

了解Catalyst 9000交换机上的REP

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[术语](#)

[REP理论](#)

[REP备用端口选举](#)

[阻塞端口通告](#)

[备用端口选举](#)

[终端端口通告](#)

[REP链路故障通知](#)

[REP首选端口和VLAN负载均衡](#)

[配置](#)

[网络图](#)

[配置](#)

[验证](#)

[命令汇总](#)

[故障排除](#)

[输入队列楔形](#)

[REP日志消息](#)

[相关信息](#)

简介

本文档介绍如何配置和验证Catalyst 9000交换机上的弹性以太网协议(REP)。

先决条件

要求

Cisco 建议您了解以下主题：

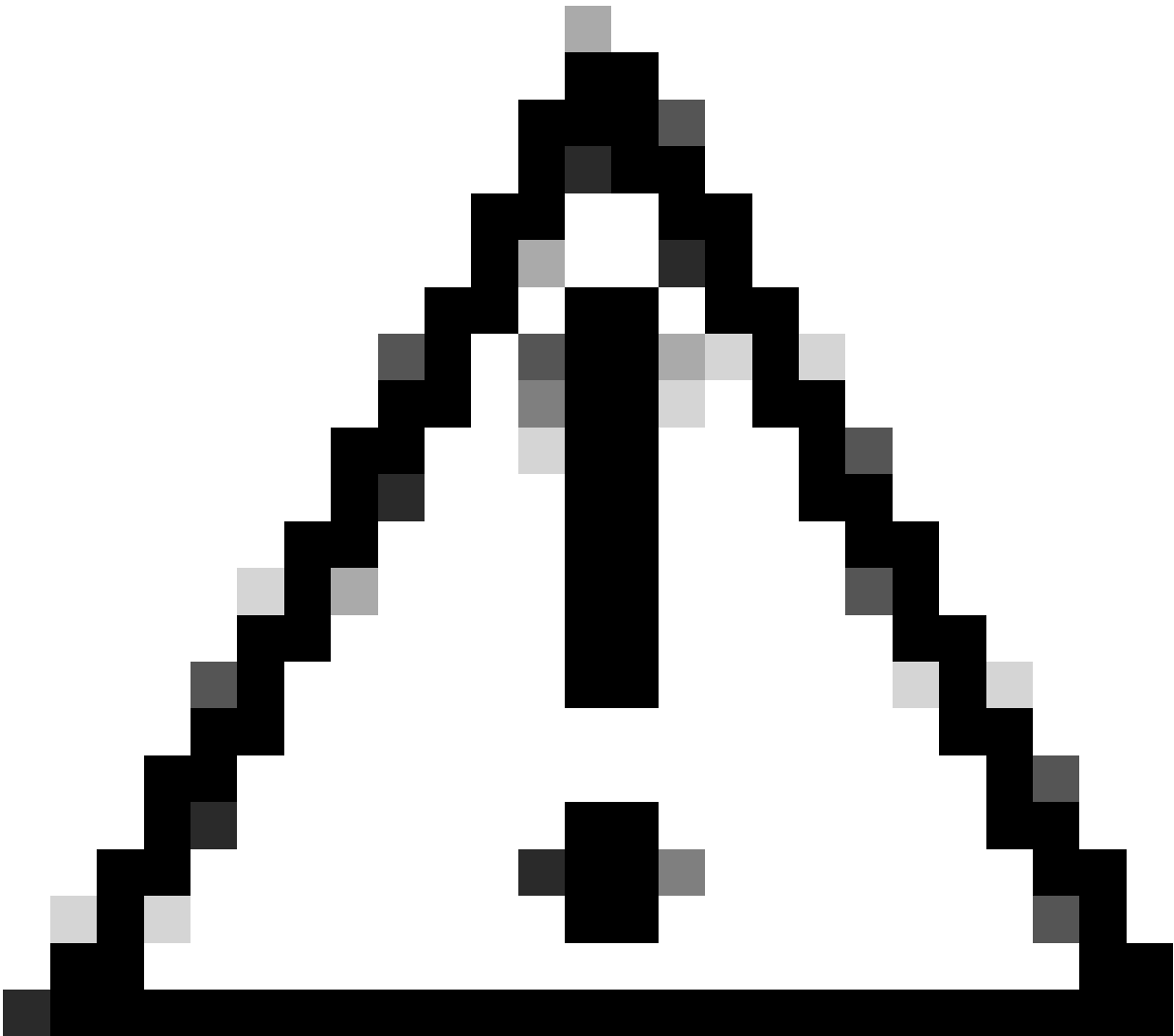
- 第2层环路预防

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Catalyst 9200

- Catalyst 9300
 - Catalyst 9400
 - Catalyst 9500
 - Catalyst 9600
 - Cisco IOS XE 17.6.5及更高版本
-



