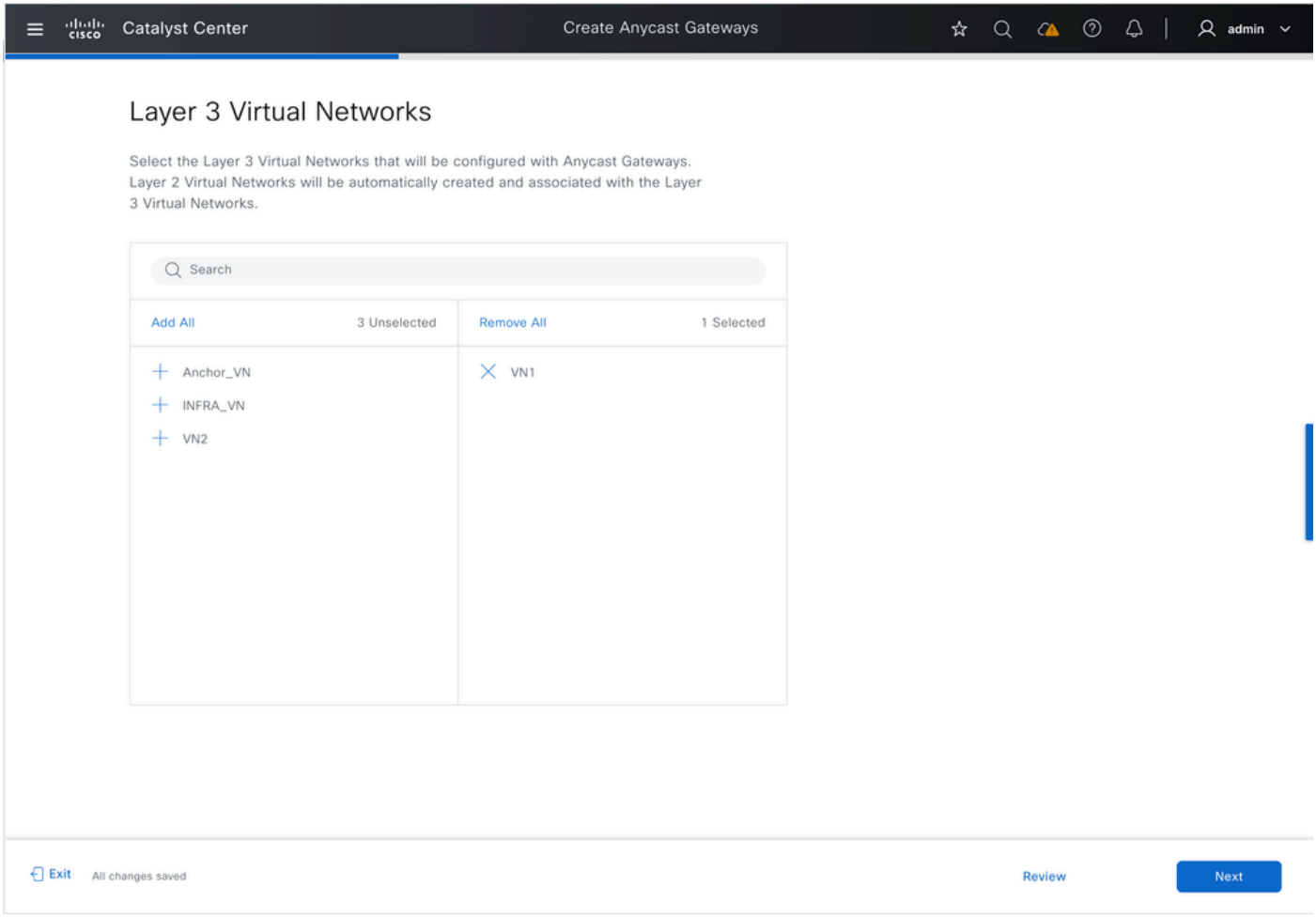
1. 转到Provision。
2. 选择交换矩阵站点。
3. 选择所需的站点。
4. 导航到任播网关。

