

使用本地终端排除ACI中的DHCP中继故障

目录

[简介](#)

[缩写](#)

[要求](#)

[使用的组件](#)

[故障排除建议](#)

[终端学习](#)

[策略部署](#)

[主机可达性](#)

[终端学习和路由](#)

[策略验证](#)

[DHCP数据包跟踪](#)

[常见问题](#)

[问题 1:L3out silent drop](#)

[问题 2:DHCP服务器不支持选项82](#)

[参考](#)

简介

本文档介绍ACI交换矩阵中DHCP中继的故障排除。

缩写

- BD:网桥域
- EPG:终端组
- ExEPG:外部终端组
- VRF:虚拟路由和转发
- 类ID或pcTag:标识EPG的标记
- DHCP:动态主机配置协议
- SVI:交换虚拟接口

要求

对于本文而言，建议您了解以下主题的一般知识：

- DHCP概念和工作流程（DORA进程）
- ACI概念：访问策略、终端学习、合同和L3out
- 必须已创建DHCP中继策略

使用的组件

此故障排除练习是在ACI版本6.0(8f)上进行的，使用第二代Nexus交换机N9K-C93180YC-EX和N9K-C93240YC-FX2。

本文中的所有命令均在实验室环境中运行，并使用RFC1819进行IP编址。如果您的网络是活动的，请确保您了解任何命令的潜在影响，确保您根据特定需要充分利用所讨论的命令。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

故障排除建议

终端学习

如果未获知终端，请验证静态端口策略，如交换机、接口和VLAN配置。对于虚拟服务器，请确认端口组已正确部署并分配到VM。

策略部署

确保DHCP中继策略(dhcpRelayP)和DHCP中继标签(dhcpLbl)已正确配置并由相应的网桥域(BD)使用。 标签策略的所有权规则如下：

- 用户租户所有权：只有该租户可以使用策略
- 公共租户所有权：所有租户都可以使用该策略，但必须在公共EPG上获取DHCP服务器
- Infra租户所有权：所有租户都可以使用该策略，DHCP服务器可以在交换矩阵的任何位置获取

如果dhcpRelayP父策略下缺少dhcpRtLblDefToRelayP子类，则没有BD正在使用中继策略，因此需要执行纠正操作。

主机可达性

DHCP客户端必须可从其BD的SVI访问。如果无法访问，请验证合同和路由配置以确保连接。

终端学习和路由

确保可从客户端所在的网桥域的SVI访问DHCP服务器。

```
<#root>
```

```
iping -V [ tenant : VRF ] -S [ SVI IP of the Client ] [ DHCP server IP]
```

```
<#root>
```

```
Leaf101#
```

```
iping -V tz:VRF1 -S 172.16.19.1 172.16.18.100
```

```
PING 172.16.18.100 (172.16.18.100) from 172.16.19.1: 56 data bytes
64 bytes from 172.16.18.100: icmp_seq=0 ttl=64 time=0.912 ms
64 bytes from 172.16.18.100: icmp_seq=1 ttl=64 time=0.706 ms
64 bytes from 172.16.18.100: icmp_seq=2 ttl=64 time=0.643 ms
64 bytes from 172.16.18.100: icmp_seq=3 ttl=64 time=0.689 ms
64 bytes from 172.16.18.100: icmp_seq=4 ttl=64 time=0.717 ms
```

```
--- 172.16.18.100 ping statistics ---
```

```
5 packets transmitted, 5 packets received, 0.00% packet loss
```

```
round-trip min/avg/max = 0.643/0.733/0.912 ms
```