注意：具有Stackwise虚拟(SVL)的交换机不支持REP

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。

背景信息

REP是Cisco专有协议，旨在防止第2层以太网络中出现网络环路并在链路故障时提供快速收敛。它是生成树协议的替代协议，通常用于需要大型第2层扩展的特定第2层拓扑，如IoT网络、工业网络或制造网络。REP“网段”是通过将配置有相同网段ID的交换机之间的端口链接在一起而形成的。利用REP负载均衡及其与STP共存的能力等功能，REP可用于构建复杂但可预测的第2层拓扑。

术语

期限	定义
网段	共享相同网段ID的端口链
网段ID	用于表示数据段的数字，介于1和1024之间
REP端口	配置为运行REP的端口。在REP端口上禁用了STP。
边缘端口	终止REP网段一个边缘的端口。
备选端口	阻塞网段中的VLAN以防止环路的端口。如果配置了负载均衡，则网段中有2个备用端口
开放端口	网段上转发所有VLAN的端口
封闭式网段	REP网段，其中两个边缘端口位于同一交换机上且相互连接。也称为“环网段”。
打开段	边缘端口彼此之间没有连接的REP网段。边缘端口位于不同的交换机上，并且在它们之间有一个阻塞端口。
链路状态层 (LSL)	负责建立邻居邻接关系和维护链路状态的三次握手协议。LSL帧每1秒在REP端口上发送一次。
硬件泛洪层 (HFL)	负责通过组播泛洪REP PDU，在链路故障后促进快速收敛的层
阻塞端口通告 (BPA)	由端口发送的消息，用于通告其阻止的VLAN列表。BPA也可以传送拓扑更改，使接收端口刷新其MAC表
终端端口通告 (EPA)	传送有关REP网段的全局信息，并由边缘端口发送
REP管理 VLAN	VLAN，用于在链路故障后泛洪REP快速通知以实现收敛。如果配置了HFL，则在此处运行。否则，REP管理VLAN为1。

REP理论

REP可以通过在称为替换端口的网段中的一个端口上阻塞VLAN来防止交换环路。当REP网段中的所有端口都处于UP状态时，替换端口会阻塞以防止环路。当REP网段中的链路发生故障时，或者如果交换机出现导致REP协议数据包链路丢失的问题，则备用端口会为其之前阻塞的VLAN进行转发。请注意，因此，REP网段只能处理网段内的单个故障端口，这一点非常重要。REP网段上若出现一个以上的链路故障，则可能导致流量丢失。

在接口上启用REP时，它会立即阻止所有VLAN。REP LSL接管并开始发送LSL PDU以建立邻接关系。使用三次握手创建邻接关系，并以1秒的间隔发送后续LSL hello数据包，以维护REP邻居。

在REP邻居发现期间，设备交换其REP网段ID及其端口ID。

- 网段ID是一个介于1和1024之间的数字，在启用REP时在接口上配置。这唯一标识了REP数据段。
- 端口ID是一个根据系统MAC地址和交换机端口号自动生成的60位字。
- 向目标MAC地址发送的LSL PDU是0180.c200.0000

```
<#root>
```

```
9200-STACK-1#
```

```
show interface port-channel1 rep detail | i PortID
```

```
PortID: 08E9
```

```
78BC1A4FDD80
```

```
<--- Port ID with system MAC in bold
```

```
9200-STACK-1#
```

```
show version | i MAC
```

```
Base Ethernet MAC Address :
```

```
78:bc:1a:4f:dd:80
```

```
<-- Switch system MAC
```

REP端口在关闭或LSL hello超时在5秒后过期后变为失败状态。

REP备用端口选举

REP备用端口是网段中阻塞VLAN的端口。

- 使用建议和同意机制在建立REP邻居之后立即选举备用端口，以确定网段中的哪个端口保持阻塞。
- 网段中的每个端口都会通告其端口密钥和端口优先级，并等待协议。
- 具有最高优先级的端口被选为备用端口。
- 选举过程通过REP BPA消息进行。

