

专线接入  
故障处理  
产品文档



腾讯云

---

**【版权声明】**

©2013-2024 腾讯云版权所有

本文档著作权归腾讯云单独所有，未经腾讯云事先书面许可，任何主体不得以任何形式复制、修改、抄袭、传播全部或部分本文档内容。

**【商标声明】**

及其它腾讯云服务相关的商标均为腾讯云计算（北京）有限责任公司及其关联公司所有。本文档涉及的第三方主体的商标，依法由权利人所有。

**【服务声明】**

本文档意在向客户介绍腾讯云全部或部分产品、服务的当时的整体概况，部分产品、服务的内容可能有所调整。您所购买的腾讯云产品、服务的种类、服务标准等应由您与腾讯云之间的商业合同约定，除非双方另有约定，否则，腾讯云对本文档内容不做任何明示或默示的承诺或保证。

---

## 文档目录

### 故障处理

通用故障排查方案

网络无法连通和数据丢包

# 故障处理

## 通用故障排查方案

最近更新时间：2024-01-13 16:02:36

本文列出了常用的故障处理指引，帮助您排查专线网络架构中网络不通问题。

## 排查顺序

1. 故障排查顺序如下：
2. [排查物理层链路故障](#)
3. [排查数据链路层故障](#)
4. [排查网络层/传输层故障](#)
5. [排查安全故障](#)
6. [排查路由故障](#)

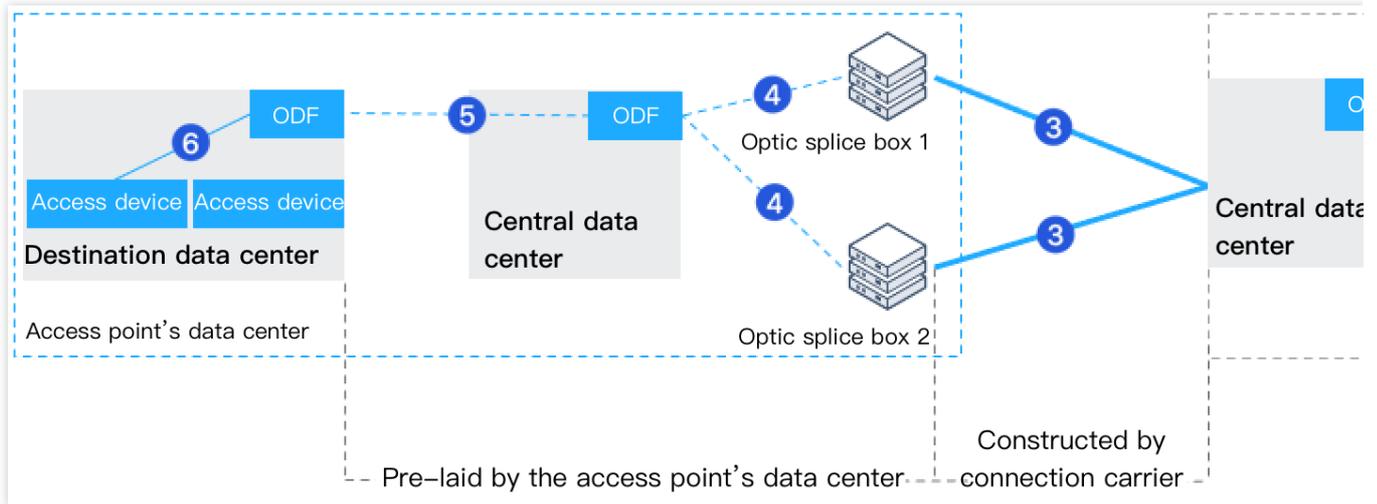
## 排查物理层链路故障

当物理端口 DOWN、两端或任意一端收发光强度异常、出现 CRC 或错包等情况，请按以下步骤排查物理层链路故障。

1. 排查本地 IDC 的 CPE 设备是否已打开，端口是否已激活。
2. 请向您的专线运营商确认专线是否已经完成端到端的接入，并要求专线运营商为您提供专线施工完成证明和端到端的网络连通性测试证明。
3. 请检查本地 IDC 光模块是否正常，并 [提交工单](#) 联系售后经理检查接入点机房的光模块是否正常。
4. 联系专线运营商和接入点运营商完成专线分段检测。