在EPG下配置时，DHCP客户端和DHCP服务器都必须获知为终端。要验证这些终端是否正确获取，您可以检查枝叶上的终端管理器表。

```
<#root>
```

```
show system internal epm endpoint [ip | mac] [ DHCP server IP | DHCP client MAC]
```

```
<#root>
```

```
Leaf101# show system internal epm endpoint ip 172.16.18.100
```

```
MAC : 0050.56b7.80cf ::: Num IPs : 1
```

```
IP# 0 : 172.16.18.100
```

```
::: IP# 0 flags : ::: l3-sw-hit: No
Vlan id : 12 ::: Vlan vnid : 8535 ::: VRF name : tz:VRF1
BD vnid : 15400880 ::: VRF vnid : 2981888
Phy If : 0x1a02c000 ::: Tunnel If : 0
Interface : Ethernet1/45
Flags : 0x80004c04 ::: sclass : 16402 ::: Ref count : 5
EP Create Timestamp : 09/11/2025 17:37:15.158380
EP Update Timestamp : 09/11/2025 19:17:41.261985
EP Flags : local|IP|MAC|sc|timer|
```

```
:::
```

```
...
```

```
Leaf101# show system internal epm endpoint mac 0050.56b7.33ee
```

```
MAC : 0050.56b7.33ee ::: Num IPs : 0
```

```
Vlan id : 25 ::: Vlan vnid : 8494 ::: VRF name : tz:VRF1
BD vnid : 15630228 ::: VRF vnid : 2981888
Phy If : 0x1a02c000 ::: Tunnel If : 0
Interface : Ethernet1/45
Flags : 0x80004804 ::: sclass : 32780 ::: Ref count : 4
EP Create Timestamp : 09/11/2025 17:33:36.158122
```

EP Update Timestamp : 09/11/2025 19:17:41.258478
EP Flags : local|MAC|sclass|timer|

::::

策略验证

验证DHCP中继策略时，可以确认以下关键属性：

- 名称：DHCP中继策略的标识符。
- 所有者：配置策略的租户，表示其可视性范围仅限于该租户。
- 地址：将DHCP请求中继到的DHCP服务器的IP地址。
- DHCP服务器的位置：通过标记（如epgDn、bdDefDn和ctxDefDn）进行验证，以确保与EPG、网桥域和VRF的正确关联。
- 策略状态：策略必须处于已形成的状态，表示已在交换矩阵中正确部署并处于活动状态。

通过在APIC上运行moqueries来执行此验证，以确认正确创建了DHCP中继策略，将其与适当的租户相关联，并正确链接到相关的网桥域。此步骤有助于及早识别错误配置，防止因策略部署缺失或不正确而导致DHCP中继失败。

<#root>

```
moquery -c dhcpRelayP -f 'dhcp.RelayP.dn*"[ tenant name ].*[ DHCP Relay Policy name ]"' -x rsp-subtree=
```

<#root>

APIC#

```
moquery -c dhcpRelayP -f 'dhcp.RelayP.dn*"tz.*Relay"' -x rsp-subtree=children
```

Total Objects shown: 1

dhcp.RelayP

name : tz-DHCP_Relay

<-- cut for brevity-->

dn : uni/tn-tz/relayp-tz-DHCP_Relay

<-- cut for brevity-->

owner : tenant

<-- cut for brevity-->

rn : relayp-tz-DHCP_Relay

dhcp.ProvDhcp

epgDn : uni/tn-tz/ap-AP1/epg-EPG1

addr : 172.16.18.100

bdDefDn : uni/bd-[uni/tn-tz/BD-BD1]-isSvc-no

<-- cut for brevity-->

ctxDefDn : uni/ctx-[uni/tn-tz/ctx-VRF1]

ctxDefStQual : none

ctxSeg : 2981888

descr :

dn : uni/tn-tz/relayp-tz-DHCP_Relay/provdhcp-[uni/tn-tz/ap-AP1/epg-EPG1]

l3CtxEncap : vxlan-2981888

<-- cut for brevity-->

name : EPG1

<-- cut for brevity-->

pcTag : 16402

<-- cut for brevity-->

dhcp.RsProv

tDn : uni/tn-tz/ap-AP1/epg-EPG1

addr : 172.16.18.1

<-- cut for brevity-->

state : formed

一旦DHCP中继策略与客户端的网桥域(BD)关联，就会自动创建相应的DHCP标签策略。此DHCP标签策略充当DHCP中继策略和BD之间的链接，从而启用中继功能。

您可以使用APIC CLI使用以下命令验证DHCP标签策略：

<#root>

moquery -c dhcpLb1 -f 'dhcp.Lb1.dn*"[tenant].*[DHCP Relay Policy name]"'