阻塞端口通告

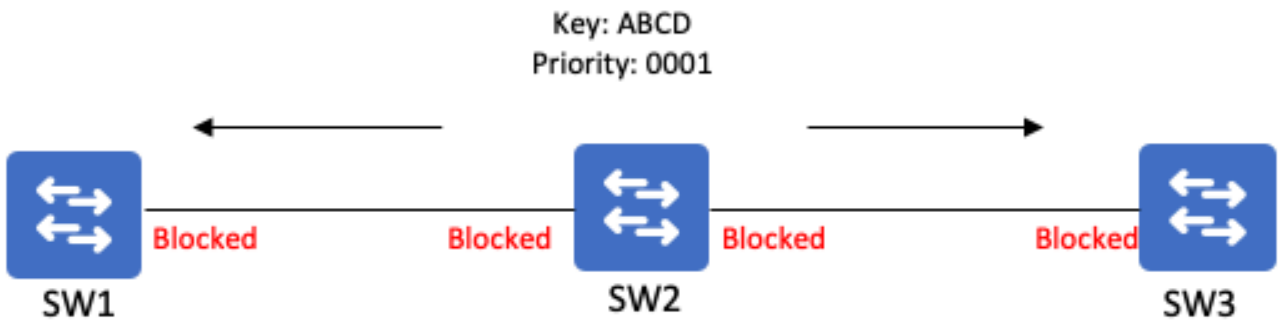
BPA消息由端口密钥和端口优先级组成。

- REP端口密钥是9字节的标识符，每次端口进入阻塞状态时生成（对于启用REP的端口，该标识符立即处于链路连接状态）。
- 它是端口ID和随机生成的编号的组合。
- 端口优先级也是9字节的标识符。

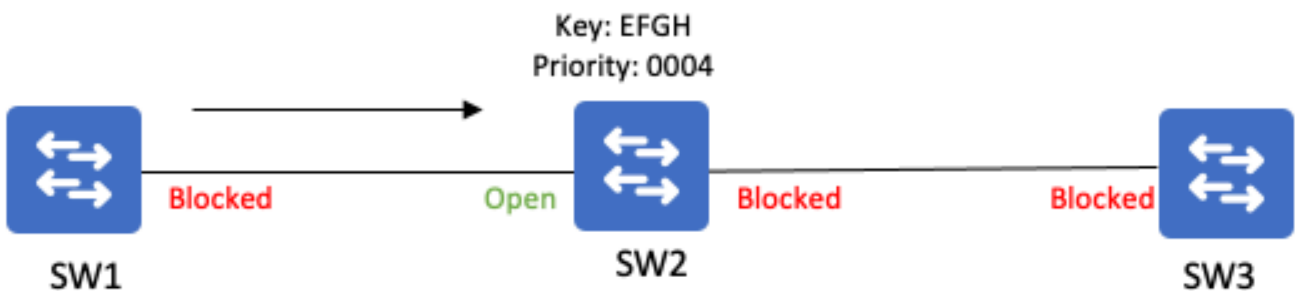
备用端口选举

1. 在链路打开时，当REP端口处于阻塞状态时，它会向其REP邻居通告其端口密钥和优先级
2. 接收端口将接收的BPA端口优先级与其自己的端口优先级进行比较
3. 接收端口以ACK消息做出响应，该消息包含BPA中从相邻端口接收的密钥。当邻居在BPA中收到自己的密钥时，它知道该BPA是来自其邻居的ACK消息
4. 如果ACK包含的端口优先级高于本地端口优先级，则本地端口会进入OPEN状态。它不会以较高的优先级响应邻居，但会将该提议从其另一个REP端口转发到另一个REP邻居
5. 另一个REP邻居将收到的端口优先级与自己的优先级进行比较。如果收到的优先级高于本地优先级，它也不会响应并转发提议。如果本地优先级更高，它将以自己的优先级对原始建议书做出响应

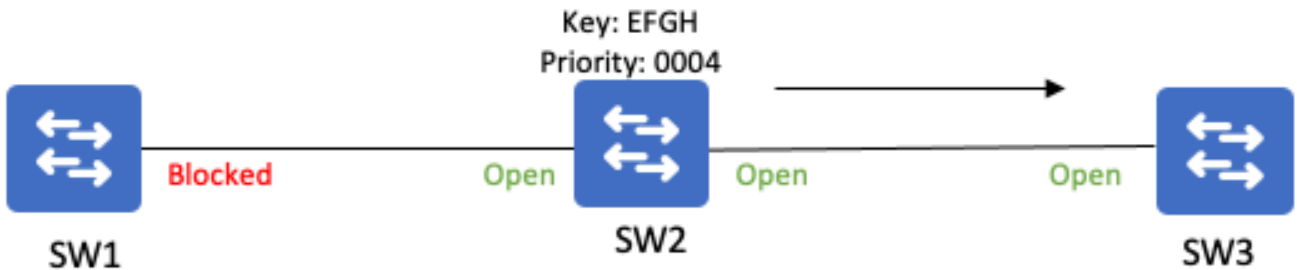
1. Advertise BPA with key and priority



2. Receive BPA with key and higher priority from SW1 causing port to go OPEN



3. Forward SW1 proposal to SW3 who opens its port due to SW1 higher priority



此过程会重复执行，直到优先级最高的端口处于阻塞模式。此端口即成为网段备用端口。备用端口继续将包含其端口密钥的BPA消息发送到REP网段。网段中的所有REP端口都缓存备用端口的密钥。