例如某专线从本地 IDC 出发，通过接入点机房楼外的光交箱进入，再经过 ODF 后接入目标机房，则需分段测试以下链路：

- ① 请自行检测本地 IDC 机房的 ODF 到接入设备间的链路是否可通信。
- ② 若您的本地 IDC 机房有多个 ODF，请检测各 ODF 间的链路是否可通信。
- ③ 联系专线运营商检测本地 IDC 到接入点机房光交箱的专线是否可通信。
- ④ 联系接入点运营商检测接入点光交箱到 ODF 之间的链路是否可通信。
- ⑤ 联系接入点运营商检测 ODF 间的链路是否可通信。
- ⑥ 联系接入点运营商检测 ODF 到接入点接入设备的链路是否可通信。



## 排查数据链路层故障

### 1. 若 VLAN ID 不为0时：

请确保运营商专线、腾讯云边界设备和本地 IDC 接入设备（包括 IDC 边界设备自身）之间的任何二层/三层设备，对您的 VLAN 标签启用了 VLAN 中继，即识别您的 VLAN 标签并允许其通过。

请确保腾讯云边界设备和您本地 IDC 边界设备（包括 IDC 边界设备自身）之间的任何二层/三层设备，对该 VLAN 进行正确的中继，且不存在 VLAN 转换的情况。

2. 请检查是否正确配置互联网 IP。确保本地 IDC 接入设备上 ARP 表项中，存在专线网关上互联 IP 对应的表项，且保持稳定，无 MAC 地址 flapping 记录。

3. 确保 IDC 接入设备上关闭 STP\Loop-detection 等二层链路环路检测协议。若开启 STP\Loop-detection 等二层链路环路检测协议，可能导致互联端口被协议阻塞。

## 排查网络层/传输层故障

1. 确保专线两端配置的 IP 地址属于同一个子网，并配置相同的子网掩码。

2. 确保专线两端配置的 IP 地址唯一，没有 IP 地址复用的情况。

3. 若您的专线开启了 BFD 双向检测，请确保 IDC 设备上的安全策略已放行 BFD 报文。

4. 若您的专线开启 NQA 检测，腾讯云标准支持的 NQA 探测类型是 ICMP-echo，请确保您的 IDC 设备上的安全策略已放行 ICMP 报文。

### 说明：

NQA 检测当前仅在专用通道2.0中支持，如果您当前为专用通道1.0，同时需要使用 NQA 检测功能，那么请联系腾讯技术人员或 [联系我们](#) 将专线切换为2.0。

5. 若需在专线两端建立 BGP 会话来实现腾讯云 VPC 路由和 IDC 路由传递：

请确保在 IDC 设备上正确配置 BGP ASN、BGP PEER IP。

请确保 BGP MD5 认证密钥两端保持完全一致。  
请确保 IDC 设备上的安全策略已放行 BGP 报文。  
请确保安全策略已放行建立 BGP 会话的 TCP 179 端口。

## 排查安全故障

### 排查 ACL 设置

请确保腾讯云子网 ACL 已放行来自或去往 IDC 业务主机的流量。  
请确保 IDC 子网 ACL 已放行来自或去往腾讯云 CVM 的流量。

### 排查安全组设置

请确保腾讯云 CVM 的安全组已放行来自或去往 IDC 业务主机的流量。  
请确保 IDC 安全组已放行来自或去往腾讯云 CVM 的流量。

## 排查路由问题

### VPC 型专线网关

#### 静态专用通道

请检查是否已正确配置 IDC 网段并成功传递至腾讯云 VPC。若未正确配置 IDC 业务地址，或 IDC 网段未传递到腾讯云 VPC，则腾讯云 VPC 访问该 IDC 服务器时路由将不可达，导致业务访问不通。

#### 1. 检查是否正确配置专用通道的 IDC 网段

1. 登录 [专线接入控制台](#)，在专用通道列表中单击目标专用通道 ID，在“高级配置”页签中查看**用户 IDC 网段**是否正确配置。
2. 若未正确配置 IDC 网段，请重新配置。具体操作请参见 [申请专用通道](#)。