您可以在此处配置IP定向广播所需的设置。



创建任播网关

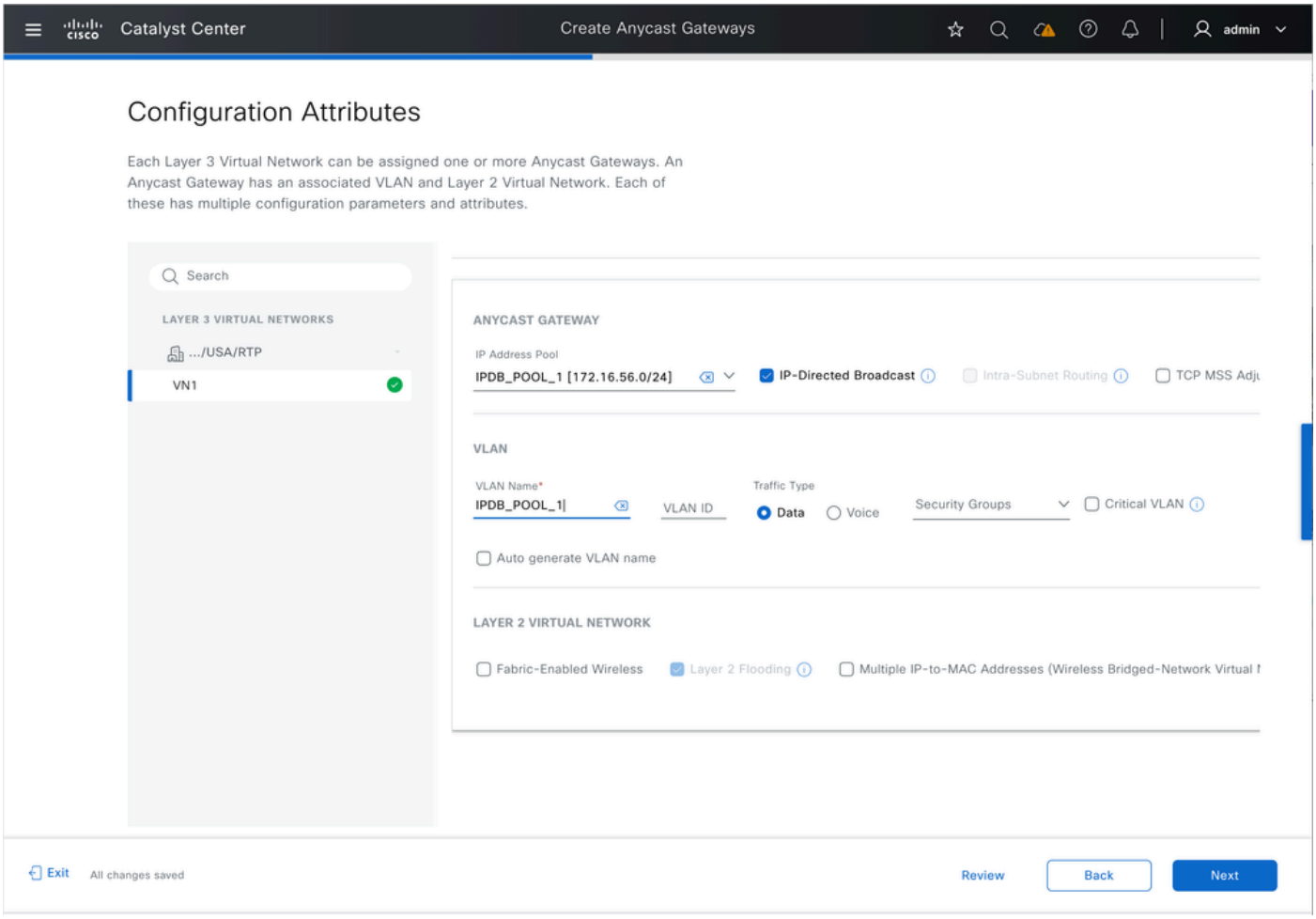
选择所需的L3虚拟网络，然后单击下一步继续。



选择L3虚拟网络

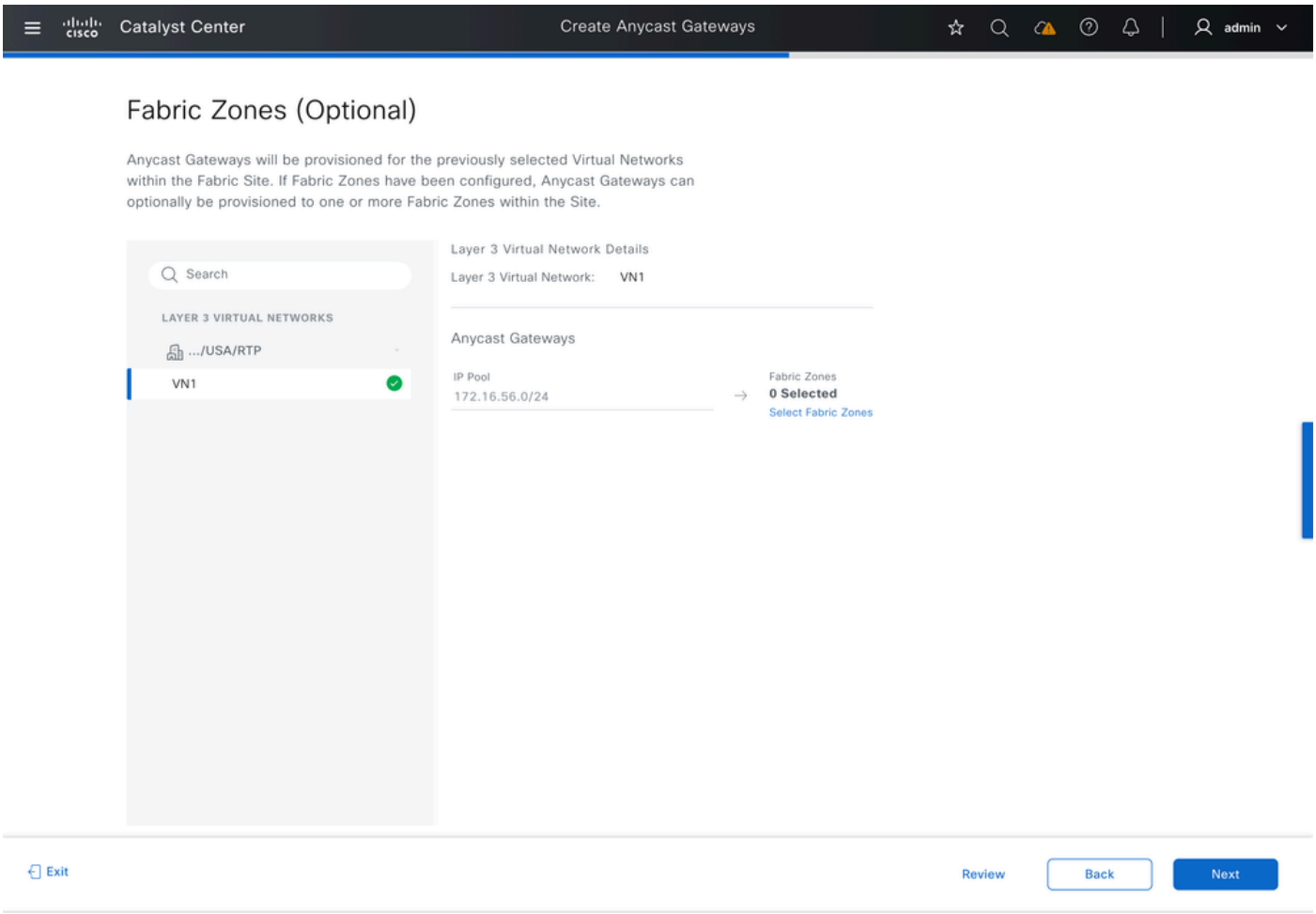
选择IP池，启用IP定向广播，然后输入VLAN名称。

提示：启用IP定向广播会自动激活L2泛洪。



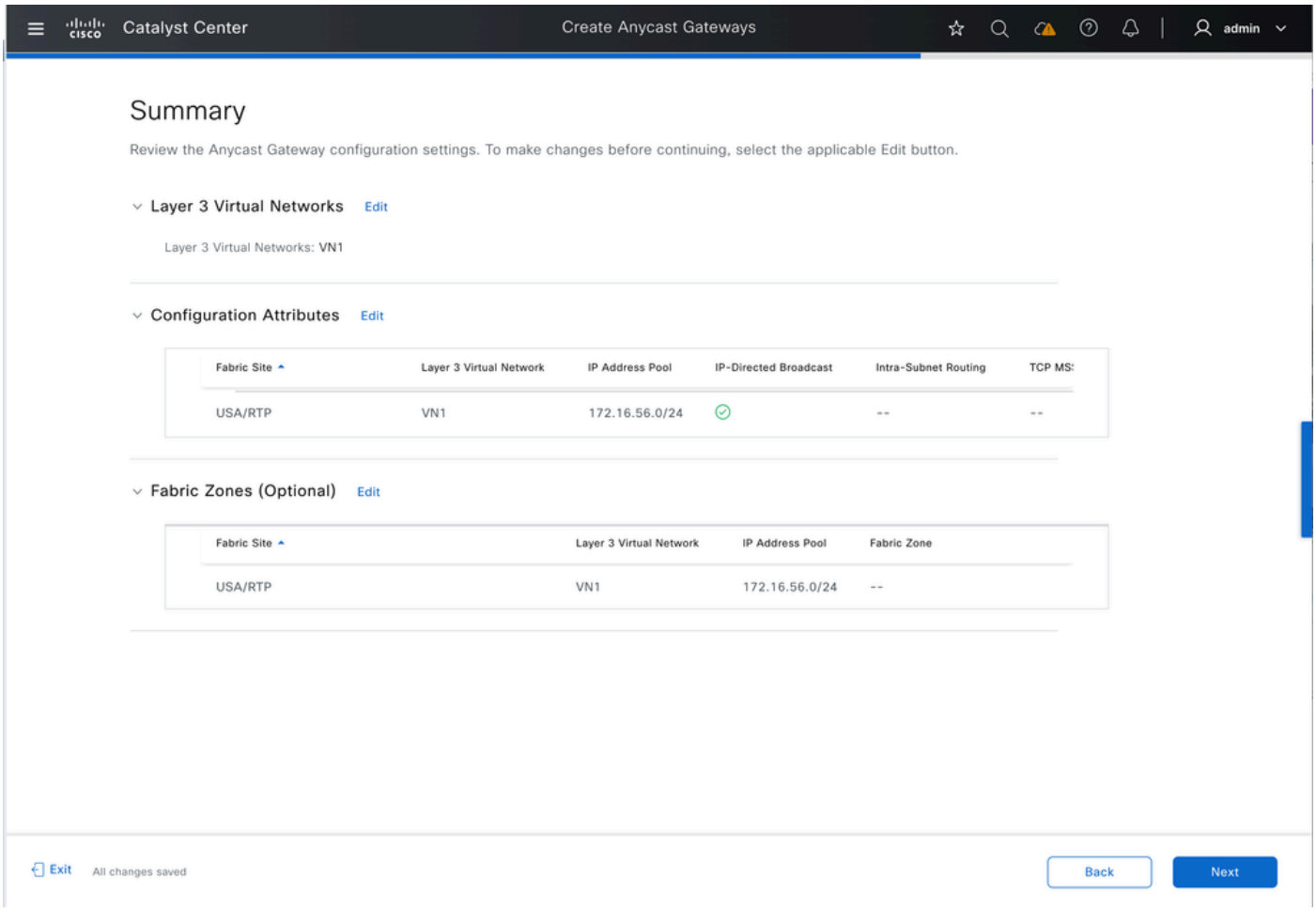
启用IP定向广播

如果存在交换矩阵区域，则可以选择将任播网关调配到站点内的一个或多个交换矩阵区域。



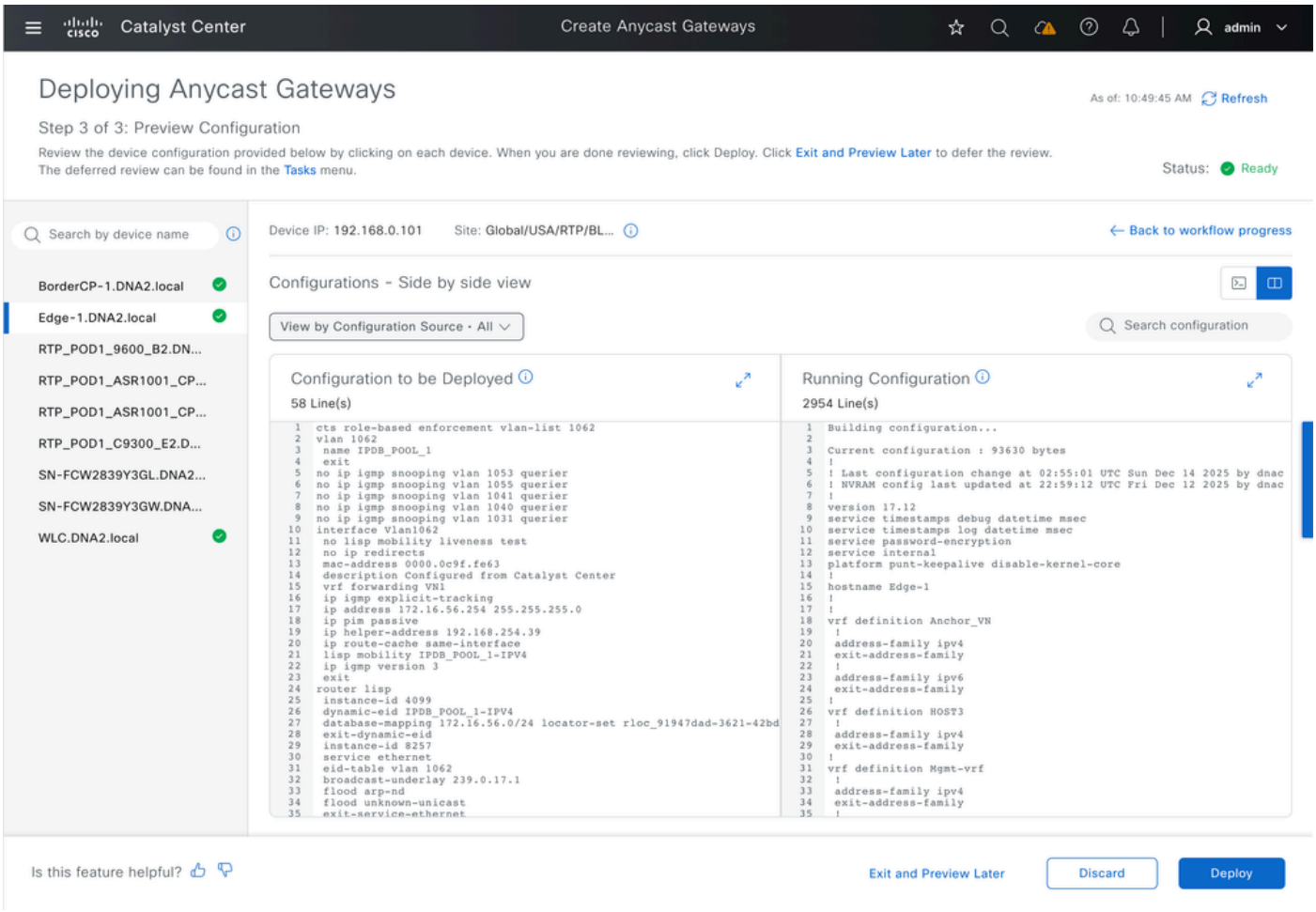
选择交换矩阵区域

在继续部署之前，请查看已配置设置的摘要以确认准确性。



摘要

预览生成的配置。单击Deploy将配置应用到交换矩阵。



配置预览

网络设备配置

边界配置 — IP传输

配置了IP Transit的交换矩阵边界将其BGP对等接口设置为“ip network-broadcast”，以允许转发IP子网广播。交换矩阵池（终端VLAN）的任播网关IP从环回接口更改为已启用“ip directed-broadcast”的SVI。交换矩阵边界需要这两种配置才能将IP子网广播数据包转换为完整广播，从而使该进程按预期运行。

IP网络广播和IP网络广播配置：

<#root>

vlan 1062

 name

IPDB_POOL_1

interface TenGigabitEthernet1/0/44 -- L3 Handoff Interface

switchport mode trunk

switchport trunk allowed vlan all

interface Vlan1062 -- Anycast Gateway interface, now converted to an SVI

no lisp mobility liveness test
no ip redirects
mac-address 0000.0c9f.fe63
description Configured from Catalyst Center

vrf forwarding VN1

ip address 172.16.56.254 255.255.255.0

ip helper-address 192.168.254.39
ip route-cache same-interface
lisp mobility IPDB_POOL_1-IPV4

ip directed-broadcast

-- Subnet broadcasts can be translated into full broadcasts

no autostate

--

Required to keep the SVI in up/up in absence of ports assigned to the VLAN

interface Vlan3002 -- BGP Peering interface, from IP Transit configuration

description vrf interface to External router
vrf forwarding VN1

ip address 192.168.10.5 255.255.255.252

no ip redirects

ip network-broadcast

--

Enabled on all L3 handoff SVIs on the VRF where the target VLAN belongs to

```
 ip pim sparse-mode
 ip route-cache same-interface
```

配置的第二部分使IP定向广播功能能够使用ARP请求（广播）唤醒静默主机，类似于传统网络在处理未知单播流量时的行为。通过此设置，交换矩阵外部的源可以使用标准单播流量唤醒终端，而不依赖于子网广播或LAN唤醒（“魔术数据包”）机制。