<#root>

APIC#

moquery -c dhcpLb1 -f 'dhcp.Lb1.dn*"tz.*Relay"'

Total Objects shown: 1

dhcp.Lb1

name : tz-DHCP_Relay

```
annotation :
childAction :
descr :
dn : uni/tn-tz/BD-BD2/dhcp1b1-tz-DHCP_Relay
extMngdBy :
lcOwn : local
modTs : 2025-09-11T16:30:03.016+00:00
monPolDn : uni/tn-common/monepg-default
nameAlias :
```

owner : tenant

```
ownerKey :
ownerTag :
rn : dhcp1b1-tz-DHCP_Relay
status : modified
tag : yellow-green
uid : 15374
userdom : :all:
```

这显示与BD关联的DHCP标签对象。

如果DHCP中继策略配置正确，它将有一个使用DHCP标签的子对象，可以通过以下命令进行验证：

<#root>

APIC#

```
moquery -c dhcpRelayP -f 'dhcp.RelayP.dn*"tz.*Relay"' -x rsp-subtree=children rsp-subtree-class=dhcpRtLb
```

Total Objects shown: 1

dhcp.RelayP

name : tz-DHCP_Relay

```
annotation :
childAction :
descr :
dn : uni/tn-tz/relayp-tz-DHCP_Relay
extMngdBy :
lcOwn : local
modTs : 2025-09-11T16:10:56.421+00:00
mode : visible
monPolDn : uni/tn-common/monepg-default
nameAlias :
```

owner : tenant

```
ownerKey :
ownerTag :
rn : relayp-tz-DHCP_Relay
status : modified
uid : 15374
userdom : :all:
```

```
# dhcp.RtLb1DefToRelayP
tDn : uni/bd-[uni/tn-tz/
```