#### 2. 检测是否正确配置路由表

1. 登录 [专线接入控制台](#)，在专用通道列表中单击目标专用通道 ID，在“基本信息”页签中单击私有网络 ID。
2. 在私有网络“基本信息”页签中单击**路由表**。
3. 在路由表“基本信息”页面查看路由表中是否正确配置目的端为 IDC 网段、下一跳为专线网关的路由策略，且状态为“启用”。
4. 若未配置目的端为 IDC 网段、下一跳为专线网关的路由策略，请重新配置。具体操作请参见 [配置路由表](#)。

#### BGP 专用通道

请确保专线网关已成功通过 BGP 协议学习到 IDC 网段，并正确传递至腾讯云 VPC。若专线网关未通过 BGP 协议学习到 IDC 网段，或 IDC 网段未传递到腾讯云 VPC，VPC 访问 IDC 服务器时路由将不可达，导致业务访问不通。

#### 检查 BGP 路由配置是否正确

1. 登录 [专线接入控制台](#)，在专用通道列表中单击目标专用通道 ID，在“高级配置”页签中查看 BGP 配置是否正确。
2. 若未正确配置，请重新配置。具体操作请参见 [申请专用通道](#)。

#### 检测是否正确配置路由表

1. 登录 [专线接入控制台](#)，在专用通道列表中单击目标专用通道 ID，在“基本信息”页签中单击私有网络 ID。
2. 在私有网络“基本信息”页签中单击[路由表](#)。
3. 在路由表“基本信息”页面查看路由表中是否正确配置目的端为 IDC 网段、下一跳为专线网关的路由策略，且状态为“启用”。
4. 若未配置目的端为 IDC 网段、下一跳为专线网关的路由策略，请重新配置。具体操作请参见 [配置路由表](#)。

## 云联网专线网关

### 静态专用通道

请检查是否正确配置专用通道的 IDC 网段，且 IDC 网段成功传递至云联网。若未正确配置 IDC 网段，或云联网未从专线网关学习到 IDC 网段，则腾讯云 VPC 访问该 IDC 服务器时路由将不可达，导致业务访问不通。

检查是否正确配置专用通道的 IDC 网段

1. 登录 [专线接入控制台](#)，在专用通道列表中单击目标专用通道 ID，在“高级配置”页签中查看[用户 IDC 网段](#)是否正确配置。
2. 若未正确配置 IDC 网段，请重新配置。具体操作请参见 [申请专用通道](#)。

检测是否为专线网关添加 IDC 网段

1. 登录 [专线接入控制台](#)，在专线网关列表中单击目标专线网关 ID。
2. 在专线网关详情页面单击 [IDC 网段](#) 页签，查看路由列表中是否正确配置 IDC 网段。
3. 若未配置 IDC 网段，请重新配置。具体操作请参见 [专线网关添加 IDC 网段](#)。

### BGP 专用通道

请检查专用通道 BGP 配置是否正确，且 IDC 网段成功传递至云联网。若专线网关未通过 BGP 协议学习到 IDC 网段，或云联网未从专线网关学习到 IDC 网段，则腾讯云 VPC 访问 IDC 服务器时路由将不可达，导致业务访问不通。

检查 BGP 路由配置是否正确

1. 登录 [专线接入控制台](#)，在专用通道列表中单击目标专用通道 ID，在“高级配置”页签中查看 BGP 配置是否正确。
2. 若未正确配置，请重新配置。具体操作请参见 [申请专用通道](#)。

检测是否为专线网关添加 IDC 网段

1. 登录 [专线接入控制台](#)，在专线网关列表中单击目标专线网关 ID。网段
2. 在专线网关详情页面单击 [IDC 网段](#) 页签，查看路由列表中查看是否正确配置 IDC 网段。
3. 若未配置 IDC 网段，请重新配置。具体操作请参见 [专线网关添加 IDC 网段](#)。

