阿里云
高速通道

最佳实践

文档版本：20190807

法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。
2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。
3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。
4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的”现状“、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。
5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含”阿里云”、Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。
6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

格式	说明	样例
	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	 **禁止:** 重置操作将丢失用户配置数据。
	该类警示信息可能导致系统重大变更甚至故障，或者导致人身伤害等结果。	 **警告:** 重启操作将导致业务中断，恢复业务所需时间约10分钟。
	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	 **说明:** 您也可以通过按Ctrl + A选中全部文件。
>	多级菜单递进。	设置 > 网络 > 设置网络类型
粗体	表示按键、菜单、页面名称等UI元素。	单击 **确定**。
`courier` 字体	命令。	执行 `cd /d C:/windows` 命令，进入Windows系统文件夹。
*## *	表示参数、变量。	`bae log list --instanceid` *`Instance_ID`*
[]或者[a|b]	表示可选项，至多选择一个。	`ipconfig` *`[-all|-t]`*
{}或者{a|b}	表示必选项，至多选择一个。	`swich` *`{stand | slave}`*

目录

1 通过物理专线访问VPC中的云服务

AnyTunnel地址

AnyTunnel地址指的是每个VPC中100.64.0.0/10内的地址，用于VPC中DNS、YUM、NTP、OSS或SLS等云服务中使用。

当您需要从本地数据中心通过物理专线访问VPC中的云服务时，需要在边界路由器（VBR）中将100.64.0.0/10网段的路由条目指向VPC方向的路由器接口，并在本地数据中心的网关设备上将100.64.0.0/10网段的路由指向VBR的阿里云侧互联IP。

> 说明:
> 由于100.64.0.0/10网段属于VPC中的保留网段，因此不能直接在VBR中添加目的网段为100.64.0.0/10的路由条目。需要将该网段拆分成100.64.0.0/11和100.96.0.0/11，在VBR中配置两个路由条目。

在VBR中配置路由

1. 登录高速通道管理控制台。
2. 在左侧导航栏中，单击物理专线连接 > 边界路由器。
3. 在目标边界路由器的操作列中，单击管理。
4. 在边界路由器详情页，单击添加路由，填写参数。在此例中配置如下：
   - 目标网段：分别为100.64.0.0/11和100.96.0.0/11
   - 下一跳方向：指向VPC方向
   - 下一跳：选择数据包的出口，在本教程中即VBR的路由器接口。
5. 单击确定，完成配置。

配置专线客户侧接入设备路由

在专线客户侧的接入设备上，增加指向阿里云的静态路由：

```
ip route 100.64.0.0/10 {阿里侧互联ip}
```

2 物理专线网络性能测试方法

物理专线接入完成后，您需要对物理专线的性能进行测试，确保物理专线可以满足您的业务需求。

前提条件

在测试前，确保您完成以下环境准备：

- 完成物理专线接入和路由配置。本地IDC与VPC必须由一根专线连通。
- 准备1台本地IDC网络接入设备: 被压力测试网络PPS的IDC网络接入设备，可作为Netperf或iperf3测试中的客户端或服务器端。

  本操作中，IDC网络设备的IP地址为：192.168.100.1。
- 准备8台专有网络ECS实例：作为Netperf或iperf3测试中的客户端端或服务器端。与本地IDC网络接入设备之间建立控制连接，传递测试配置相关的信息，以及测试结果。

  本操作中使用8台规格为ecs.se1.2xlarge 镜像为centos_7_2_64_40G_base_20170222.vhd的ECS实例，IP地址为172.16.0.2 – 172.16.0.9。

搭建测试环境

安装Netperf

Netperf是一个网络性能的测量工具，主要针对基于TCP或UDP传输。

完成以下操作，分别在IDC网络设备和8台ECS实例上安装Netperf：

1. 执行以下命令下载Netperf。

```
wget -c "https://codeload.github.com/HewlettPackard/netperf/tar.gz/
netperf-2.5.0" -O netperf-2.5.0.tar.gz
```

2. 执行以下命令安装Netperf。

```
tar -zxvf netperf-2.5.0.tar.gz
cd netperf-netperf-2.5.0
./configure
make
make install
```

3. 执行`netperf -h`和`netserver -h`验证安装是否成功。

安装iPerf3

Iperf3是一个网络性能测试工具。Iperf3可以测试最大TCP和UDP带宽性能。

完成以下操作，分别在IDC网络设备和8台ECS实例上安装iPerf3：

1. 执行以下命令下载iPerf3。

```
yum install git -y
git clone https://github.com/esnet/iperf
```

2. 执行以下命令安装iPerf3。

```
cd iperf
./configure && make && make install && cd ..
cd src
ADD_PATH="$(pwd)"
PATH="${ADD_PATH}:${PATH}"
export PATH
```

3. 执行命令`iperf3 -h`，验证安装是否成功。

开启多队列功能

在IDC网络接入设备内部执行以下命令，开启多队列功能。（假设与物理专线相连的接口为eth0。）

```
ethtool -L eth0 combined 4
echo "ff" > /sys/class/net/eth0/queues/rx-0/rps_cpus
echo "ff" > /sys/class/net/eth0/queues/rx-1/rps_cpus
echo "ff" > /sys/class/net/eth0/queues/rx-2/rps_cpus
echo "ff" > /sys/class/net/eth0/queues/rx-3/rps_cpus
```

使用Netperf工具测试物理专线的包转发性能

Netperf安装完成后会创建两个命令行工具：netserver（服务器端）和netperf（客户端）。两个工具的主要参数说明如下表所示。

工具名称	主要参数	参数说明
Netserver（服务器端：接收端工具）	-p	监听的的端口号。
netperf（客户端：发送端工具）	-H	IDC网络接入设备或VPC服务器的IP地址。
	-p	IDC网络接入设备或VPC服务器的端口。
	-l	运行时间。
	-t	发送报文的协议类型：TCP_STREAM 或 UDP_STREAM。 建议使用UDP_STREAM。

工具名称	主要参数	参数说明
	-m	数据包大小。 · 测试pps（packet per second）时，建议设置为1。 · 测试bps（bit per second）时，建议设置为1400。

测试收方向

1. 在IDC网络接入设备内启动netserver进程，指定不同端口，如下所示：

```
netserver -p 11256
netserver -p 11257
netserver -p 11258
netserver -p 11259
netserver -p 11260
netserver -p 11261
netserver -p 11262
netserver -p 11263
```

2. 在VPC内的8台ECS实例上启动netperf进程，分别指定到IDC网络接入设备的不同netserver端口。

```
netperf -H 192.168.100.1 -p 11256 -t UDP_STREAM -l 300 -- -m 1 #第一台
netperf -H 192.168.100.1 -p 11257 -t UDP_STREAM -l 300 -- -m 1 #第二台
netperf -H 192.168.100.1 -p 11258 -t UDP_STREAM -l 300 -- -m 1 #第三台
netperf -H 192.168.100.1 -p 11259 -t UDP_STREAM -l 300 -- -m 1 #第四台
netperf -H 192.168.100.1 -p 11260 -t UDP_STREAM -l 300 -- -m 1 #第五台
netperf -H 192.168.100.1 -p 11261 -t UDP_STREAM -l 300 -- -m 1 #第六台
netperf -H 192.168.100.1 -p 11262 -t UDP_STREAM -l 300 -- -m 1 #第七台
netperf -H 192.168.100.1 -p 11263 -t UDP_STREAM -l 300 -- -m 1 #第八台
```