在稳定的REP网段中，所有端口在替换端口上均一致通过具有相同的替换端口密钥副本实现。在链路故障情况下，维护备用端口的端口密钥ID的每台交换机都会变得相关。

终端端口通告

EPA消息由边缘端口每4秒生成一次。这些消息由网段中的每个REP接口转发，并且每个端口将自己的拓扑信息添加到消息中。

一旦边缘端口收到网段中另一个边缘端口生成的EPA，它就会拥有整个网段的完整拓扑。

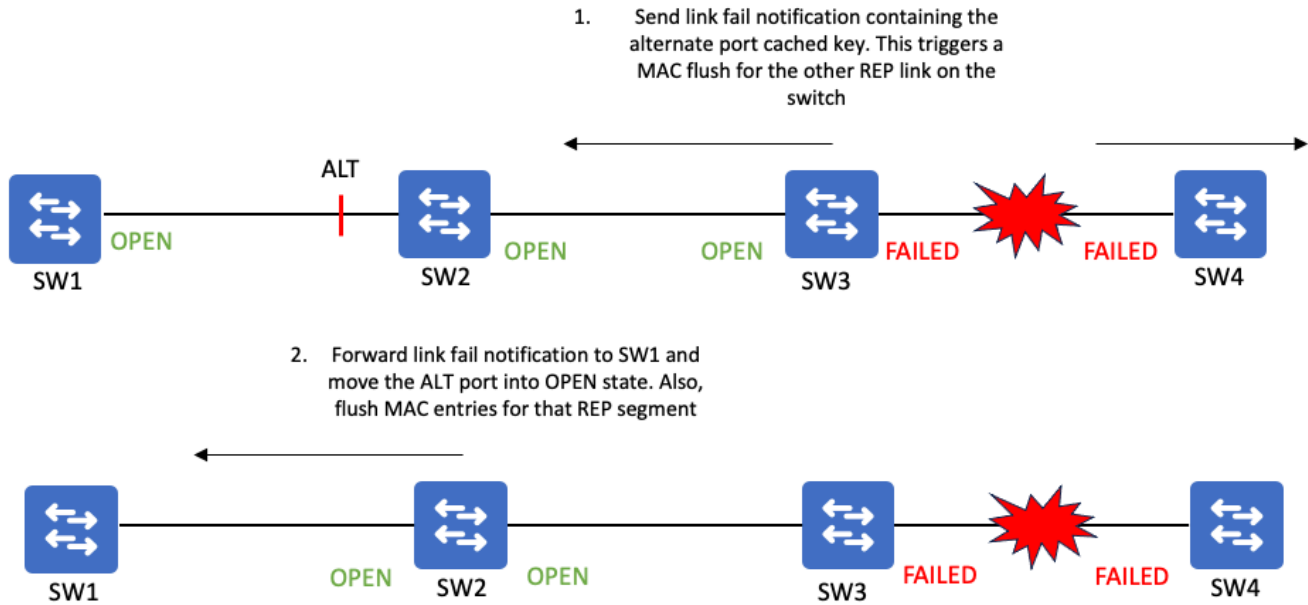
EPA允许每个边缘端口相互看到并促进主边缘端口的选举。优先级最高的边缘端口成为主边缘端口

。

REP链路故障通知

当链路在REP网段中发生故障时，它将进入“故障”状态，并发送包含备用端口的缓存密钥的链路故障通知。发送交换机还刷新其REP链路仍在运行的MAC地址。

REP邻居交换机收到链路故障通知并将其转发到网段上的任何REP邻居，并刷新REP网段中端口的MAC地址条目。如果收到链路故障通知的交换机包含网段上的备用端口，则该交换机将端口转换为打开状态。



链路故障通知有两种分发方式：

1. REP快速通知，通过发送BPA消息到思科组播地址0100.0ccc.cccc
2. 通过发送REP BPDU帧中的BPA消息发送REP可靠通知（类似于REP LSL帧）。

功能	快速通知	可靠通知
硬件已转发	Yes	无
可靠	无	是（通过序列号和重新传输方式）
通过备用/阻塞端口	无	Yes

转发到REP网段之外	Yes	无
在REP管理VLAN上发送	Yes	否 (使用本征VLAN)

REP链路故障通知的作用与STP TCN类似，因为它们被传送到CPU并在REP端口上触发MAC刷新。通过在面向STP网段的REP端口上进行额外配置，可以将REP链路故障通知转换为STP TCN，以告知STP域由于REP链路故障而刷新MAC。