# 网络无法连通和数据丢包

最近更新时间：2024-01-13 16:02:36

## 现象描述

部分业务出现网络无法连通，数据丢包的现象，导致业务异常。

## 可能原因

故障可能原因如下：

**物理专线中断**：物理专线损坏，例如因施工导致的线缆被误挖断。

**带宽跑满**：专用通道带宽太小，不满足业务需求。

**安全策略配置不当**：云上、云下访问来回路径不一致。

**静态路由故障**：静态路由未绑定 BFD（双向转发检测机制）导致业务访问异常。

**BGP 路由故障**：BGP 路由条目超过产品限制。

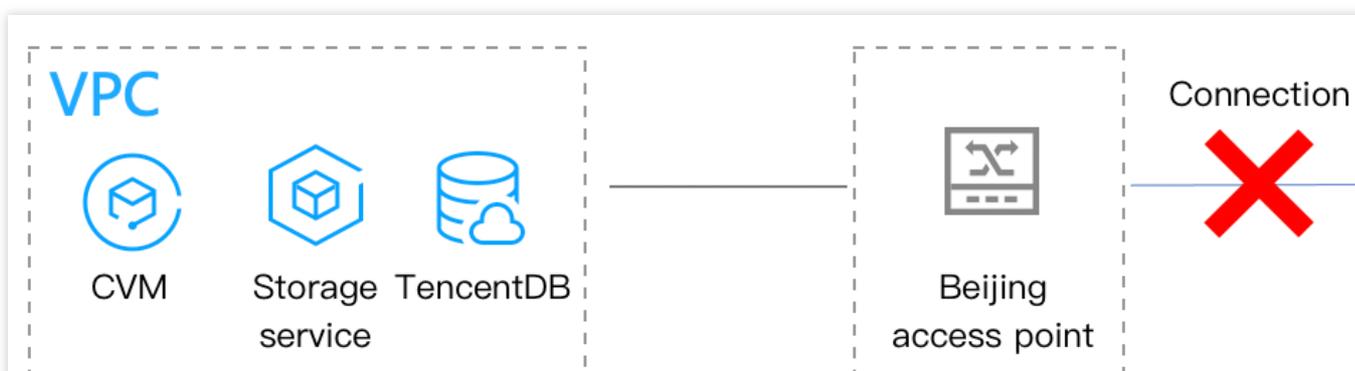
**IP 地址冲突**：云上地址空间和 VPC 地址空间重叠。

## 处理方案

### 物理专线中断

#### 单点单线模式

用户 IDC 通过一条物理专线与一个腾讯云接入点相连，再连接至腾讯云 VPC。若专线中断时，业务直接中断。

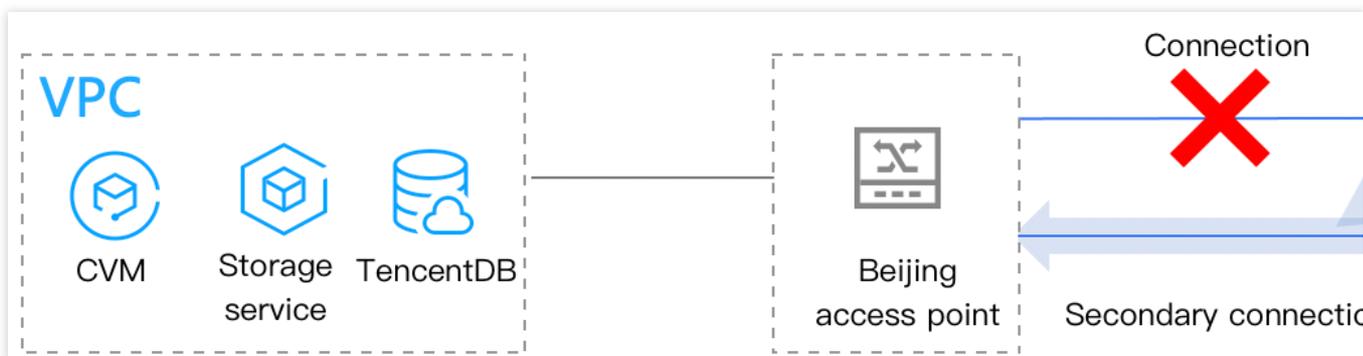


#### 解决方法

收集专线线路 ID，并联系运营商报障。单点单线接入模式的专线不具备容灾能力，建议您合理规划物理线路，提升专线网络架构的稳定性和高可用性，物理线路规划请参见 [网络规划](#)。