<#root>

```
router lisp
 prefix-list SITE_LOCAL_EIDS_V4
 172.16.56.0/24

instance-id 4099



dynamic-eid IPDB_POOL_1-IPV4



database-mapping 172.16.56.0/24 locator-set rloc_0f43c5d8-f48d-48a5-a5a8-094b87f3a5f7


instance-id 8257


   service ethernet
     eid-table vlan 1062

     broadcast-underlay 239.0.17.1

-- Enables Layer 2 Flooding to use BUM group 239.0.17.1


 flood arp-nd                  -- Enables the flooding of ARP requests with Layer 2 Flooding


 flood unknown-unicast
     database-mapping mac locator-set rloc_0f43c5d8-f48d-48a5-a5a8-094b87f3a5f7
ip dhcp snooping vlan 1062
```

边缘配置

交换矩阵边缘节点配置与启用了第2层泛洪的标准有线池的配置匹配。边缘节点上未显示“ip directed-broadcast”CLI命令。

<#root>

```
cts role-based enforcement vlan-list 1062
```

```
vlan 1062

 name
IPDB_POOL_1



interface Vlan1062


 no lisp mobility liveness test
 no ip redirects
 mac-address 0000.0c9f.fe63
 description Configured from Catalyst Center
 vrf forwarding VN1
 ip igmp explicit-tracking
ip address 172.16.56.254 255.255.255.0


 ip pim passive
 ip helper-address 192.168.254.39
 ip route-cache same-interface
 lisp mobility IPDB_POOL_1-IPV4
 ip igmp version 3

router lisp
 instance-id 4099
   dynamic-eid IPDB_POOL_1-IPV4
     database-mapping 172.16.56.0/24 locator-set rloc_91947dad-3621-42bd-ab6b-379ecebb5a2b
 instance-id 8257


   service ethernet


 eid-table vlan 1062



  broadcast-underlay 239.0.17.1


     flood arp-nd
     flood unknown-unicast
   remote-rloc-probe on-route-change
 instance-id-range 8240 , 8245 , 8249 , 8254 , 8256 -
8257

 override
  remote-rloc-probe on-route-change
  service ethernet

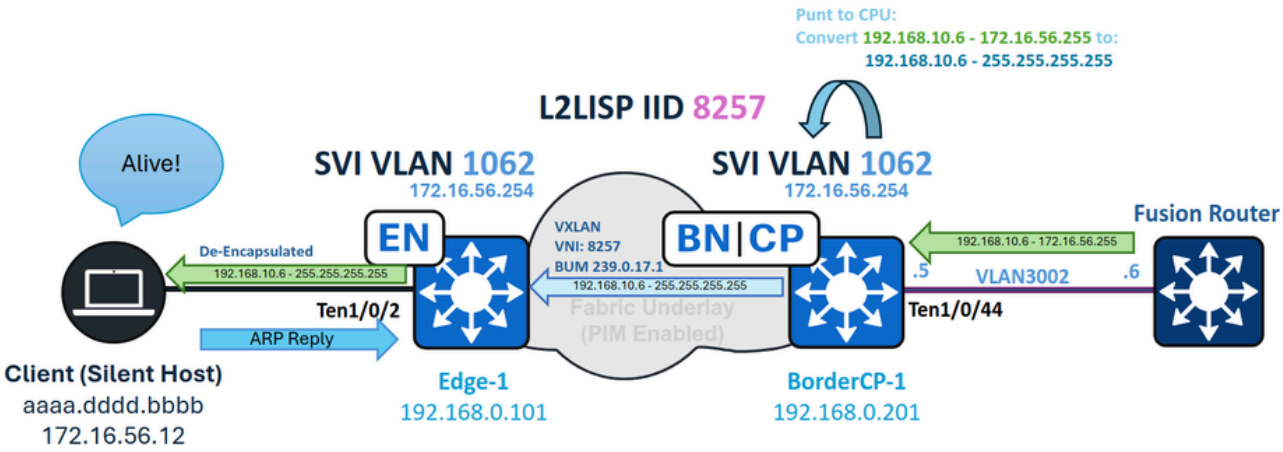

eid-table vlan

 1041 , 1048 , 1053 , 1059 , 1061 -
1062
```

```
    database-mapping mac locator-set rloc_91947dad-3621-42bd-ab6b-379ecebb5a2b

 ip dhcp snooping vlan 1062
```

IP定向广播转发



IPDB转发

边界 — 入口CPU分支和子网广播转换

在本示例中，目的IP为172.16.56.255(地址池172.16.56.0/24的广播地址)的IP子网广播从外部网络路由，首先到达交换矩阵边界。入口第3层接口是IP传输SVI(VLAN 3002)。 由于该接口上启用了“ip network-broadcast”，因此数据包被接受进行完全广播转换；如果没有此配置，数据包将被丢弃。

数据包到达SVI 3002，作为广播数据包被传送到交换机CPU。配置了IP network-broadcast后，允许数据包并将其转换为完整广播。

<#root>

```
BorderCP-1#show run interfave Vlan3002



interface Vlan3002
  vrf forwarding VN1
  ip address 192.168.10.5 255.255.255.252
  ip network-broadcast

BorderCP-1#show ip cef vrf VN1 172.16.56.255
172.16.56.255/32
   receive for Vlan1062       --- The routing result is "receive", indicating that the packet undergoes
```

在CPU处理期间，VLAN 1062（目标接口）将数据包转换为完整广播，因为它配置了“ip directed-broadcast”。

<#root>

BorderCP-1#show ip interface vlan 1062 | i Directed

Directed broadcast forwarding is enabled

您可以使用debug ip packet命令对此事件进行故障排除。为避免输出过度和资源使用率过高，请始终在运行此调试时应用访问列表作为过滤器。

<#root>

ip access-list standard 10

10 permit

192.168.10.6   --- Directed Broadcast source IP

BorderCP-1#debug ip packet detail 10

IP:

s=192.168.10.6 (Vlan3002)

,

d=172.16.56.255

(nil), len 100,

input feature

```
ICMP type=8, code=0, MCI Check(110), rtype 0, forus FALSE, sendself FALSE, mtu 0, fwdchk FALSE
IP: s=192.168.10.6 (Vlan3002), d=172.16.56.255 (nil), len 100, input feature
ICMP type=8, code=0, Role-based Proxy(116), rtype 0, forus FALSE, sendself FALSE, mtu 0, fwdchk FALSE

FIBipv4-packet-proc: route packet from Vlan3002 src 192.168.10.6 dst 172.16.56.255



FIBfwd-proc: VN1:172.16.56.255/32 receive entry


FIBipv4-packet-proc: packet routing failed

IP: tableid=3, s=192.168.10.6 (Vlan3002), d=172.16.56.255 (Vlan1062) nexthop=172.16.56.255, routed via F


IP: s=192.168.10.6 (Vlan3002), d=172.16.56.255 (Vlan1062), len 100, output feature
ICMP type=8, code=0, feature skipped, Role-based Access List(53), rtype 1, forus FALSE, sendself FALSE,

IP: s=192.168.10.6 (Vlan3002), d=172.16.56.255 (Vlan1062), g=255.255.255.255, len 100, forward directed
```

入口边界用作BUM封装的组播源(S)和组(G)，使用其Loopback 0作为源地址，配置的BUM组作为目标。

在PIM控制平面上，确保指向交换矩阵边缘的下行链路出现在组播路由的传出接口列表中。对于数据平面，请使用show ip mfib count命令验证边界上的S、G条目的硬件转发计数器是否增加。

<#root>

```
BorderCP-1#show ip mroute 239.0.17.1 192.168.0.201 | be \(

(
192.168.0.201
,
239.0.17.1
), 5w0d/00:02:33, flags: FTA

Incoming interface: Null0
, RPF nbr 0.0.0.0
 Outgoing interface list:

TenGigabitEthernet1/0/42
```

```
, Forward/Sparse, 2d09h/00:03:23, flags:
```