REP首选端口和VLAN负载均衡

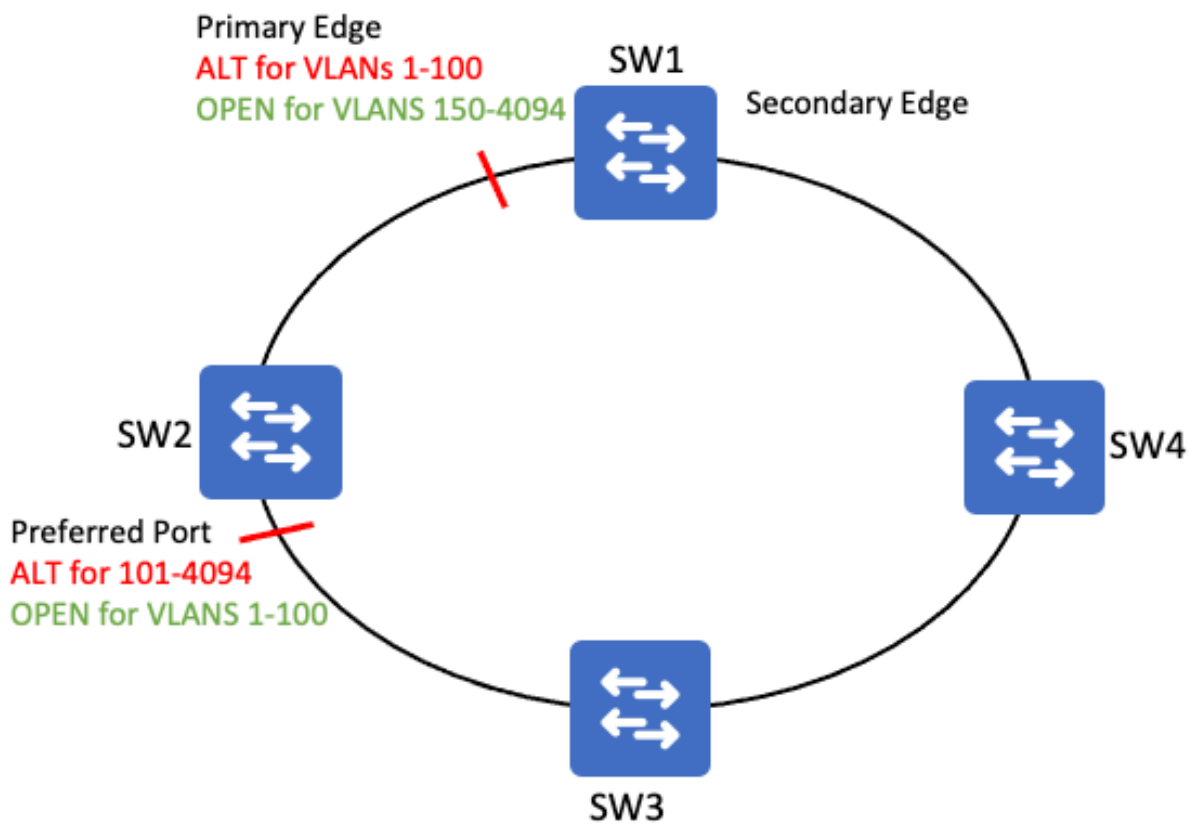
配置VLAN负载均衡时，REP主边缘端口是启动负载均衡的端口。REP首选端口是首选成为替代端口的端口。