### 单点双线模式

双线单接入点模式中，用户 IDC 通过两条物理专线与一个腾讯云接入点连接，再连接至腾讯云 VPC。若某一条物理专线中断时，触发容灾。



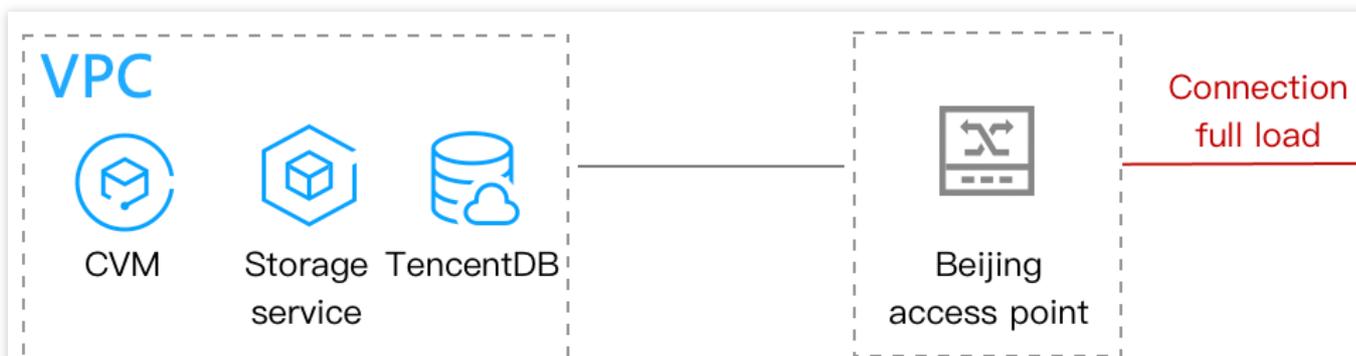
#### 解决方法

1. 当专线故障后，请及时通过业务监控系统确认是否业务受损。
2. 触发容灾后，请收集流量切换带来的云上、云下访问的延时和路径变化，判断备用专线是否正常使用。
3. 若备用专线不能正常使用，则通过收集的 ping 和 traceroute 测试信息来定位问题。

### 带宽跑满

#### 单点单专线模式

用户 IDC 通过一条物理专线与一个腾讯云接入点相连，再连接至腾讯云 VPC。若专用通道带宽跑满时，则会产生丢包，导致数据丢失。



#### 解决方法

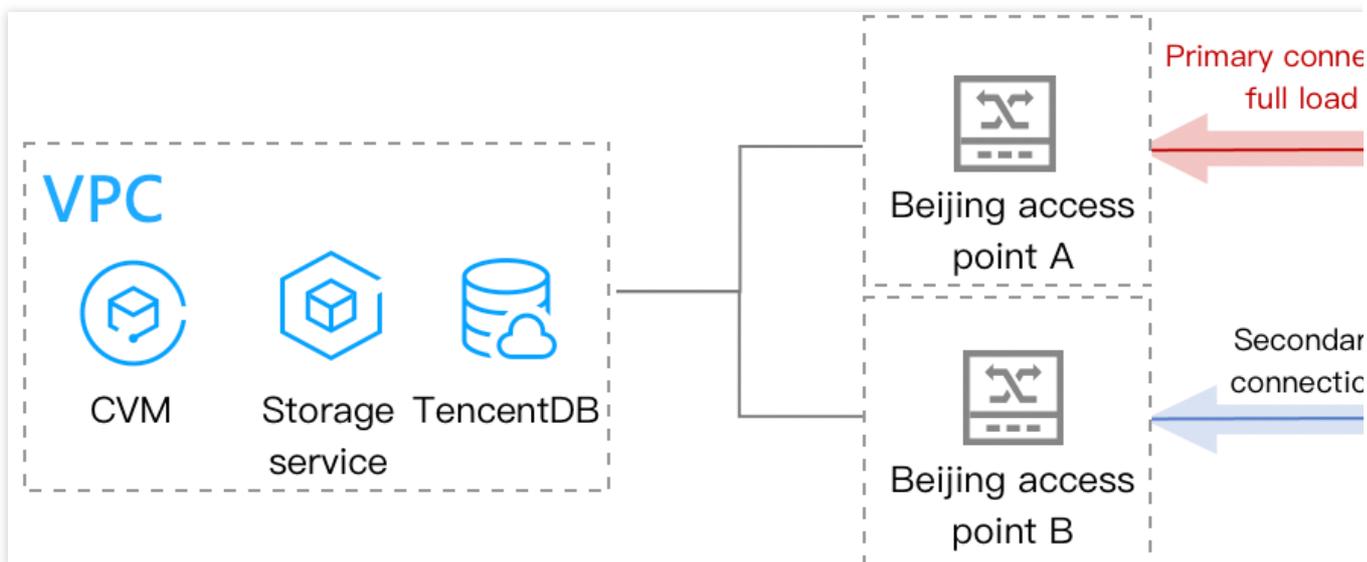
1. 登录 [专线接入控制台](#)，在“变更专用通道”页面调整带宽，具体操作请参见 [变更通道](#)。
2. 若您的专用通道带宽上限已达物理专线上限，请先在业务侧进行容灾切换，然后联系专线经理扩容专线。
3. 在业务优先恢复的同时，需要对导致流量跑满原因进行溯源。