3. 如果需要测试bps，将上述命令修改为：

```
netperf -H 192.168.100.1 -p 11256 -t UDP_STREAM -l 300 -- -m 1400
 #第一台
netperf -H 192.168.100.1 -p 11257 -t UDP_STREAM -l 300 -- -m 1400
 #第二台
netperf -H 192.168.100.1 -p 11258 -t UDP_STREAM -l 300 -- -m 1400
 #第三台
netperf -H 192.168.100.1 -p 11259 -t UDP_STREAM -l 300 -- -m 1400
 #第四台
netperf -H 192.168.100.1 -p 11260 -t UDP_STREAM -l 300 -- -m 1400
 #第五台
netperf -H 192.168.100.1 -p 11261 -t UDP_STREAM -l 300 -- -m 1400
 #第六台
```

```
netperf -H 192.168.100.1 -p 11262 -t UDP_STREAM -l 300 -- -m 1400
 #第七台
netperf -H 192.168.100.1 -p 11263 -t UDP_STREAM -l 300 -- -m 1400
 #第八台
```

测试发方向

1. 在8台VPC ECS实例内启动netserver进程，指定端口，如下所示：

```
netserver -p 11256
```

2. 在IDC网络接入设备内启动8个netperf进程，指定为不同IP地址。

```
 netperf -H 172.16.0.2 -p 11256 -t UDP_STREAM -l 300 -- -m 1 #第一台
ECS实例
 netperf -H 172.16.0.3 -p 11256 -t UDP_STREAM -l 300 -- -m 1 #第二台
ECS实例
 netperf -H 172.16.0.4 -p 11256 -t UDP_STREAM -l 300 -- -m 1 #第三台
ECS实例
 netperf -H 172.16.0.5 -p 11256 -t UDP_STREAM -l 300 -- -m 1 #第四台
ECS实例
 netperf -H 172.16.0.6 -p 11256 -t UDP_STREAM -l 300 -- -m 1 #第五台
ECS实例
 netperf -H 172.16.0.7 -p 11256 -t UDP_STREAM -l 300 -- -m 1 #第六台
ECS实例
 netperf -H 172.16.0.8 -p 11256 -t UDP_STREAM -l 300 -- -m 1 #第七台
ECS实例
 netperf -H 172.16.0.9 -p 11256 -t UDP_STREAM -l 300 -- -m 1 #第八台
ECS实例
```

3. 如果需要测试bps，将上述命令修改为：

```
 netperf -H 192.168.100.1 -p 11256 -t UDP_STREAM -l 300 -- -m 1400
 #第一台ECS实例
 netperf -H 192.168.100.1 -p 11257 -t UDP_STREAM -l 300 -- -m 1400
 #第二台ECS实例
 netperf -H 192.168.100.1 -p 11258 -t UDP_STREAM -l 300 -- -m 1400
 #第三台ECS实例
 netperf -H 192.168.100.1 -p 11259 -t UDP_STREAM -l 300 -- -m 1400
 #第四台ECS实例
 netperf -H 192.168.100.1 -p 11260 -t UDP_STREAM -l 300 -- -m 1400
 #第五台ECS实例
 netperf -H 192.168.100.1 -p 11261 -t UDP_STREAM -l 300 -- -m 1400
 #第六台ECS实例
 netperf -H 192.168.100.1 -p 11262 -t UDP_STREAM -l 300 -- -m 1400
 #第七台ECS实例
 netperf -H 192.168.100.1 -p 11263 -t UDP_STREAM -l 300 -- -m 1400
 #第八台ECS实例
```

分析测试结果

客户端的netperf进程执行完毕后，会显示如下结果。

```
Socket  Message  Elapsed      Messages
Size    Size     Time         Okay Errors   Throughput
bytes   bytes    secs            #      #   10^6bits/sec
124928       1   10.00     4532554      0       3.63
```

```
    212992             10.00      1099999                0.88
```

显示结果中各字段含义如下表所示。

字段	含义
Socket Size	缓冲区大小
Message Size	数据包大小（Byte）
Elapsed Time	测试时间（s）
Message Okay	发送成功的报文数
Message Errors	发送失败的的报文数
Throughput	网络吞吐量（Mbit/s）

通过发送成功的报文数除以测试时间，即可算出测试链路的pps，即pps=发送成功的报文数/测试时间。

使用iPerf3测试物理专线的带宽

iPerf3的主要参数说明如下表所示。

工具名称	主要参数	参数说明
iPerf3	-s	表示作为服务器端接收数据。
	-i	设置每次报告之间的时间间隔，单位为秒。
	-p	指定服务端的监听端口。
	-u	表示使用UDP协议发送报文。若不指定该参数则表示使用TCP协议。
	-l	设置读写缓冲区的长度。通常测试包转发性能是建议该值设为16，测试带宽是建议该值设为1400。
	-b	UDP模式使用的带宽，单位bits/s。
	-t	设置传输的总时间。Iperf在指定的时间内，重复的发送指定长度的数据包，默认值为10秒。

工具名称	主要参数	参数说明
	-A	设置CPU亲和性，可以将的iPerf3进程绑定对应编号的逻辑CPU，避免iPerf3的进程在不同的CPU间被调度。

测试收方向

1. 在IDC网络接入设备中以server模式启动iperf3进程，指定不同端口，如下所示：

```
iperf3 -s -i 1 -p 16001
iperf3 -s -i 1 -p 16002
iperf3 -s -i 1 -p 16003
iperf3 -s -i 1 -p 16004
iperf3 -s -i 1 -p 16005
iperf3 -s -i 1 -p 16006
iperf3 -s -i 1 -p 16007
iperf3 -s -i 1 -p 16008
```

2. 在VPC ECS实例上以client模式启动iperf3进程，分别指定到IDC网络接入设备的不同端口。

```
iperf3 -u -l 16 -b 100m -t 120 -c 192.168.100.1 -i 1 -p 16001 -A 1
iperf3 -u -l 16 -b 100m -t 120 -c 192.168.100.1 -i 1 -p 16002 -A 2
iperf3 -u -l 16 -b 100m -t 120 -c 192.168.100.1 -i 1 -p 16003 -A 3
iperf3 -u -l 16 -b 100m -t 120 -c 192.168.100.1 -i 1 -p 16004 -A 4
iperf3 -u -l 16 -b 100m -t 120 -c 192.168.100.1 -i 1 -p 16005 -A 5
iperf3 -u -l 16 -b 100m -t 120 -c 192.168.100.1 -i 1 -p 16006 -A 6
iperf3 -u -l 16 -b 100m -t 120 -c 192.168.100.1 -i 1 -p 16007 -A 7
iperf3 -u -l 16 -b 100m -t 120 -c 192.168.100.1 -i 1 -p 16008 -A 8
```