BD-BD2

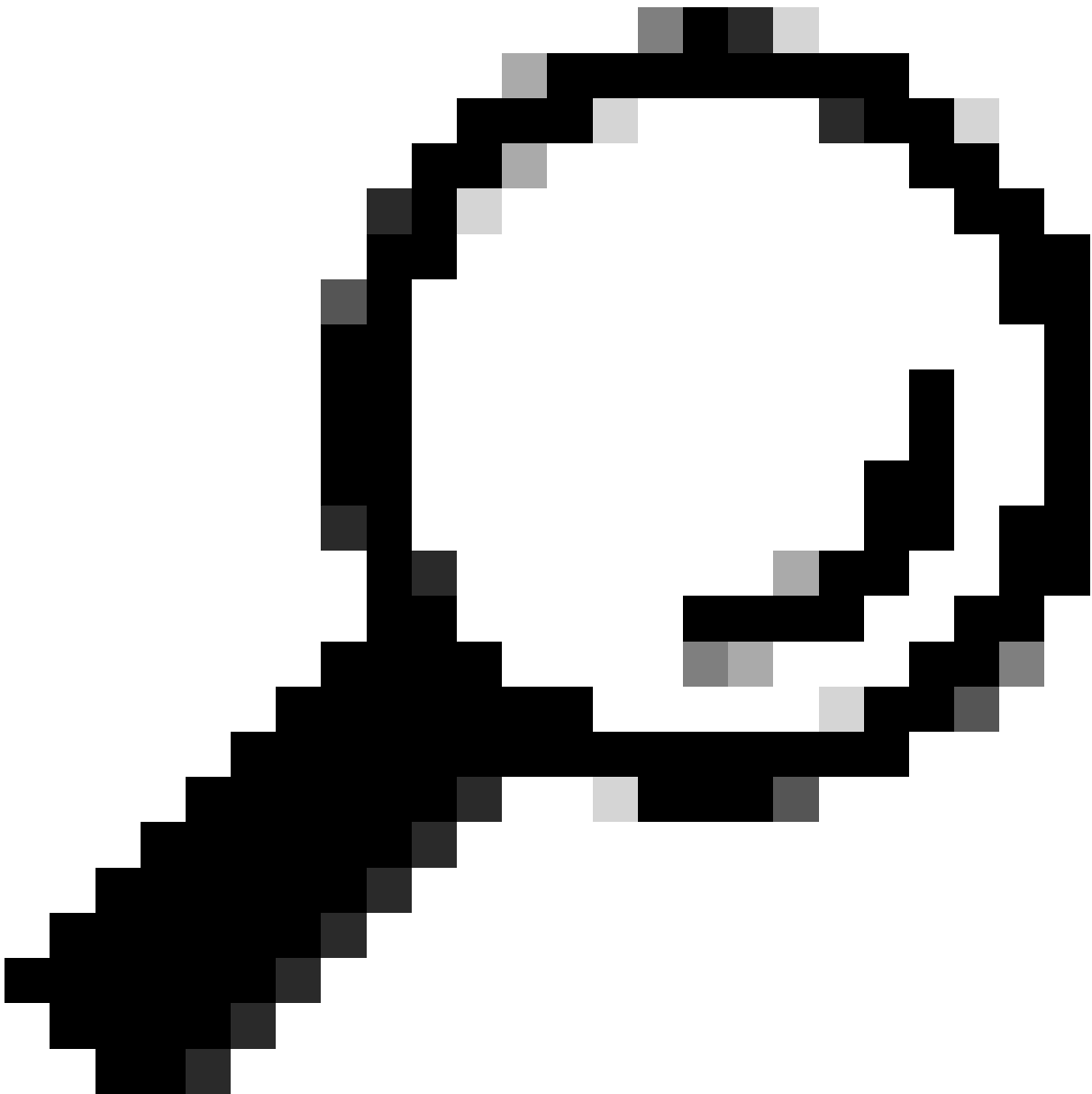
```
] -isSvc-no/dhcp1b1def-tz-DHCP_Relay
childAction : deleteNonPresent
dn : uni/tn-tz/relayp-tz-DHCP_Relay/rt1b1DefToRelayP-[uni/bd-[uni/tn-tz/BD-BD2]-isSvc-no/dhcp1b1def-tz-
lcOwn : local
modTs : 2025-09-11T16:30:03.106+00:00
rn : rt1b1DefToRelayP-[uni/bd-[uni/tn-tz/BD-BD2]-isSvc-no/dhcp1b1def-tz-DHCP_Relay]
status :
tCl : dhcpLb1Def
```

DHCP数据包跟踪

ACI将发送到CPU的所有DHCP数据包记录在trace文件中，可以分析该文件以对DHCP发现、提供、请求和确认(DORA)进程进行故障排除。使用此命令查看DHCP数据包跟踪：

<#root>

```
show dhcp internal event-history traces
```



提示：单个DHCP数据包会生成超过100个跟踪条目。强烈建议结合正则表达式使用grep来过滤相关输出，以便进行高效分析。

在Cisco ACI的DHCP跟踪分析过程中，可以确认几个关键属性以确保DHCP中继正常运行：

- 添加电路id子选项：

表示正在将DHCP选项82添加到数据包，这对于中继代理信息至关重要。

- GI 地址：

表示在DHCP中继策略中配置的DHCP服务器IP地址。

- 帮助地址：

中继用于访问DHCP服务器的SVI IP地址。

- 客户端和服务端位于同一VRF中：

确认DHCP客户端和服务端属于同一VRF情景。

- 消息：

观察到的DHCP消息的类型，例如Discover、Offer、Request或Ack。

- ctx名称：

配置DHCP标签策略的VRF名称。

- Smac:

DHCP客户端的MAC地址。

- UDP源/目标端口：

使用的DHCP端口，客户端通常为68，服务器通常为67。

<#root>

Leaf101# s

how dhcp internal event-history traces | grep -A34 -B70 "00 50 56 b7 33 ee" | egrep "(Rec.*pkt.*intf|ip

2) 2025 Sep 11 04:14:46.660433 _relay_handle_packet_from_pkt_mgr: 480 : Relaying the DHCP pkt on intf: V
28) 2025 Sep 11 04:14:46.659985 _relay_add_circuitid_rmtid_msiteinfo: 3354 :

Add circuit id suboption

: if_index: Ethernet1/45 (1a02c000) , svlan: 24, option def id: 0 epg_vnid 8529.