#### 双线双接入点模式

用户 IDC 分别通过一条物理专线与同地域两个腾讯云接入点相连，再连接至腾讯云 VPC。

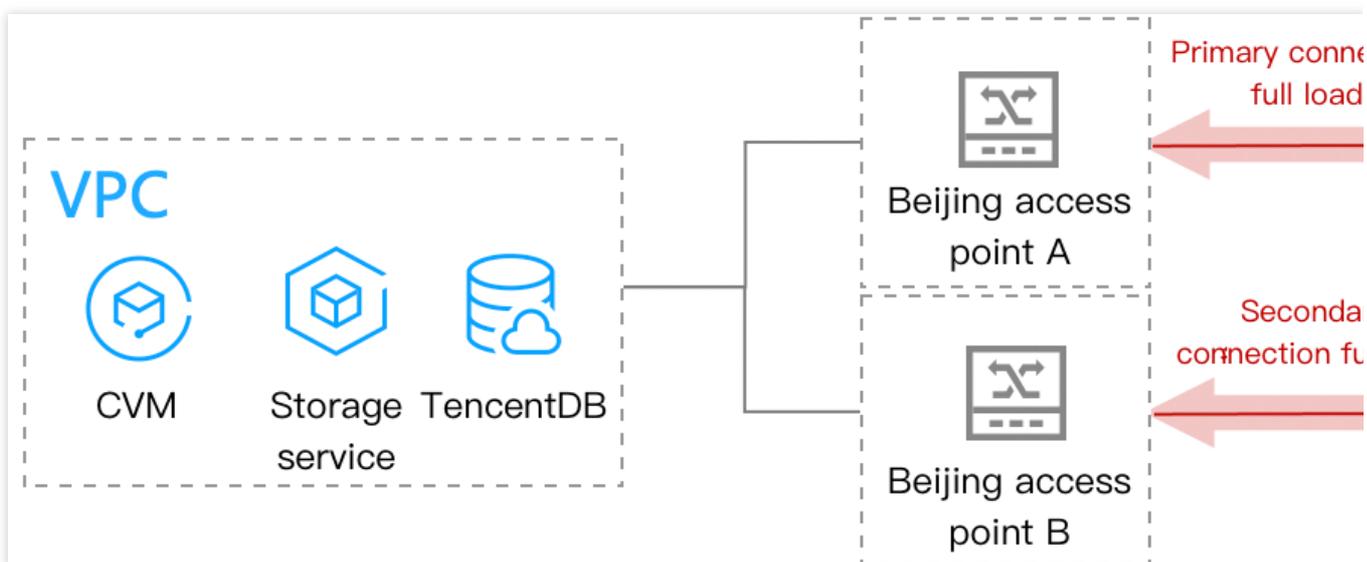
### 主备模式

若主专线的业务带宽跑满时，则会产生丢包，导致数据丢失。可以通过将两条专线的主备模式调整为负载模式，减轻线路流量压力，恢复业务数据。



### 负载模式

若主专线和备用专线均满载，则会产生丢包，导致数据丢失。



### 解决方法

3.1 登录 [专线接入控制台](#)，在“变更专用通道”页面调整带宽，具体操作请参见 [变更通道](#)。