由于负载均衡是通过其他配置从主边缘端口发起的，因此主边缘端口在负载均衡方案中是相关的。

通过配置首选端口应阻塞哪些VLAN来实现负载均衡。

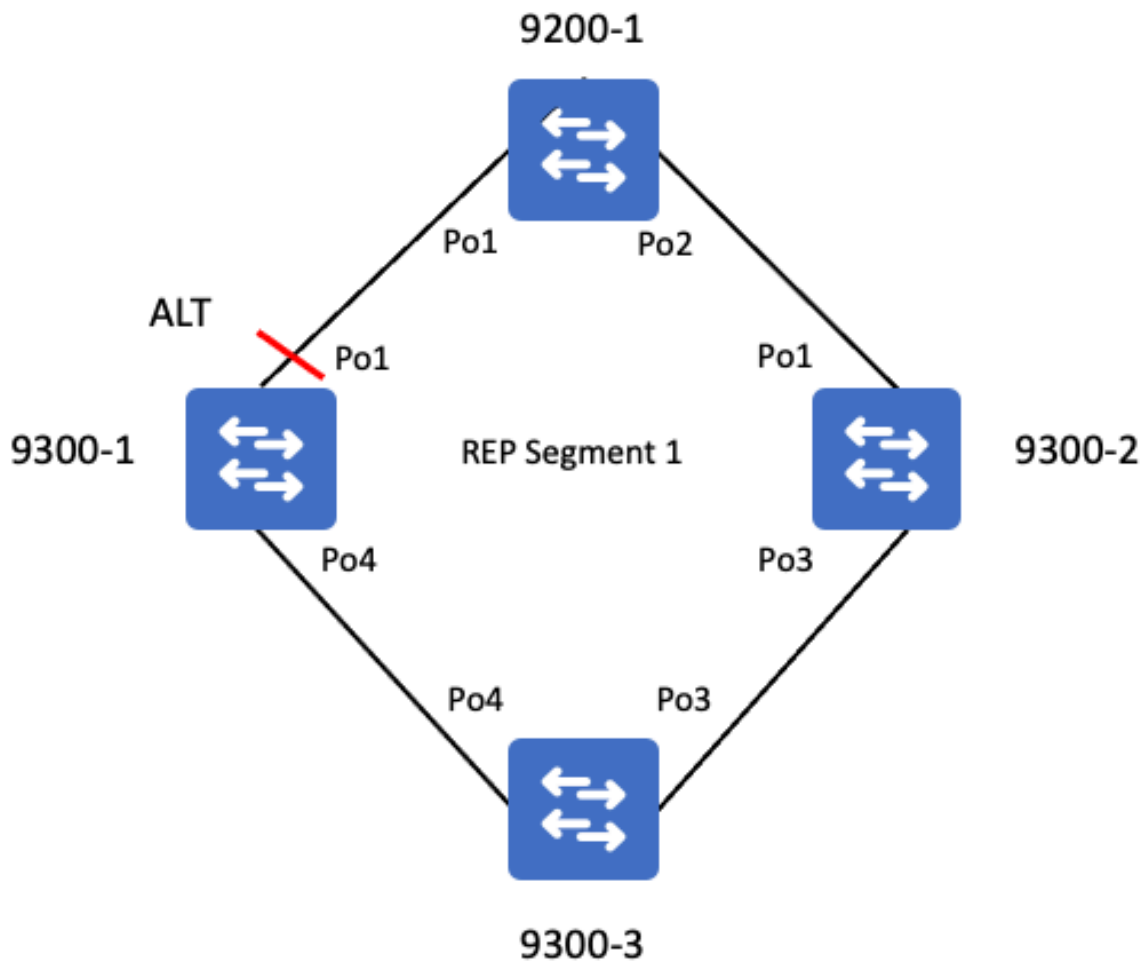
- 其余VLAN在主边缘端口上被阻塞。
- 当VLAN负载均衡已配置且处于活动状态时，有2个备用端口。

配置负载均衡后，直到从主边缘端口触发链路故障或手动抢占时，负载均衡才会生效。



配置

网络图



配置

所有端口必须配置为具有匹配REP网段ID的中继端口。边缘交换机需要edge参数。

```
<#root>
```

```
9200-STACK-1#
```

```
show running-config interface port-channel 1
```

```
Building configuration...
```

```
Current configuration : 100 bytes
```

```
!
```

```
interface Port-channel1
```

```
switchport mode trunk          <-- Must be a trunk
```

```
load-interval 30
```

```
rep segment 1 edge            <-- configure edge port in REP segment 1
```

```
end
```

不是边缘端口的REP端口不需要edge关键字。

```
<#root>
9300-STACK-2#
show running-config interface port-channel 1
Building configuration...
Current configuration : 69 bytes
!
interface Port-channel1
 switchport mode trunk

rep segment 1          <-- non-edge REP port configuration
end
```

验证

配置完所有网段端口后，该网段即已完成，应该没有出现故障的端口。

确认REP拓扑。

```
<#root>
9200-STACK-1#
show rep topology

REP Segment 1
BridgeName          PortName  Edge Role
-----
9200-STACK-1       Po1
Pri Open          <-- primary edge port
9300-STACK-1       Po1
Alt
<-- alternate port that is blocking VLANs
9300-STACK-1       Po4          Open
9300-STACK-3       Po4          Open
9300-STACK-3       Po3
Open          <-- port is OPEN and forwarding all VLANs
9300-STACK-2       Po3          Open
9300-STACK-2       Po1          Open
9200-STACK-1       Po2
Sec Open          <-- secondary edge port
```

确认接口上的REP状态。

```
<#root>
```

```
9200-STACK-1#
```

```
show interface port-channel 1 rep <-- check REP status for the port
```

```
Interface          Seg-id Type          LinkOp   Role
-----
Port-channel1      1      Primary Edge      TWO_WAY
Open <-- Edge port is not blocking any VLANs
```