..

31) 2025 Sep 11 04:14:46.659934 _relay_add_option82: 3151 : Mac addr is 28:6f:7f:eb:54:9f

32) 2025 Sep 11 04:14:46.659930 _relay_add_option82: 3147 : Adding option82 suboptions

35) 2025 Sep 11 04:14:46.659924 _relay_send_packet: 1975 :

gi address is 172.16.18.1

..

37) 2025 Sep 11 04:14:46.659921 _relay_send_packet: 1965 :

Helper address is 172.16.18.100

38) 2025 Sep 11 04:14:46.659918 _relay_send_packet: 1956 :

Client and Server are in the same VRF

39) 2025 Sep 11 04:14:46.659793 _relay_send_packet: 1898 : ifindex is Vlan24

40) 2025 Sep 11 04:14:46.659786 _relay_send_packet: 1833 : dhcp_relay_send_packet: relayback_ifindex is

..

42) 2025 Sep 11 04:14:46.659730 _relay_handle_packet_from_pkt_mgr: 447 :

DHCPDISCOVER msg

43) 2025 Sep 11 04:14:46.659728 _relay_handle_packet_from_pkt_mgr: 438 : ifindex is Vlan24
..

61) 2025 Sep 11 04:14:46.657274 _snoop_handle_istack_packet: 1763 :

ctx name is tz:VRF1

64) 2025 Sep 11 04:14:46.657062 _snoop_handle_istack_packet: 1751 :

Smac = [00 50 56 b7 33 ee]

65) 2025 Sep 11 04:14:46.657057 _snoop_handle_istack_packet: 1749 : Dmac = [ff ff ff ff ff ff];

68) 2025 Sep 11 04:14:46.657050 _snoop_handle_istack_packet: 1737 : Logical interface: Vlan24

72) 2025 Sep 11 04:14:46.657044 _snoop_handle_istack_packet: 1721 : Physical interface: Ethernet1/45

..

86) 2025 Sep 11 04:14:46.657024 _snoop_handle_istack_packet: 1669 :

UDP src port 68 UDP dst port 67

88) 2025 Sep 11 04:14:46.657021 _snoop_handle_istack_packet: 1577 : destination ip address 255.255.255.

89) 2025 Sep 11 04:14:46.657018 _snoop_handle_istack_packet: 1574 : source ip address 0.0.0.0

95) 2025 Sep 11 04:14:46.656991 _snoop_handle_istack_packet: 1533 : Received pkt on Vlan 25 intf Ether

常见问题

问题 1:L3out silent drop

- 问题

当L3Out使用vPC接口与相邻路由器形成邻居关系时，每台交换机使用自己的vTEP发送数据包。如果vPC对等设备收到的DHCP提供包含其自身的vTEP地址，它会通过交换矩阵转发数据包，导致发起方vTEP以静默方式丢弃数据包，而不显示故障日志。