3.2 若您的专用通道带宽上限已达物理专线上限：

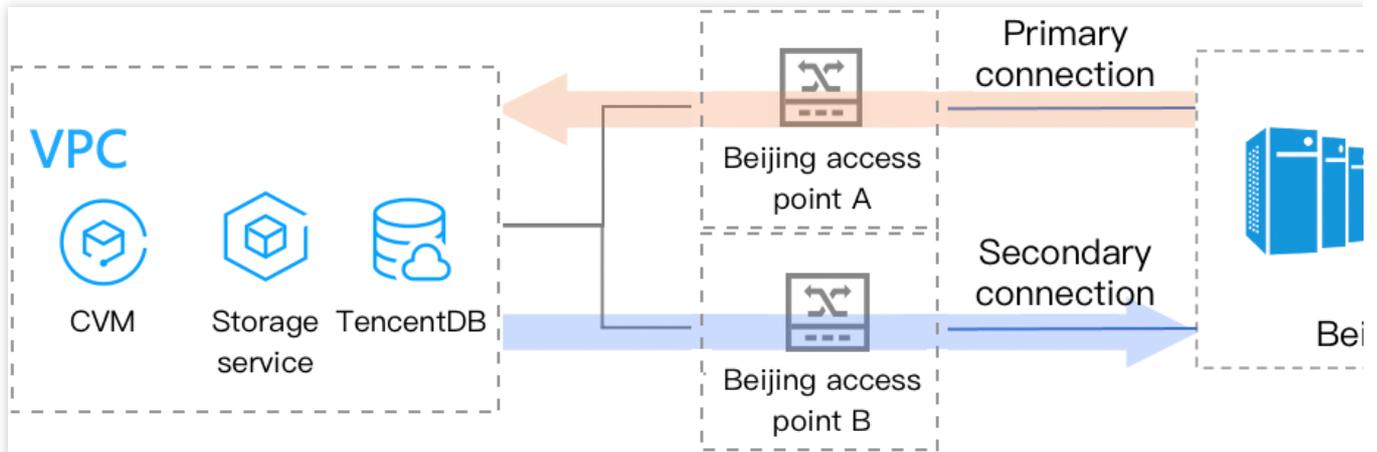
主备模式：将两条专线的主备模式调整为负载模式，减轻线路流量压力，恢复业务数据。

负载模式：请先在业务侧进行容灾切换，然后联系专线经理扩容专线。

3.3 在业务优先恢复的同时，需要对导致流量跑满原因进行溯源。

### 安全策略配置不当

用户 IDC 分别通过一条物理专线与同地域两个腾讯云接入点相连，再连接至腾讯云 VPC。若 IDC 访问腾讯云 VPC 通过主专线，腾讯云 VPC 访问 IDC 通过备专线，来回路径不一样，会导致专线流量不通。