测试发方向

1. 在每个VPC ECS实例上server模式启动iperf3进程并指定端口。

```
iperf3 -s -i 1 -p 16001
```

2. 在IDC接入设备上以client模式启动8个iperf3进程，`-c`的值为各个陪练机的IP地址。

```
iperf3 -u -l 16 -b 100m -t 120 -c 172.16.0.2 -i 1 -p 16001 -A 1
iperf3 -u -l 16 -b 100m -t 120 -c 172.16.0.3 -i 1 -p 16001 -A 2
iperf3 -u -l 16 -b 100m -t 120 -c 172.16.0.4 -i 1 -p 16001 -A 3
iperf3 -u -l 16 -b 100m -t 120 -c 172.16.0.5 -i 1 -p 16001 -A 4
iperf3 -u -l 16 -b 100m -t 120 -c 172.16.0.6 -i 1 -p 16001 -A 5
iperf3 -u -l 16 -b 100m -t 120 -c 172.16.0.7 -i 1 -p 16001 -A 6
iperf3 -u -l 16 -b 100m -t 120 -c 172.16.0.8 -i 1 -p 16001 -A 7
iperf3 -u -l 16 -b 100m -t 120 -c 172.16.0.9 -i 1 -p 16001 -A 8
```

分析测试结果

客户端的iPerf3进程执行完毕后，会显示如下结果。

```
[ ID]  Interval        Transfer    Bandwidth      Jitter    Lost/Total
 Datagrams
[  4]  0.00-10.00 sec  237 MBytes  199 Mbits/sec  0.027 ms  500/30352
 (1.6%)
```

```
[  4]  Sent 30352  datagrams
```

显示结果中各字段含义如下表所示。

字段	含义
Transfer	传输的总数据量
Bandwidth	带宽大小
Jitter	抖动
Lost/Total Datagrams	丢失报文数/总报文数（丢包率）

PPS=对端收到的包／时间

 说明:

建议您在server端运行`sar`命令来统计实际收到的包并作为实际结果，例如：`sar -n DEV 1 320`。

阿里云侧速率限制

除了物理专线的限制外，VPC与本地数据中心之间的通信还受到以下限制。

- OSS的读写速率上限为5Gbit/s。
- 为了提高可靠性，从VPC到边界路由器（VBR）方向的单个hash流，在阿里云内部被限速为“高速通道规格带宽/12”。例如VBR到VPC的带宽为large1，即1Gbps带宽，则单个hash流的最大带宽为85Mbps。

  hash流定义：源IP地址、源端口、传输层协议、目的IP地址和目的端口，这五个量组成的一个集合所定义的数据流。 例如：“192.168.1.1 10000 TCP 121.14.88.76 80”就构成了一个hash流。即一个IP地址为192.168.1.1的终端通过端口10000，利用TCP协议，和IP地址为121.14.88.76，端口为80的终端进行的连接就是一个hash流。

3 通过高速通道实现就近接入和一点接入连接全球

功能概述

高速通道可以帮助您在本地IDC和部署在各地域的阿里云VPC之间建立高质量、高可靠的内网通信。阿里云高速通道产品有如下两大核心功能。

- VPC互连

  高速通道支持位于相同地域或不同地域，同一账号或不同账号的VPC之间进行内网互通。目前同地域间的VPC互连不收取费用。

  阿里云通过在两侧VPC的路由器上分别创建路由器接口，以及自有的骨干传输网络来搭建高速通道，轻松实现两个VPC之间安全可靠，方便快捷的通信。详情参见VPC互连。

- 专线接入

  您可以通过物理专线在物理层面上连接您的本地数据中心到阿里云，然后建立边界路由器和路由器接口来连接数据中心与阿里云VPC。详情参见物理专线接入。

就近接入

用户在使用专线将本地IDC和阿里云VPC互连时，选择距离本地IDC最近的接入点即可，无需在本地IDC和VPC所在地域间建立专线。其中接入点分为阿里云自有接入点和合作伙伴接入点。

- 阿里云自有接入点

  您可以通过高速通道控制台的专线接入点信息来获取阿里云自有接入点的信息。如果您的本地IDC位于接入点所在的城市，您可以直接申请专线接入到这些接入点。

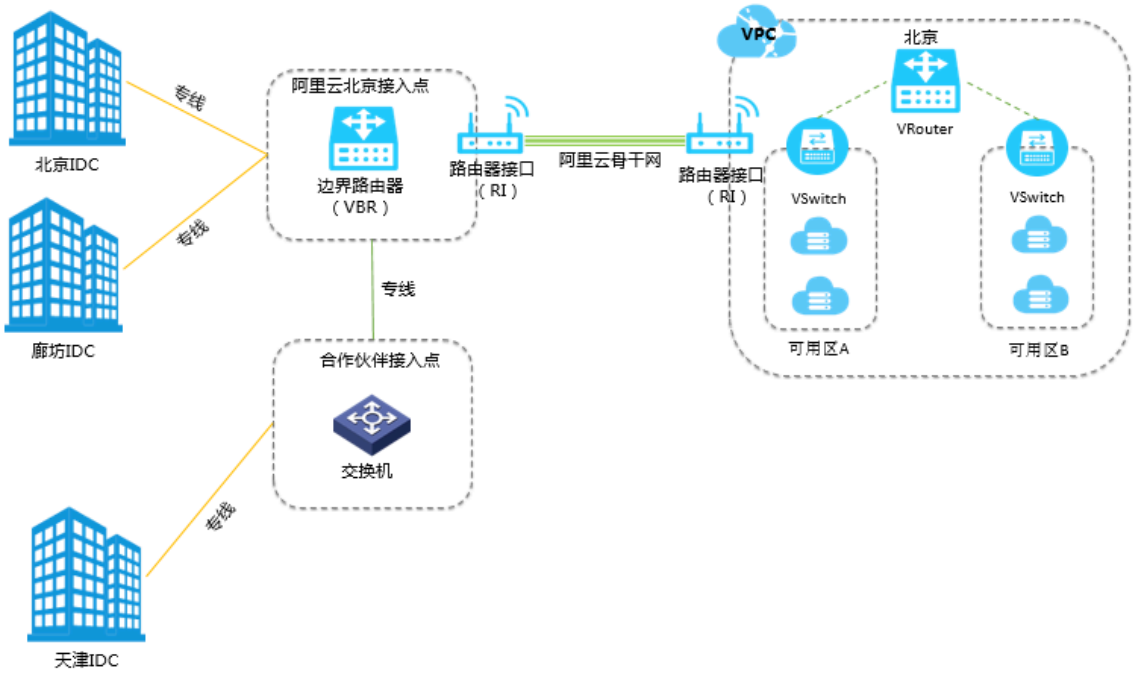
- 合作伙伴接入点

  合作伙伴的接入点已经提前和阿里云建立了专线连接，您只需要在本地IDC和合作伙伴接入点间建立专线连接就可以实现本地IDC和云上VPC间的内网互连。您可以参考高速通道控制台的合作伙伴信息，并联系阿里云合作伙伴获取专线接入的相关信息。

  如果您的本地IDC所在城市既没有阿里云自有接入点，也没有阿里云合作伙伴接入点，您可以自行选择一个距离您的本地IDC较近的接入点，在IDC和该接入点之间建立连接即可。