-- Downlink to Fabric Edge or Intermediate Node

BorderCP-1#show ip mfib 239.0.17.1 192.168.0.201 count

```
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kilobits per second
Other counts: Total/RPF failed/Other drops(OIF-null, rate-limit etc)
Default
  16 routes, 6 (*,G)s, 3 (*,G/m)s
```

Group: 239.0.17.1

Source: 192.168.0.201,

```
    SW Forwarding: 1/0/130/0, Other: 0/0/0
```

HW Forwarding: 2124804

```
/0/116/0, Other: 0/0/0
 Totals - Source count: 1, Packet count: 2124805
Groups: 1, 1.00 average sources per group
```

本文档不深入解释底层组播树形成或第2层泛洪。如果缺少、不完整或错误的S、G状态，则网络蠕虫的底层组播部分需要独立的故障排除。

边缘 — 入口广播

在交换矩阵边缘上，组播上封装在VXLAN中的传入广播被解封装并转发到与VNI(8257)关联的VLAN，到达所有端口在生成树中处于转发状态。

首先，验证来自BUM组的边界（以边界环回作为源）的S，G条目存在，并转发流量。使用相同的mroute和mfib命令检查此情况，确保与VLAN(1062)对应的L2LISP子接口列为传出接口。

<#root>

Edge-1#show ip mroute 239.0.17.1 192.168.0.201 | be \(
(192.168.0.201, 239.0.17.1),

```
 2d09h/00:01:10, flags: JT
```

Incoming interface: TenGigabitEthernet1/1/2,

```
 RPF nbr 192.168.98.2
```

Outgoing interface list:

L2LISP0.8257

, Forward/Sparse-Dense, 2d09h/00:02:21, flags:

Edge-1#show ip mfib 239.0.17.1 192.168.0.201 verbose | be Forwarding

```
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts: Total/RPF failed/Other drops
I/O Item Counts: HW Pkt Count/FS Pkt Count/PS Pkt Count Egress Rate in pps
Default
```

(192.168.0.201,239.0.17.1)

```
 Flags: K HW DDE
   0x12C OIF-IC count: 0, OIF-A count: 1
   SW Forwarding: 2/0/402/0, Other: 0/0/0
```

HW Forwarding: 145023

```
/0/128/0, Other: 0/0/0
   TenGigabitEthernet1/1/2 Flags: RA A MA
```

L2LISP0.8257

,

L2LISP Decap Flags: RF F NS

```
      CEF: OCE (lisp decap)
      Pkts: 0/0/2 Rate: 0 pps
```

解封后，数据包在VLAN 1062上转发到分配给该VLAN的所有端口。

<#root>

Edge-1#show spanning-tree vlan 1062

VLAN1062

```
  Spanning tree enabled protocol rstp
  Root ID      Priority 33830
               Address 00b1.e331.d580
               This bridge is the root
```

```
               Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

   Bridge ID   Priority 33830 (priority 32768 sys-id-ext 1062)
               Address 00b1.e331.d580
               Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
               Aging Time 300 sec

Interface           Role Sts Cost      Prio.Nbr  Type
------------------- ---- --- --------- -------- --------------------------------

Te1/0/2             Desg FWD 20000     128.3     P2p Edge



Po1                 Desg FWD 20000     128.3049  P2p
```

终端收到广播数据包后，必须将该数据包识别为相关信息并做出响应。因此，终端可以发送ARP数据包，更新交换机上的设备跟踪表。

<#root>

```
Edge-1#show device-tracking database interface Te1/0/2 | be Network

    Network Layer Address Link Layer Address Interface vlan prlvl age state     Time left


ARP 172.16.56.12           aaaa.dddd.bbbb     Te1/0/2   1062 0005   0s REACHABLE 241 s
```

在设备跟踪中重新注册终端后，将其导入到边缘节点的LISP数据库中，然后注册到控制平面。

对于LISP Pub-Sub部署，控制平面将新注册的终端信息发布到边界，即时创建LISP映射缓存条目以将流量转发到适当的边缘节点。

<#root>

```
BorderCP-1#show lisp instance-id 4099 ipv4 map 172.16.56.12/32

LISP IPv4 Mapping Cache for LISP 0 EID-table vrf VN1 (IID 4099), 1 entries

172.16.56.12/32

, uptime: 5w0d, expires: never,

via pub-sub

,
```

```
complete

, local-to-site
 SGT: 2

 Sources: pub-sub


 State: complete, last modified: 5w0d, map-source: local
 Exempt, Packets out: 6(2432 bytes), counters are not accurate (~ 5w0d ago)
 Configured as EID address space


Locator

       Uptime

State

 Pri/Wgt Encap-IID


192.168.0.101

 5w0d

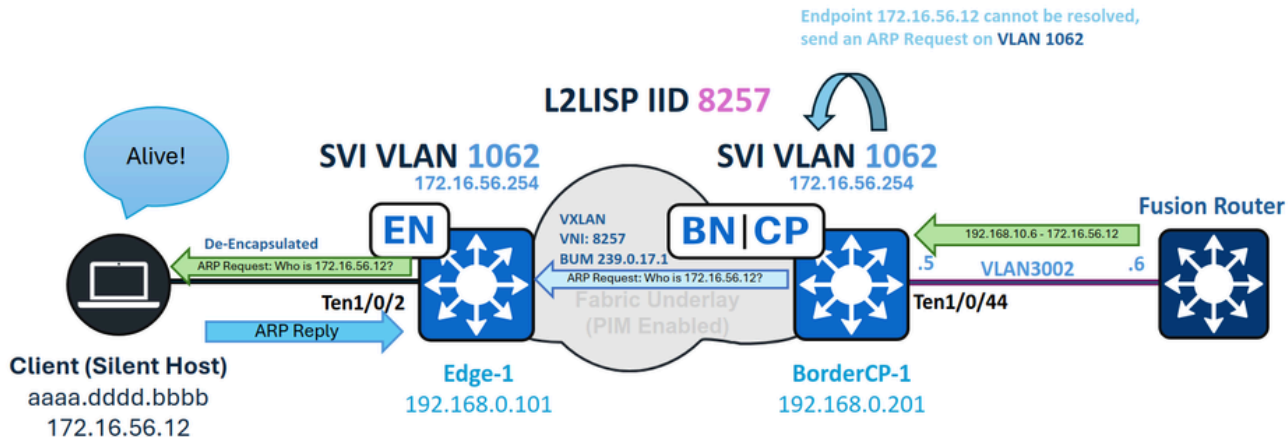
up

    10/10    -
  Last up-down state change: 5w0d, state change count: 1
  Last route reachability change: 5w0d, state change count: 1
  Last priority / weight change: never/never
  RLOC-probing loc-status algorithm:
    Last RLOC-probe sent: 00:22:19 (rtt 4ms)
```

对于LISP/BGP(SDA 1.0)部署，如果部署是分布式（未配置），更新未知终端的LISP映射缓存最多可能需要一分钟，因为负映射回复(NMR)必须首先过期。

如果静默主机没有设定响应数据包的程序，则必须忽略数据包（如子网广播）。某些终端需要“魔术数据包”（例如UDP回应），而其他终端仅响应广播ARP。静默主机本身决定哪种类型的数据包会触发它唤醒。在最常见的选项中，通常首选ARP请求，如未知单播转发部分所述。