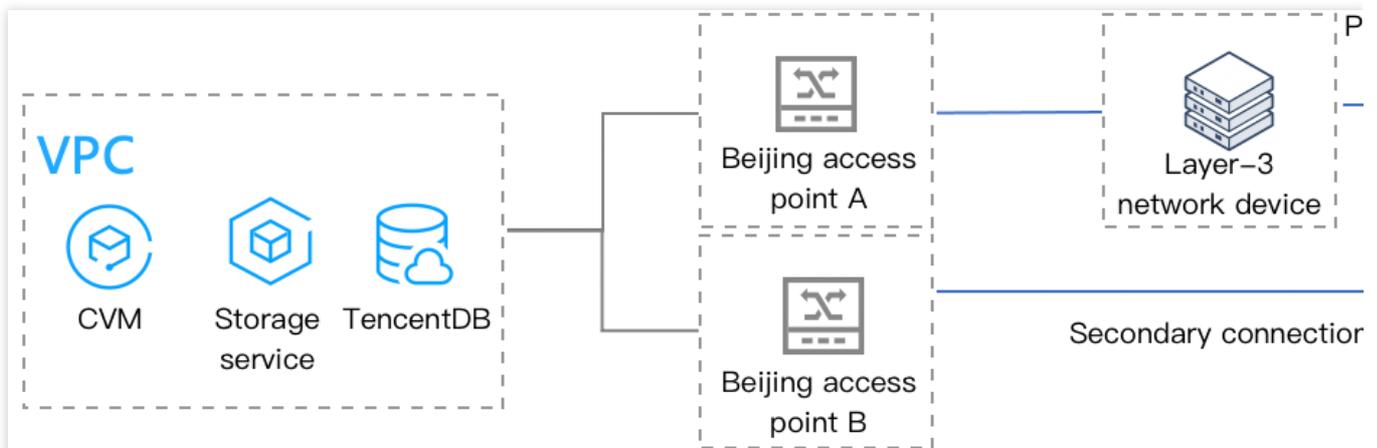
**解决方法**

1. 检查主专线和备专线上是否接入了不同的安全设备（如防火墙），若接入安全设备，则需确保两个安全设备策略一致，且对双向的报文进行安全策略放行。
2. 更新安全策略后，在 IDC 的边界设备上配置 IDC 的业务 IP（该业务 IP 必须是闲置或经业务部门确认可用于测试），然后在边界设备上用该业务 IP 访问云上的业务 IP，测试是否通信正常。
3. 若上述两个操作仍未解决您的问题，则故障可能在 IDC 内部，请自行定位排查。

**静态路由故障**

用户 IDC 分别通过一条物理专线与同地域两个腾讯云接入点相连，再连接至腾讯云 VPC。

若主专线串接了三层设备，当 IDC 侧设备端口异常或者三层设备到 IDC 之间的链路异常时，接入点 A 无法感知且不会触发告警。这种情况下，专用通道的静态路由仍然会发送给专线网关，因此流量仍将被转发至故障的专线上导致业务不通。



**解决方法**

建议您配置 BFD。在静态路由关联两端配置 BFD 后，会定期发送探测包，若一段时间内没有收到对端发送的回复，则判定对端故障，与之关联的路由随之失效且不会转发至专线网关。

具体步骤：[提工单](#) 申请开启专用通道 BFD 功能，腾讯云后台将下发配置。

**说明：**

腾讯云默认的 BFD 为动态 BFD，本端 TX Interval 等于 MAX（本端 Desired Min TX Interval，对端 Required Min RX Interval）。

若专用通道为1.0 版本：

若在2019年10月1日之前申请，Desired Min TX Interval 和 Required Min RX Interval 均为100ms，Detect Mult 为 3。

若在2019年10月1日及以后申请，Desired Min TX Interval 和 Required Min RX Interval 均为300ms，Detect Mult 为 3。

若专用通道为2.0 版本：

Desired Min TX Interval 和 Required Min RX Interval 最小为1000ms，Detect Mult 为 3。

**BGP 路由故障**

每条专用通道可接受的 BGP 路由条目数为100条，超过的路由将不会被接受，导致业务故障。

**解决方法**

请合理规划网络地址，进行 CIDR 子网合并，减少 IDC 发往腾讯云 VPC 的路由条目数。

**IP 地址冲突**

云上 VPC 和云下 IDC 均遵循 TCP/IP 协议的网络空间，基于目的 IP 进行三层寻址，基于目的 MAC 进行二层寻址。因此，在混合云场景中，可能因为云上地址空间和 VPC 地址空间重叠导致 IP 地址冲突、业务访问受限的问题。

**解决方法**

1. 进行合理的网络规划。

1.1 将腾讯云 VPC 和本地 IDC 的地址进行统一规划。

1.2 将互联 IP 等网络地址进行全局统一规划。

2. 若业务场景不允许进行网络拆分再规划，可以使用 NAT 型的专线网关，实现 VPC 的地址进行本端地址转换和 IDC 的对端地址转换功能，进而实现 VPC 和 IDC 两端地址的彼此隐藏。具体操作请参见 [配置网络地址转换 \(NAT\)](#)。

**说明：**

每个 NAT 型的专线网关本端 IP 转换和对端 IP 转换规则数量分别都是100条。