  例如，一个用户在北京、天津和廊坊各有一个本地IDC，那么该用户可以根据以下策略进行专线接入：

  - 由于北京有阿里云的自有接入点，该用户只需使用专线把位于北京的IDC和阿里云北京接入点连接即可。
  - 由于天津没有阿里云的自有接入点，但有合作伙伴接入点，该用户可以使用专线把位于天津的IDC和天津的合作伙伴接入点连接起来即可。
  - 廊坊既没有阿里云的自有接入点，也没有合作伙伴接入点，由于位于廊坊的IDC距离阿里云北京接入点距离较近，该用户可以使用专线把位于廊坊的IDC和阿里云北京接入点连接。
  - 说明：
    下图中只有黄色的专线是该用户需要找运营商或者合作伙伴施工的线路。



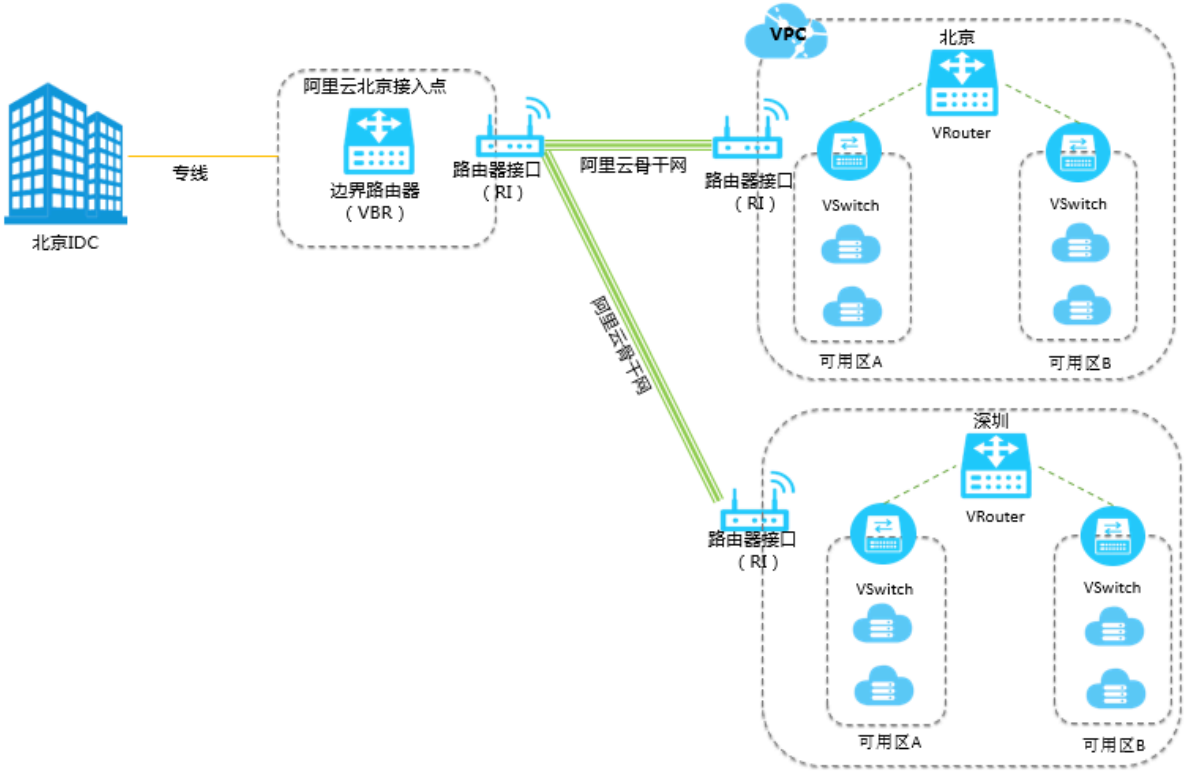
一点接入连接全球

您只需要接入任何一个接入点，就可以通过该接入点和阿里云遍布全球各地域的VPC连接起来。

例如，一个用户需要将位于北京的IDC通过专线接入到位于北京和深圳的VPC。此时，该用户只需要用一条专线将IDC连接至到阿里云北京接入点，然后在边界路由器（VBR）上创建两个分别连接至两个VPC的路由器接口（RI）即可。

说明:

下图中只有黄色的专线是该用户需要找运营商或者合作伙伴施工的线路。



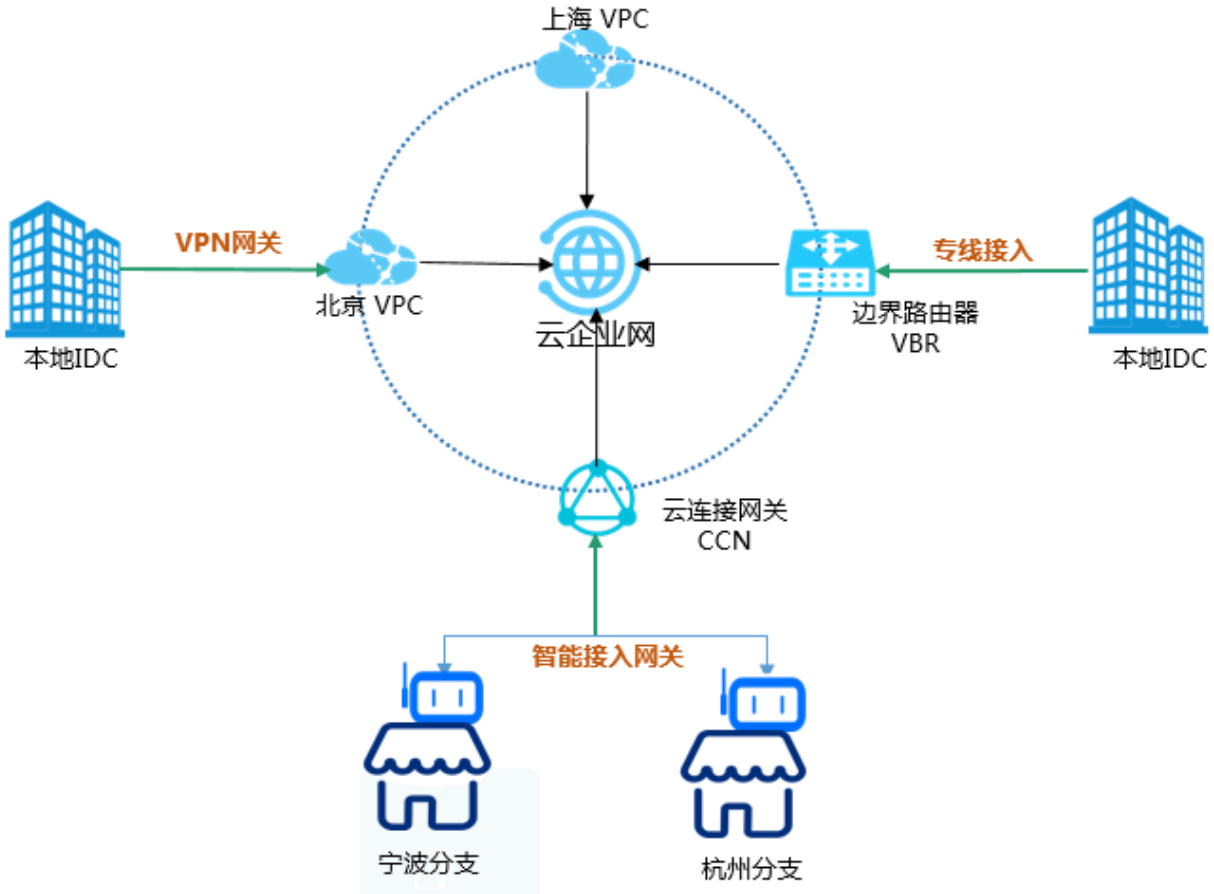
4 连接本地IDC

您可以通过VPN网关、高速通道物理专线、智能接入网关将本地数据中心和云上VPC打通，构建混合云。

概述

您可以在本地数据中心和阿里云专有网络间建立私网通信，构建混合云。然后将本地的IT基础架构无缝地扩展到阿里云上，借助阿里云海量的计算、存储、网络、CDN资源，应对业务波动，提高应用的稳定性。

您可以通过VPN网关、高速通道物理专线、智能接入网关将本地数据中心和云上VPC打通。并且，可以通过云企业网实现全球网络互通。



连接方案

方案	说明
VPN接入	您可以通过VPN网关的IPsec-VPN将本地数据中心和VPC连接起来。VPN网关默认包含了两个不同的网关实例形成主备双机热备，主节点故障时自动切换到备节点。 VPN网关基于Internet通信，网络延迟和可用性取决于Internet。如果您对网络延迟没有特别高的需求，建议您选择VPN网关。 配置详情，请参见建立VPC到本地数据中心的连接。
专线接入	您可以通过租用一条运营商的专线将本地数据中心连接到阿里云接入点，建立专线连接。高速通道提供自主接入和一站式接入服务。 物理专线接入网络质量好，带宽高。如果您对网络质量有很高的要求，建议您选择高速通道专线接入。 配置详情，请参见#unique_11。
冗余专线接入	通过冗余物理专线将您的本地数据中心接入到阿里云，在您的本地数据中心和阿里云上的VPC间建立高质量、高可靠的内网通信。阿里云目前支持最多4条物理专线实现等价多路径路由（ECMP）。 配置详情，请参见冗余专线接入。
智能接入网关接入	智能接入网关（Smart Access Gateway）是阿里云提供的一站式快速上云解决方案。企业可通过智能接入网关实现Internet就近加密接入，获得更加智能、更加可靠、更加安全的上云体验。 智能接入网关配置简单，成本低。如果您有多个本地分支上云的需求，建议您选择智能接入网关。 配置详情，请参见智能接入网关上云。
通过BGP主备链路接入	通过专线接入和云企业网组合的方式，实现本地IDC通过主备链路上云，并和云上不同地域VPC互通。 配置详情，请参见IDC通过BGP主备链路上云方案。

方案	说明
专线备份接入	将智能接入网关作为已有物理专线的备用链路接入阿里云，构建高可用的混合云环境。 配置详情，请参见专线备份配置教程。

5 对等连接迁移至云企业网

5.1 已使用对等连接的VPC迁移至云企业网

您可以将已使用高速通道对等连接的专有网络（VPC）平滑迁移至云企业网。云企业网（Cloud Enterprise Network, CEN）可以在不同专有网络之间，专有网络与本地数据中心间搭建私网通信通道。通过自动路由分发及学习，CEN可以提高网络的快速收敛和跨网络通信的质量和安全性，实现全网资源的互通。

警告:

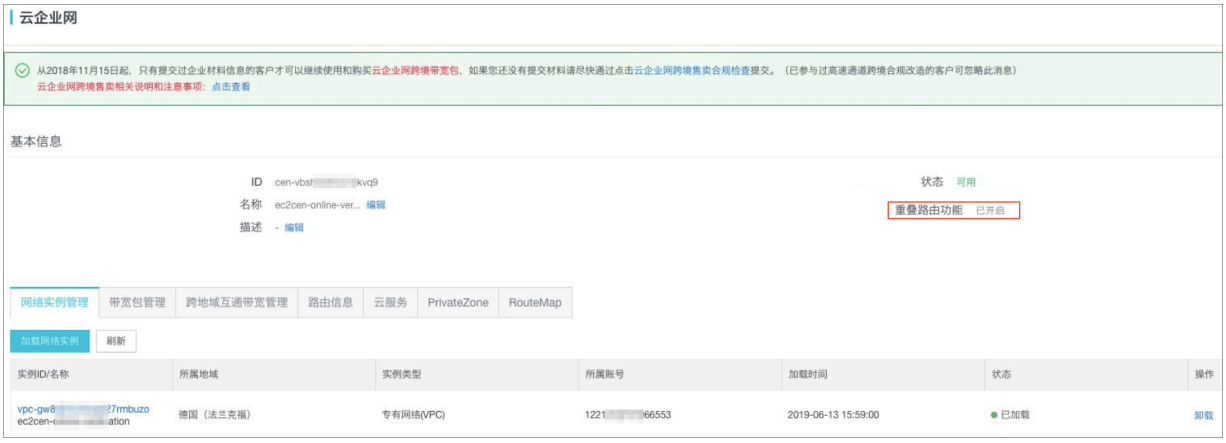
在将VPC平滑迁移至CEN后，请不要冻结或删除华东1（杭州）和华东2（上海）这两个地域内建立的同地域对等连接。

准备工作

如果您要使用已有的CEN实例，确保网络重叠功能已开启。

说明:

如果存在未开启网络重叠功能的老实例，请开启网络重叠功能。



迁移操作

参考以下步骤，将已使用对等连接的VPC迁移至云企业网：

说明:

在迁移前，确保您已经完成所需的准备工作。

1. 登录云企业网控制台。
2. 在云企业网实例页面，单击CEN实例ID链接。

3. 在网络实例管理页面，单击加载网络实例加载要迁移的VPC实例。详细说明，请参见网络实例。

4. 如果需要跨地域互通，请在CEN实例中购买带宽包并配置私网互通带宽。

   详细说明，请参见设置跨地域互通带宽。

5. 如果VPC中存在指向ECS实例、VPN网关、HAVIP等路由条目，请根据连通性需求，在VPC控制台将这些路由发布到CEN中。

6. 登录CEN控制台，在路由信息页面查看路由配置。确保加载VPC后，不存在冲突路由。

   高速通道对等连接配置的静态路由优先于CEN的动态路由。即如果存在高速通道静态路由，不允许任何比该静态路由更明细或与该静态路由相同的CEN路由学习进来。此时建议您将高速通道路由进行拆分，在CEN完成路由学习后再删除拆分的路由，保证平稳迁移。