Detail输出进一步显示了端口的REP状态

```
<#root>
```

```
9200-STACK-1#
```

```
show interfaces port-channel1 rep detail
```

```
Port-channel1 REP enabled
Segment-id: 1 (Primary Edge)
PortID:
```

```
08E978BC1A4FDD80 <-- port ID made from system MAC + random number
```

```
Preferred flag: No
Operational Link Status: TWO_WAY
Current Key:
```

```
0BE934ED1B4798003405 <-- cached key of the segment Alternate port
```

```
Port Role: Open
Blocked VLAN:
```

```
Admin-vlan: 1 <-- REP admin vlan
```

```
Preempt Delay Timer: disabled
```

```
LSL Ageout Timer: 5000 ms
```

```
<-- default link status adjacency hold down timer
```

```
LSL Ageout Retries: 5
Configured Load-balancing Block Port:
```

```
none <-- no load balancing configured on the port
```

```
Configured Load-balancing Block VLAN: none
```

```
STCN Propagate to: none <-- sending TCNs into STP domain is disabled
```

```
LSL PDU rx: 924743, tx: 612406
HFL PDU rx: 1, tx: 1
BPA TLV rx: 611945, tx: 2
```

```
BPA (STCN, LSL) TLV rx: 0, tx: 0
BPA (STCN, HFL) TLV rx: 0, tx: 0
EPA-ELECTION TLV rx: 13, tx: 11
EPA-COMMAND TLV rx: 0, tx: 0
EPA-INFO TLV rx: 152998, tx: 152999
```

命令汇总

```
show rep topology
show rep topology detail
show rep topology segment <Id>
show rep topology segment <Id> detail
show rep topology archive
show rep topology archive detail
show interfaces gig<X/X> rep
show interfaces gig<X/X> rep detail
```

故障排除

输入队列楔形

在某些代码版本上，REP HSL数据包可以楔入接口的输入队列。

- 如果HSL数据包填满输入队列且无法处理LSL融合数据包，这可能会影响REP融合
- 这是由Cisco Bug ID [CSCwc](#)引起的52868
- 输入队列处理所有协议的处理。一旦队列变为“已满”，它将耗尽合法的网络控制流量，无法手动清空。

队列楔形的症状

- CDP、IGMP等协议停止工作（您可能会在CDP中丢失邻居、IGMP组播编程问题等）。
- 根据到达需要处理的接口的功能和协议的不同，故障症状也会有所不同。
- 接口输入队列用于到达要排队并传送到CPU进行处理接口的数据包
- 当某个数据包无法出列时，输入队列会被塞满，最终达到输入队列限制
- 一旦达到接口输入队列限制，就不能再存储其他数据包，而是会丢弃这些数据包。

检验队列楔形

通过REP管理VLAN的REP硬件泛洪层数据包导致L2端口上的输入队列被楔住。

```
<#root>
```

```
C9300#
```

```
show interface gi1/0/48
```

```
GigabitEthernet1/0/48 is up, line protocol is up (connected)
```

```
Hardware is Gigabit Ethernet, address is 7486.0b0c.e0b0 (bia 7486.0b0c.e0b0)
Description: PORT
MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
Full-duplex, 1000Mb/s, media type is 10/100/1000BaseTX
input flow-control is on, output flow-control is unsupported
ARP type: ARPA, ARP Timeout 04:00:00
Last input 01:14:45, output 00:00:00, output hang never
Last clearing of "show interface" counters never
```

```
Input queue: 2438/2000
```

```
/16/0 (size/max/drops/flushes); Total output drops: 0
```

```
<-- 2438 frames in the input queue who's limit is 2000
```

```
<...snip...>
```

检查此CLI以确认接口是否保存有REP HFL帧的缓冲区

- HFL帧的目的MAC是0100.0ccc.ccce

```
<#root>
```

```
C9300#
```

```
show
```

```
buffers input-interface gi1/0/48 packet
```

```
Tracekey : 1#09f7811786f1de5ddfa0f5542a69f593
```

```
Buffer information for Middle buffer at 0x7F81FE8E9000
```

```
data_area 0x7F820F78F004, refcount 1, next 0x0, flags 0x210
```

```
linktype 189 (LINK_REP), enctype 3 (SNAP), encsize 22, rxtyp 88
```

```
if_input 0x7F820E71DB50 (GigabitEthernet1/0/48), if_output 0x0 (None)
```

```
inputtime 3d14h (elapsed 03:11:48.761)
```

```
outputtime 00:00:00.000 (elapsed never), oqnumber 65535
```

```
datagramstart 0x7F820F78F072, datagramsize 565, maximum size 804
```

```
mac_start 0x7F820F78F072, addr_start 0x7F820F78F072, info_start 0x7F820F78F080
```

```
network_start 0x7F820F78F088, transport_start 0x0, caller_pc :55FBF3ED3000+37680AC
```

```
7F820F78F072:
```

```
0100CCC CCCE
```

```
A0F8
```