未知单播转发



未知单播转发

当为IP定向广播启用地址池时，它不仅允许处理子网广播，还允许交换矩阵边界充当转发未知单播流量的网关。在这种情况下，未知单播流量是指发往当前未在控制平面中注册的终端的数据包。

类似于传统网络网关在遇到不完整的ARP条目时发送ARP请求，边界会生成ARP请求并将其泛洪到所有交换矩阵节点。这可以确保静默主机接收请求、唤醒并发送ARP应答，从而在控制平面中重新注册自己。

此功能之所以可行，是因为终端VLAN(1062)在交换矩阵边界上同时配置为SVI和L2LISP实例。在L2 IID中启用“flood arp-nd”后，边界可以在流量流向未知LISP EID时泛洪SVI生成的ARP请求，确保静默主机收到ARP请求并有机会响应并更新其在控制平面中的注册。

<#root>

```
BorderCP-1#show vlan id 1062

VLAN Name        Status Ports
---- ----------------------------------------

1062


IPDB_POOL_1

 active

L2LI0:8257

,

Te1/0/44

BorderCP-1#show run | se 8257


instance-id 8257


 remote-rloc-probe on-route-change
  service ethernet
```

eid-table vlan 1062

broadcast-underlay 239.0.17.1

flood arp-nd

flood unknown-unicast
database-mapping mac locator-set rloc_0f43c5d8-f48d-48a5-a5a8-094b87f3a5f7

当交换矩阵边界收到发往SVI 3002（终端VN/VRF的一部分）上的172.16.56.12的数据包时，它将尝试LISP解析，因为CEF输出设置为“收集”（表示设备尝试使用下游层协议解析目标邻接）。 此过程同时触发未注册（静默）主机的LISP映射请求和ARP解析。

<#root>

BorderCP-1#show lisp instance-id 4099 ipv4 map-cache 172.16.56.12

LISP IPv4 Mapping Cache for LISP 0 EID-table vrf VN1 (IID 4099), 1 entries

172.16.56.0/24,

uptime: 00:00:30, expires: never, via dynamic-EID, send-map-request, local-to-site
Sources: NONE
State:

send-map-request

, last modified: 00:00:30, map-source: local
Exempt, Packets out: 2(1152 bytes), counters are not accurate (~ 2d15h ago)
Configured as EID address space
Configured as dynamic-EID address space
Encapsulating dynamic-EID traffic
Negative cache entry, action:

send-map-request -- LISP Resolution attempted

<#root>

BorderCP-1#show ip cef vrf VN1 172.16.56.12

172.16.56.0/24

attached to LISP0.4099

BorderCP-1#show ip cef vrf VN1 172.16.56.12 internal | se output chain:

output chain:
PushCounter(LISP:172.16.56.0/24) 766CBD050CF0

glean for LISP0.4099

创建不完整的ARP条目，提示边界向未知终端172.16.56.12发送ARP请求。此ARP请求作为广播数据包使用第2层泛洪和泛洪ARP-ND功能向下游转发。

要验证第2层泛洪是否正常运行，请监控边界本地S、G的MFIB计数器。

<#root>

BorderCP-1#show ip mroute 239.0.17.1 192.168.0.201 | be \(

(

192.168.0.201

,

239.0.17.1

), 5w0d/00:02:33, flags: FTA

Incoming interface: Null0

, RPF nbr 0.0.0.0
 Outgoing interface list:

TenGigabitEthernet1/0/42

, Forward/Sparse, 2d09h/00:03:23, flags:

-- Downlink to Fabric Edge or Intermediate Node

BorderCP-1#show ip mfib 239.0.17.1 192.168.0.201 count

Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kilobits per second
Other counts: Total/RPF failed/Other drops(OIF-null, rate-limit etc)
Default
  16 routes, 6 (*,G)s, 3 (*,G/m)s

Group: 239.0.17.1

Source: 192.168.0.201,

SW Forwarding: 1/0/130/0, Other: 0/0/0

HW Forwarding: 2124804

/0/116/0, Other: 0/0/0
Totals - Source count: 1, Packet count: 2124805
Groups: 1, 1.00 average sources per group

泛洪的ARP数据包到达静默主机，唤醒它并提示ARP应答。此响应更新交换矩阵边缘上的设备跟踪(SISF)表并创建LISP数据库条目。因此，交换矩阵边缘会启动到控制平面的注册。

<#root>

Edge-1#show device-tracking database interface Te1/0/2 | be Network

Network Layer Address Link Layer Address Interface vlan prlvl age state Time left

ARP 172.16.56.12 aaaa.dddd.bbbb Te1/0/2 1062 0005 0s REACHABLE 241 s

在设备跟踪中重新注册终端后，将其导入到边缘节点的LISP数据库中，然后注册到控制平面。

对于LISP Pub-Sub部署，控制平面将新注册的终端信息发布到边界，即时创建LISP映射缓存条目以将流量转发到适当的边缘节点。

<#root>

BorderCP-1#show lisp instance-id 4099 ipv4 map 172.16.56.12/32

LISP IPv4 Mapping Cache for LISP 0 EID-table vrf VN1 (IID 4099), 1 entries

172.16.56.12/32

, uptime: 5w0d, expires: never,

via pub-sub

,

complete

, local-to-site
SGT: 2

Sources: pub-sub

State: complete, last modified: 5w0d, map-source: local

```
 Exempt, Packets out: 6(2432 bytes), counters are not accurate (~ 5w0d ago)
 Configured as EID address space


Locator

       Uptime

State

 Pri/Wgt Encap-IID


192.168.0.101

 5w0d

up

    10/10    -
  Last up-down state change: 5w0d, state change count: 1
  Last route reachability change: 5w0d, state change count: 1
  Last priority / weight change: never/never
  RLOC-probing loc-status algorithm:
    Last RLOC-probe sent: 00:22:19 (rtt 4ms)
```

对于LISP/BGP(SDA 1.0)部署，如果部署是分布式（未配置），更新未知终端的LISP映射缓存最多可能需要一分钟，因为负映射回复(NMR)必须首先过期。



提示：边界不会解析静默主机的ARP;仅需要终端注册。当无提示主机应答时，ARP数据包将作为第2层单播发送，因此不会向边界泛洪。因此，不要期望在边界上看到ARP条目或设备跟踪条目。

在身份验证模板中启用LAN唤醒

当交换矩阵用户启用了No Authentication（无身份验证）时，只要端口是启用泛洪的VLAN的一部分，边界泛洪数据包就会到达静默主机；但是，对于封闭式身份验证（尤其是封闭式身份验证），两个主要因素变得很重要。

身份验证前为主机手动分配VLAN

如果未分配VLAN，则端口不会接收来自其指定VLAN的泛洪数据包。当预期由RADIUS分配VLAN时，会创建“鸡还是蛋？”困境：泛洪数据包无法转发到其他VLAN（通常称为VLAN跳跃），以触发用户身份验证并从RADIUS获取VLAN分配。