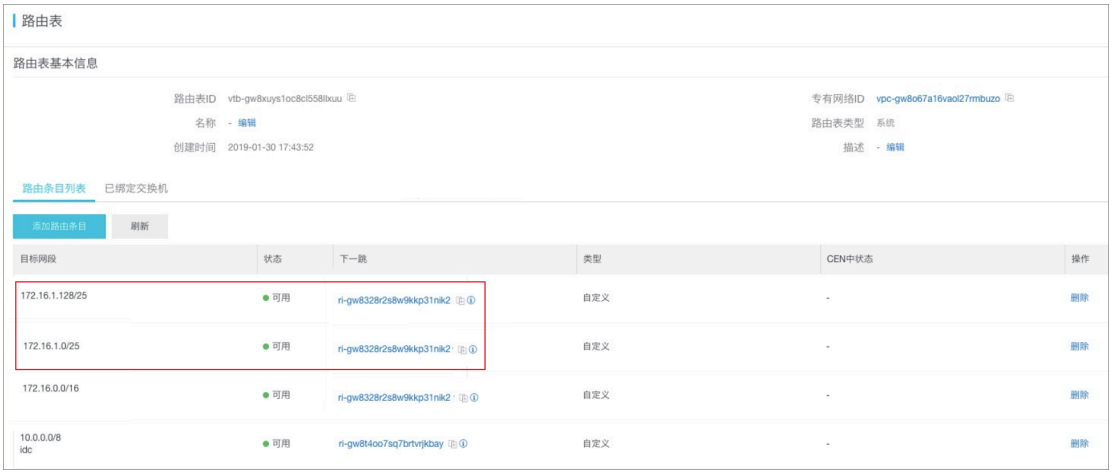
   以下图中的CEN路由172.16.1.0/24为例，该路由比指向高速通道的路由172.16.0.0/16更明细，所以出现了路由冲突。

   - 如果采用闪断迁移，可以（在VPC控制台上）直接删除高速通道路由172.16.0.0/16，CEN路由自动生效，完成该路由的迁移。

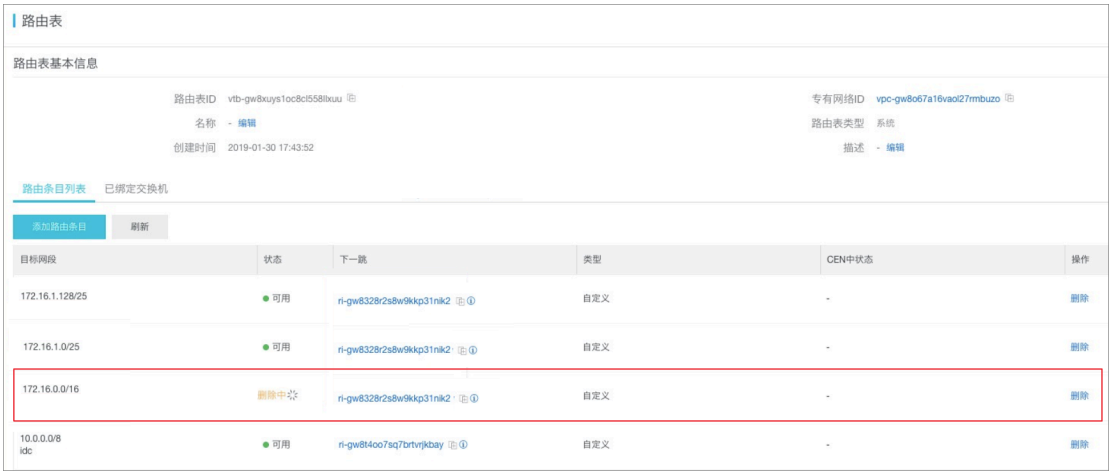
     闪段时长和CEN路由条目数量成正比，对于重要的业务建议您使用平滑迁移方式。
   - 如果采用平滑迁移，需要按照比CEN路由172.16.1.0/24更明细的目标拆分，可以将路由172.16.0.0/16拆分为172.16.1.0/25和172.16.1.128/25两条明细路由。

     a. 在VPC控制台，找到要拆分的路由条目所在的路由表。

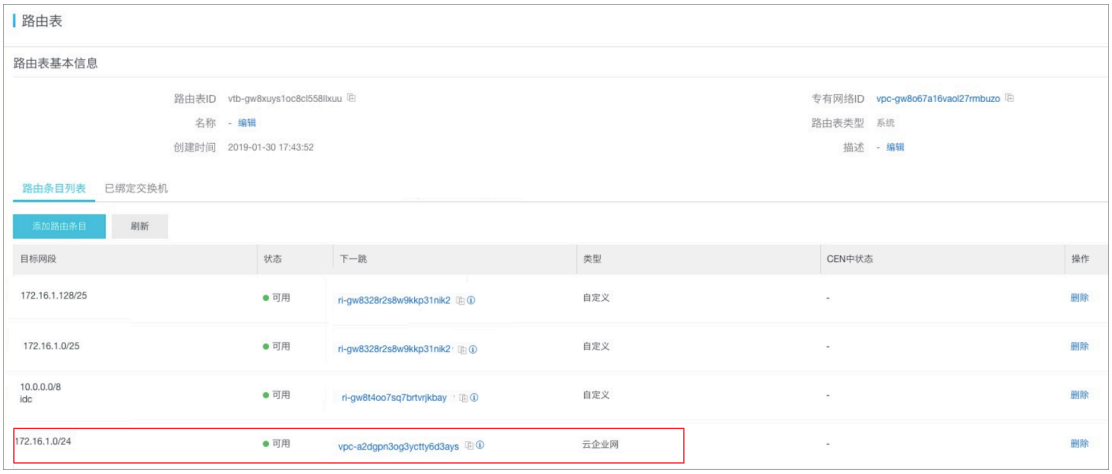
     b. 单击添加路由条目分别添加两条目标网段为172.16.1.0/25和172.16.1.128/25，下一跳为高速通道路由器接口的路由条目。



     c. 添加成功后，在VPC路由表中单击删除删除高速通道路由172.16.0.0/16。



d. 单击刷新查看CEN路由是否生效。



e. CEN路由生效后，在VPC路由表中删除172.16.1.0/25和172.16.1.128/25两条明细路由，完成该条路由的平滑迁移。

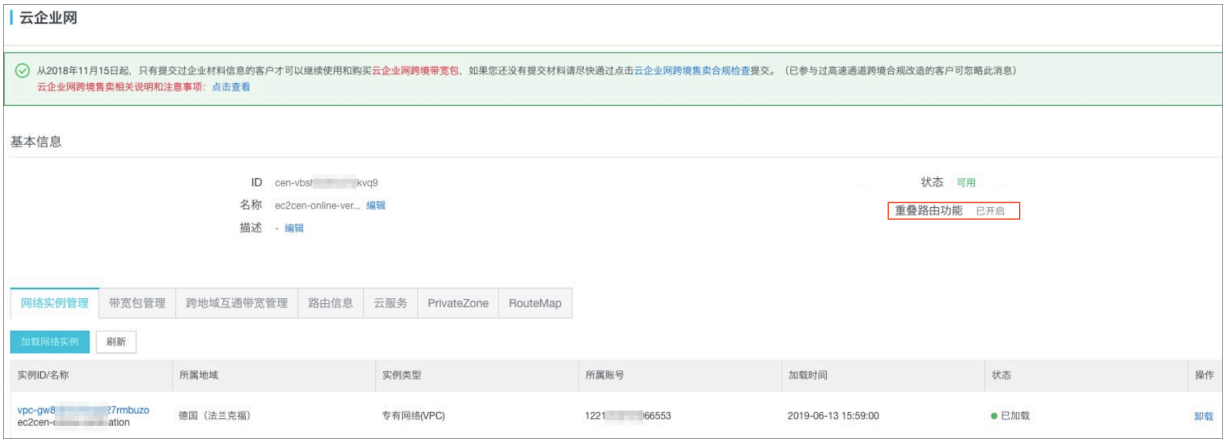
5.2 已使用对等连接的VBR迁移至云企业网

您可以将已使用高速通道对等连接的边界路由器（VBR）平滑迁移至云企业网。云企业网（Cloud Enterprise Network, CEN）可以在不同专有网络之间，专有网络与本地数据中心间搭建私网通信通道。通过自动路由分发及学习，CEN可以提高网络的快速收敛和跨网络通信的质量和安全性，实现全网资源的互通。