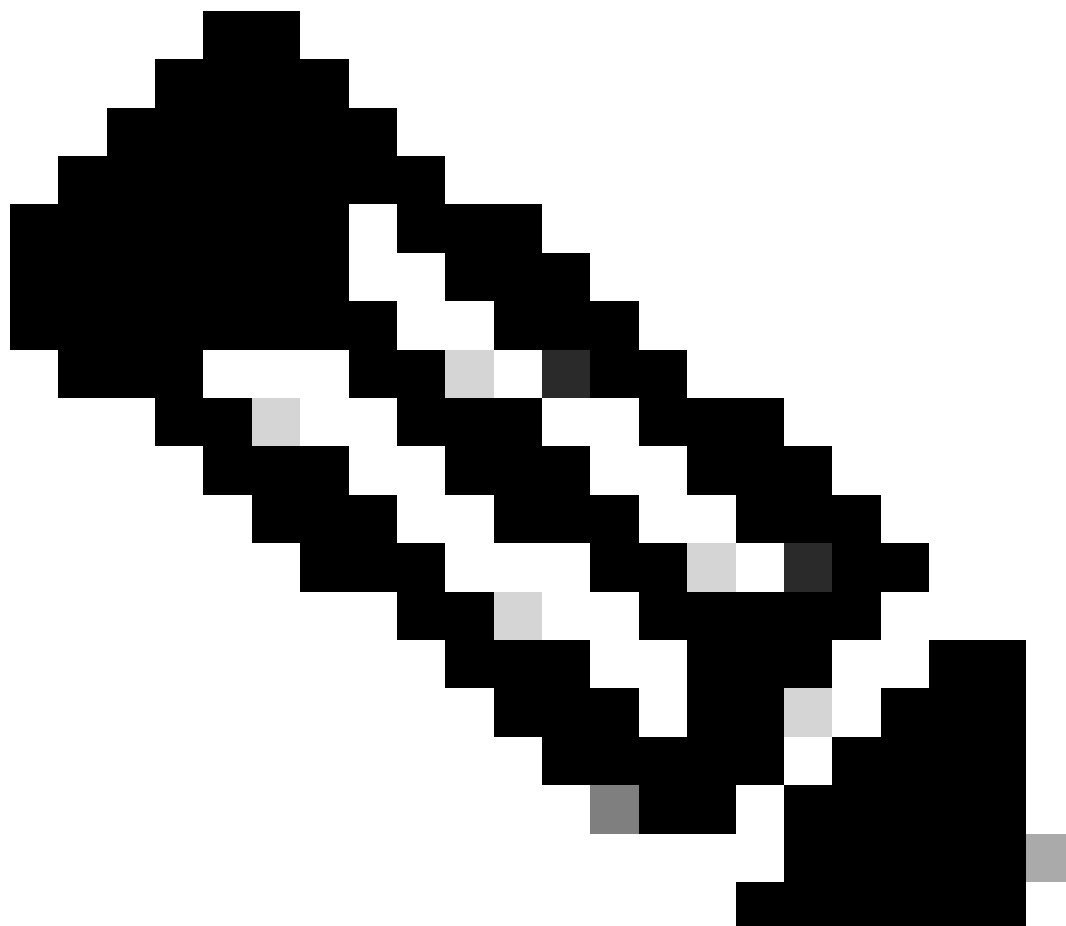
```
...LLN x
```

```
<--- HFL destination MAC is in the queue
```

补救队列楔形

- 重启设备(如果不重新加载，输入队列将无法清除。Shut / no shut of interface does not clear these buffers)
- 升级到不受此问题影响的代码版本
- 调整输入队列大小(在您确定不再有任何HSL帧将到达的情况下，您可以尝试增加输入队列大小。请记住，下次发生HSL泛洪时，问题可能会再次出现)。

在这种状态下，出现了一些REP系统日志。这些日志将在下一节中列出



注意：请记住，这是一个指示邻居之间LSL丢失的通用日志，这可能是由其他原因造成的。因此，确定此特定问题很有用，但不仅仅限于此问题

REP日志消息

日志消息	定义	恢复操作
------	----	------

<p>%REP-4-LINKSTATUS : TenGigabitEthernet1/1/1 (网段1) 由于邻居未响应而不可用</p>	<p>表示邻居之间的LSL丢失</p>	<ul style="list-style-type: none"> • 确认接口没有楔入输入队列 • 检验链路是否没有CRC错误和其他递增错误 • 验证CPU传送路径中是否没有CoPP或丢弃
<p>%REP-5-EDGEMISCONFIG : 拓扑无效。为网段配置了两个以上的边缘端口</p>	<p>当接收的边缘端口通告与发出的边缘端口通告不同时显示</p>	<ul style="list-style-type: none"> • 当拓扑中的多个端口从故障状态恢复时预期行为，出现此消息，但在拓扑建立后不会出现 • rep拓扑中每个发生故障的端口都充当边缘端口并发出通告

相关信息

- [第2层配置指南, Cisco IOS XE Bengaluru 17.6.x \(Catalyst 9500交换机 \)](#)
- 思科漏洞ID [CSCwc52868](#)

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）。