在主机自注册中配置端口时，如果设备标识为“静默”，则使用数据池的下拉菜单手动分配VLAN。

在VLAN分配之前，静默主机无法进行身份验证的问题不是SD-Access独有的问题；这是任何传统安全网络中都存在的常见设计挑战。

<#root>

```
interface TenGigabitEthernet1/0/2



 switchport access vlan 1062



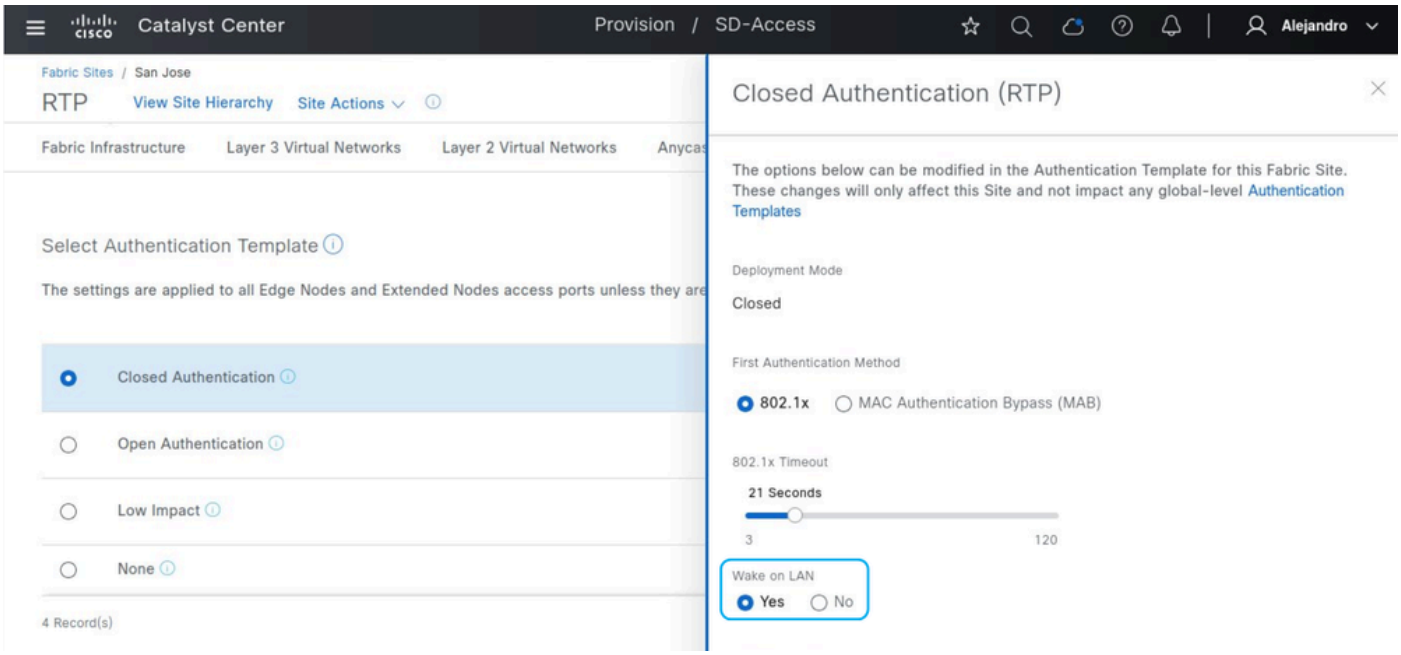
 switchport mode access
 device-tracking attach-policy IPDT_POLICY
 dot1x timeout tx-period 7
 dot1x max-reauth-req 3


source template DefaultWiredDot1xClosedAuth


 spanning-tree portfast
 spanning-tree bpduguard enable
```

访问控制方向

默认情况下，如果在主机自注册中的身份验证模板设置中未启用LAN唤醒，则身份验证模板使用“access-session control-direction both”。 此配置导致端口丢弃传入数据包和将从端口转发出来的数据包。启用LAN唤醒后，设置更改为“access-session control-direction in”，仅限制入口流量。此调整允许数据包到达并唤醒静默主机，使其能够启动MAB身份验证。



LAN唤醒

不使用LAN唤醒：

<#root>

```
Edge-1#show run all | se template DefaultWiredDot1xClosedAuth
template DefaultWiredDot1xClosedAuth


 dot1x pae authenticator
 dot1x timeout supp-timeout 7
 dot1x max-req 3
 switchport mode access
 switchport voice vlan 2046
 mab radius
 access-session host-mode multi-auth
 access-session
 control-direction both


 access-session
closed


access-session port-control auto


Edge-1#show authentication session interface Te1/0/2 detail | i Oper
Oper host mode: multi-auth

Oper control dir: both
Oper host mode: multi-auth
```

```
Oper control dir: both
```

在终端进行身份验证之前，分配给它的接口在生成树状态中不会列为已启用泛洪。

<#root>

```
Edge-1#show spanning-tree interface Te1/0/2


no spanning tree info available for TenGigabitEthernet1/0/2
```

启用LAN唤醒后：

<#root>

```
Edge-1#show run | se template DefaultWiredDot1xClosedAuth
template DefaultWiredDot1xClosedAuth


 dot1x pae authenticator
 dot1x timeout supp-timeout 7
 dot1x max-req 3
 switchport mode access
 switchport voice vlan 2046
 mab
 access-session control-direction in


 access-session closed


 access-session port-control auto


Edge-1#show authen session interface Te1/0/2 de | i Oper

Oper host mode: multi-auth
Oper control dir: in

Oper host mode: multi-auth
Oper control dir: in
```

即使在身份验证之前，端口也会启用出口流量，允许数据包到达和唤醒静默主机。

<#root>

```
Edge-1#show spanning-tree interface TenGigabitEthernet 1/0/2

Vlan                Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------

VLAN1062

            Desg

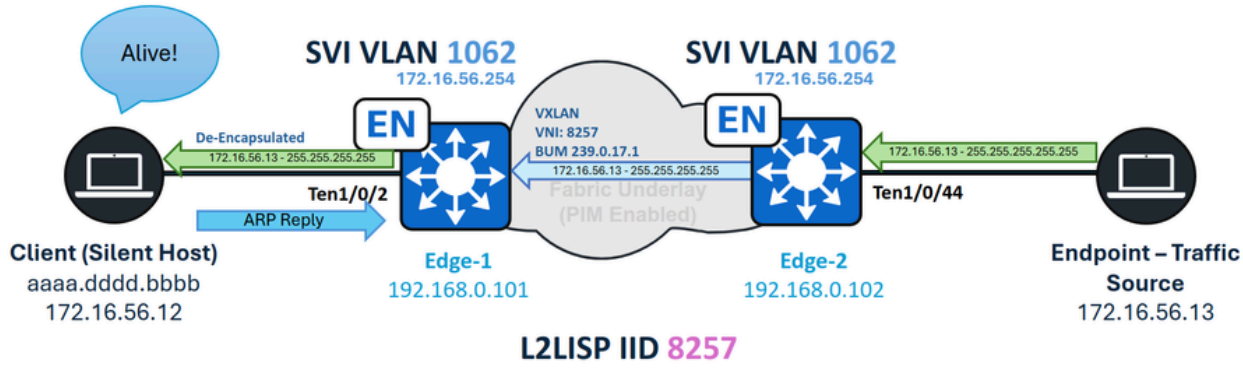
FWD

 19        128.2    P2p Edge
```