准备工作

如果您要使用已有的CEN实例，确保网络重叠功能已开启。

> **说明:**
> 如果存在未开启网络重叠功能的老实例，请开启网络重叠功能。



迁移操作

参考以下步骤，将已使用对等连接的VBR迁移至云企业网：

说明：

在迁移前，确保您已经完成所需的准备工作。

1. **如果VBR配置了健康检查，建议您先在高速通道控制台删除健康检查配置。**
2. **登录云企业网控制台。**
3. **在云企业网实例页面，单击CEN实例ID链接。**
4. **在网络实例管理页面，单击加载网络实例加载要迁移的VBR和VPC实例。详细说明，请参见网络实例。**

5. 如果需要跨地域互通，请在CEN实例中购买带宽包并配置私网互通带宽。

   详细说明，请参见设置跨地域互通带宽。

6. 如果VPC中存在指向ECS实例、VPN网关、HAVIP等路由条目，请根据连通性需求，在VPC控制台将这些路由发布到CEN中。

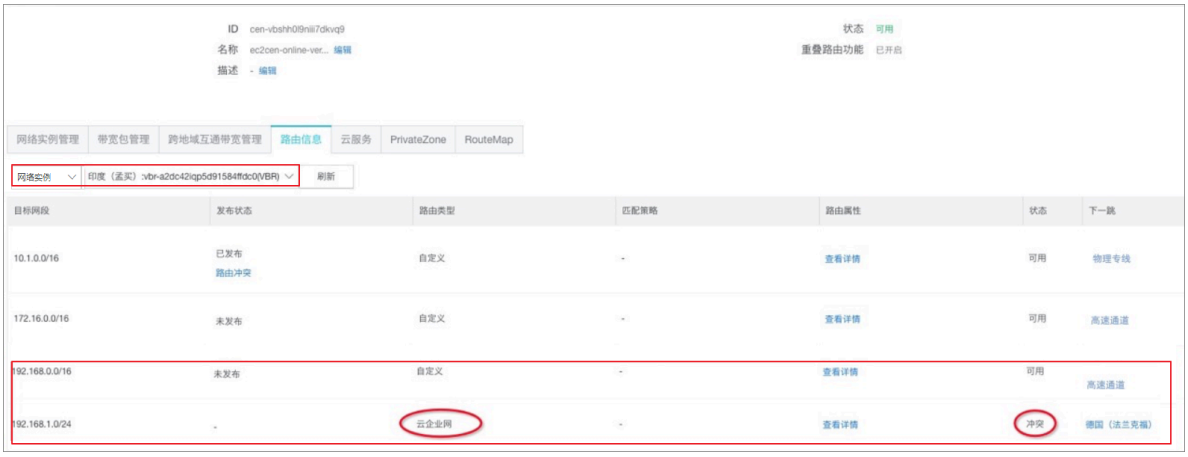
7. 如果本地IDC需要访问云服务例如OSS和PrivateZone等，请在云企业网控制台进行配置。

   配置说明，请参见设置PrivateZone访问。

8. 登录CEN控制台，在路由信息页面查看路由配置。确保加载VBR和VPC后，不存在冲突路由。

   高速通道对等连接配置的静态路由优先于CEN的动态路由。即如果存在高速通道静态路由，不允许任何比该静态路由更明细或与该静态路由相同的CEN路由学习进来。此时建议您将高速通道路由进行拆分，在CEN完成路由学习后再删除拆分的路由，保证平稳迁移。

   以下图中的CEN路由192.168.1.0/24为例，该路由比指向高速通道的路由192.168.0.0/16更明细，所以出现了路由冲突。



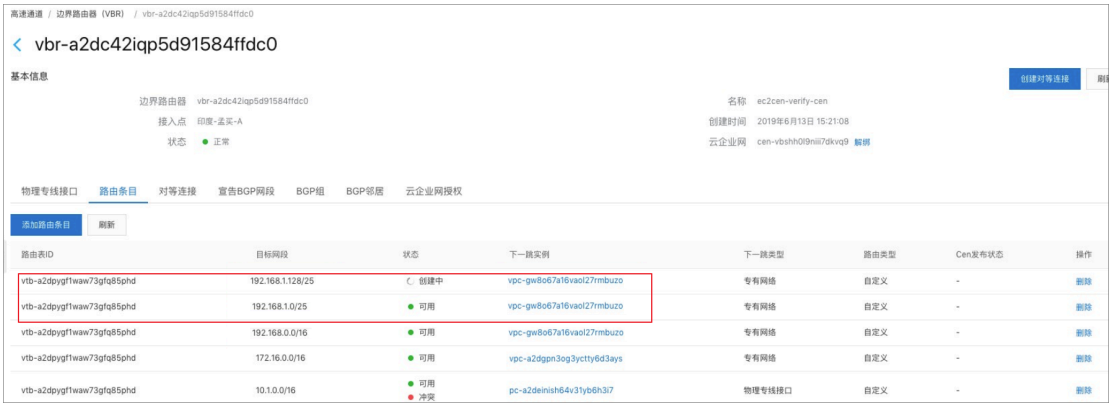
- 如果采用闪断迁移可以直接删除高速通道路由192.168.0.0/16，CEN路由自动生效。

  闪段时长和CEN路由条目数量成正比，对于重要的业务建议您使用平滑迁移方式。

- 如果采用平滑迁移，需要按照比CEN路由192.168.1.0/24更明细的目标拆分，可以将高速通道路由192.168.0.0/16拆分为192.168.1.0/25和192.168.1.128/25两条明细路由。