要检查此类丢弃，请使用以下命令：

```
<#root>
```

```
show
```

```
dhcp
```

```
internal event-history traces |
```

```
egrep
```

```
"(
```

```
failed|Drop
```

```
).*packet" | head
```

```
<#root>
Leaf101#
```

```
show dhcp internal event-history traces | egrep "(failed|Drop).*packet" | head
```

```
53) 2025 Sep 10 04:14:26.685020 _snoop_handle_istack_packet: 1881 : Drop DHCP DISCOVER/REQUEST packet b
172) 2025 Sep 10 04:14:23.792669 _snoop_handle_istack_packet: 1881 : Drop DHCP DISCOVER/REQUEST packet
239) 2025 Sep 10 04:14:22.516679 _snoop_handle_istack_packet: 1881 : Drop DHCP DISCOVER/REQUEST packet
444) 2025 Sep 10 04:14:17.055216 _snoop_handle_istack_packet: 1881 : Drop DHCP DISCOVER/REQUEST packet
563) 2025 Sep 10 04:14:14.450437 _snoop_handle_istack_packet: 1881 : Drop DHCP DISCOVER/REQUEST packet
736) 2025 Sep 10 04:14:09.056993 _snoop_handle_istack_packet: 1881 : Drop DHCP DISCOVER/REQUEST packet
803) 2025 Sep 10 04:14:07.344467 _snoop_handle_istack_packet: 1881 : Drop DHCP DISCOVER/REQUEST packet
906) 2025 Sep 10 04:14:06.290135 _snoop_handle_istack_packet: 1881 : Drop DHCP DISCOVER/REQUEST packet
1025) 2025 Sep 10 04:14:03.770388 _snoop_handle_istack_packet: 1881 : Drop DHCP DISCOVER/REQUEST packet
1094) 2025 Sep 10 04:14:03.234017 _snoop_handle_istack_packet: 1881 : Drop DHCP DISCOVER/REQUEST packet
```

- 解决方案

导航到租户> [tenant name] >网络> L3outs > [L3out name] >逻辑节点配置文件> [LNP name]
>逻辑接口配置文件[LIP name] > SVI > [SVI策略]

完成后，创建或打开Secondary IP address并启用Enable for DHCP Relay复选框。

Create Secondary IP address

Address: 192.168.1.1/24

Enable for DHCP Relay: ☒

Use the Secondary IP Address as DHCP Relay Gateway Address

Cancel Submit

这将强制使用vPC vTEP地址而不是本地vTEP发送消息，并且数据包按照预期进行转发。

问题 2:DHCP服务器不支持选项82

选项82在ACI等VXLAN环境中至关重要，它根据vTEP地址在源枝叶和目的之间创建电路。此命令包

括：

- 电路ID:看到DHCP发现的传入接口、VLAN和EPG VNID。
- 远程ID:接收发现的交换机的TEP地址。

如果缺少选项82，则会丢弃DHCP中继数据包。通过检查DHCP跟踪日志中是否存在指示缺少选项82的错误，验证在连接到DHCP服务器的枝叶上存在选项82。

此命令验证连接DCHP服务器的枝叶交换机是否收到具有有效DHCP选项82的优惠

```
<#root>
```

```
Leaf101#
```

```
show
```

```
dhcp
```

```
internal event-history traces |
```

```
egrep
```

```
"(
```

```
failed|Drop
```

```
). *packet" | head
```

```
67) 2025 Sep 10 05:16:52.336785 _relay_handle_packet: 1478 : dhcp_relay_handle_packet: DHCP UDP failed
68) 2025 Sep 10 05:16:52.336772 _relayback_response: 929 : dhcp_relayback_response : option 82 not pres
479) 2025 Sep 10 05:11:07.308085 _relay_handle_packet: 1478 : dhcp_relay_handle_packet: DHCP UDP failed
480) 2025 Sep 10 05:11:07.308073 _relayback_response: 929 : dhcp_relayback_response : option 82 not pre
891) 2025 Sep 10 05:10:22.312386 _relay_handle_packet: 1478 : dhcp_relay_handle_packet: DHCP UDP failed
892) 2025 Sep 10 05:10:22.312374 _relayback_response: 929 : dhcp_relayback_response : option 82 not pre
1303) 2025 Sep 10 05:09:37.309888 _relay_handle_packet: 1478 : dhcp_relay_handle_packet: DHCP UDP faile
1304) 2025 Sep 10 05:09:37.309874 _relayback_response: 929 : dhcp_relayback_response : option 82 not pr
1715) 2025 Sep 10 05:08:52.295721 _relay_handle_packet: 1478 : dhcp_relay_handle_packet: DHCP UDP faile
1716) 2025 Sep 10 05:08:52.295709 _relayback_response: 929 : dhcp_relayback_response : option 82 not pr
```

参考

[ACI交换矩阵中的DHCP中继深度故障排除 — TACDCN-2017](#)

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）。