替代方案

边缘节点和相同VLAN — 第2层泛洪

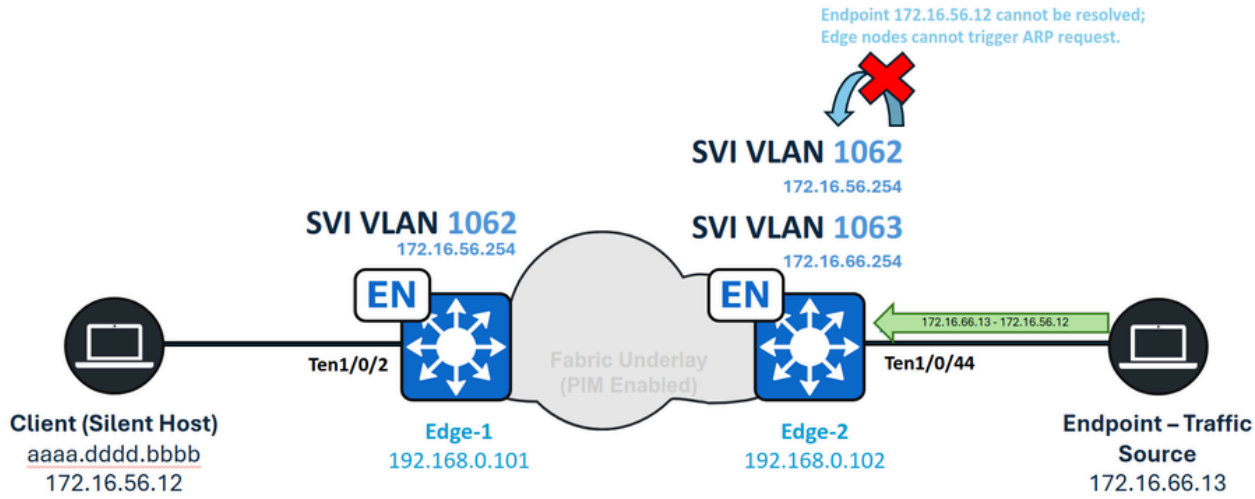
如果目标是从与主机位于相同VLAN的交换矩阵中的设备唤醒静默主机，则不需要IP定向广播功能。相反，启用第2层泛洪（在非无线池中）足以允许交换广播数据包、子网广播或ARP请求。对于封闭式身份验证，LAN唤醒要求保持不变。



相同VLAN — 静默主机处理

边缘节点和不同VLAN — 未知单播

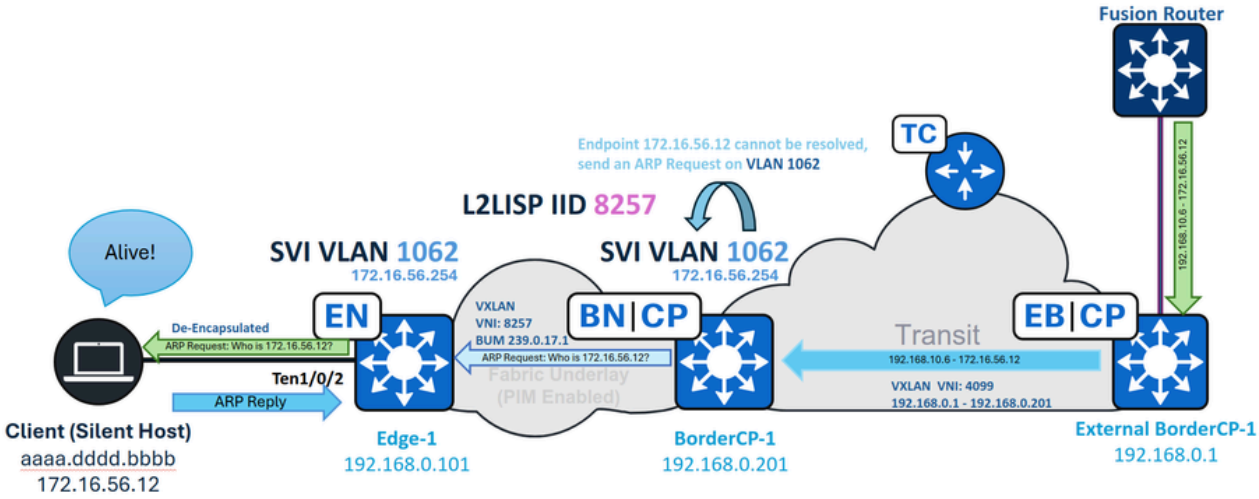
当交换矩阵内的终端向连接到交换矩阵边缘节点的静默主机发送单播流量时，未知单播转发路径不可用。与交换矩阵边界不同，交换矩阵边缘节点具有定义为LISP代理ETR的边界，当检测到未知终端时，该边界会自动启用称为“信号与转发”的转发功能。交换矩阵边缘必须在第一次尝试解析地址时触发所需的ARP请求。但是，一旦LISP将终端识别为未知EID，后续数据包就不会触发其他ARP请求。此场景被视为不受支持。



未知单播VLAN间

SD访问传输 — 未知单播

对于SD-Access Transit，本地支持未知单播流量，没有任何特殊要求。源自远程边界的流量通过SD-Access Transit网络路由，子网广播被视为常规路由流量。当流量到达本地站点边界时，将执行标准操作，包括流量收集、ARP请求泛洪和LISP解析。

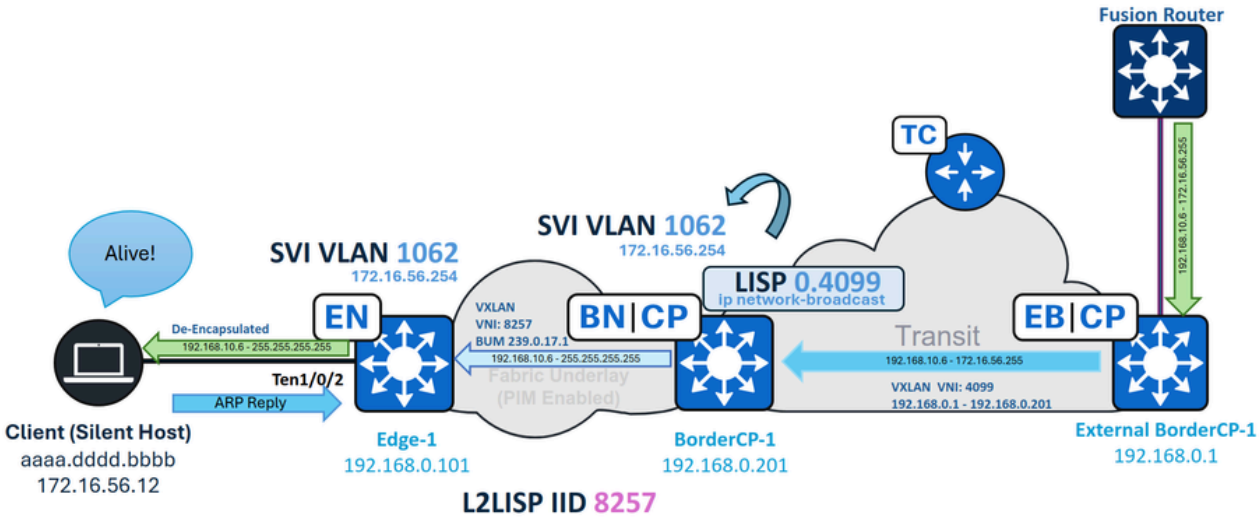


SD访问传输未知单播

SD访问传输 — IP定向广播

当使用SD-Access Transit时，本地站点边界在VN的LISP子接口（例如，接口4099）上接收IP定向广播，而不是在SVI上。要确保通过IP定向广播功能接受广播并将其转换为子网广播，您必须在

LISP子接口上手动配置“ip network-broadcast”参数。



SD访问传输IPDB

在BorderCP-1（本地站点边界）上：

```
interface LISP0.4099
  ip network-broadcast
```

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）。