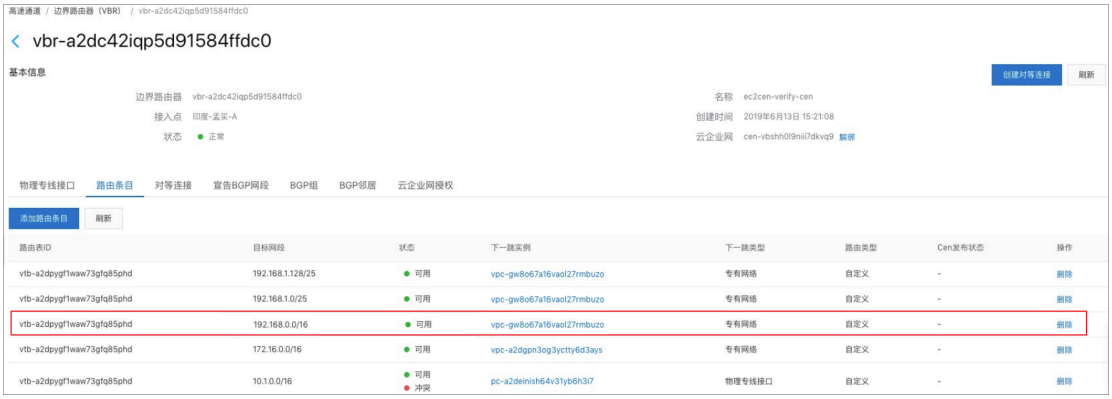
  a. 在高速通道控制台VBR详情页面，单击路由条目进入VBR路由表页面。

  b. 单击添加路由条目分别添加两条目标网段为192.168.1.0/25和192.168.1.128/25，下一跳为专有网络的路由条目。

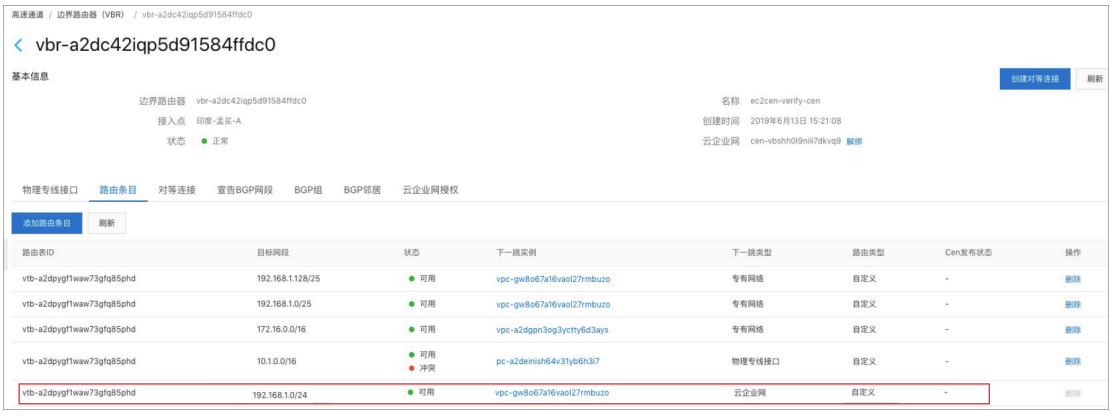


  c. 如果是BGP路由，需要添加192.168.1.0/25和192.168.1.128/25相关的网段宣告。

d. 删除高速通道路由192.168.0.0/16。



e. 单击刷新查看CEN路由是否生效。



f. 在VBR路由表中删除192.168.1.0/25和192.168.1.128/25两条明细路由，并删除宣告BGP路由。

g. 在CEN控制台，为已迁移的VBR配置健康检查。配置详情，请参见配置健康检查。

5.3 迁移回滚

您可以通过修改路由回滚迁移。

迁移方式不同，回滚方案也不同：

- 闪断迁移：重新添加已删除的高速通道静态路由，比该高速通道静态路由更明细或相等的CEN路由全部被删除。

- 平滑迁移：直接添加删除的明细路由进行回滚即可。

说明:

如果迁移的VBR配置了BGP路由，VBR的路由宣告也需要同时回滚。

6 实现对等连接冗余网络架构

为了保证单条物理专线出现故障时，可以顺利切换至冗余专线，您需要为每个VBR上连的对等连接配置健康检查和路由权重。

前提条件

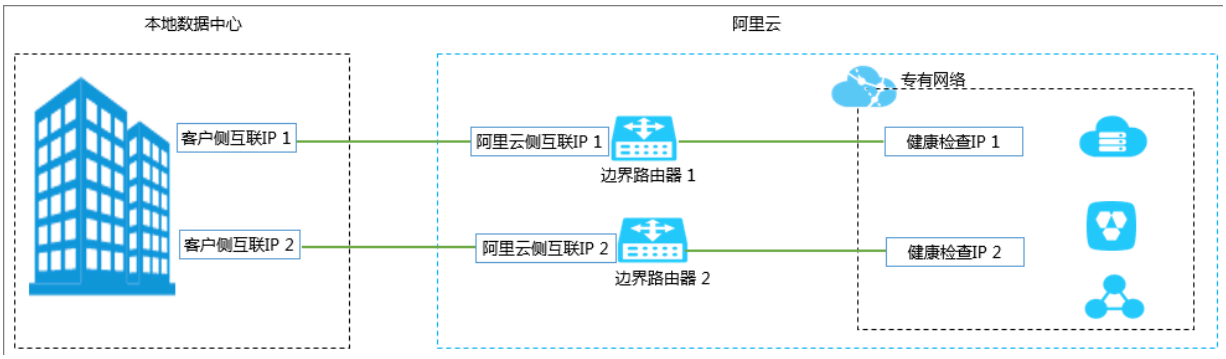
配置健康检查和路由权重前，您需要确保以下操作已完成：

- 确保您已经申请了两个物理专线接口，并且阿里云和本地IDC的物理专线网络已经连通。
- 确保您已经创建了两个从边界路由器到云上VPC的对等连接，详情请参见自主申请专线接口和VBR上联。
- 边界路由器和本地IDC之间配置的是静态路由配置，未使用BGP。

背景信息

阿里云每两秒从健康检查IP地址向本地数据中心中的客户侧互联IP发送一个ping报文，如果某条物理专线上连续8个ping报文都无法得到回复，则将流量切换至另一条链路。

> 说明：
> 如果本地数据中心网络设备配置了Copp策略（如思科设备） 或者本机防攻击策略（如华为设备）可能会导致健康探测报文被丢弃，造成健康检查链路震荡，建议本地数据中心网络设备取消控制面限速配置。



网路拓扑信息如下：

参数	地址段
互连的VPC	192.168.0.0/16
本地IDC	172.16.0.0/16
第一个VBR和IDC的互联地址	· VBR网关IP：10.10.10.1 · 本地IDC网关IP：10.10.10.2 · 掩码：255.255.255.252

参数	地址段
第二个VBR和IDC的互联地址	· VBR网关IP：10.10.11.1 · 本地IDC网关IP：10.10.11.2 · 掩码：255.255.255.252
第一个对等连接健康检查	· 源IP：192.168.10.1 · 目的IP：10.10.10.2
第二个对等连接健康检查	· 源IP：192.168.10.2 · 目的IP：10.10.11.2

步骤一 配置健康检查

您需要给两个对等连接分别配置健康检查。

1. 登录高速通道管理控制台。
2. 在左侧导航栏，选择专有网络对等连接 > VBR上连。
3. 单击已创建的目标对等连接操作列的 > 健康检查。

4. 在健康检查页面，单击设置。
5. 在修改边界路由器页面，配置健康检查信息。

   具体参数说明如下：

参数	说明
源IP	互通的VPC内未被使用的任意一个私网IP地址。

参数	说明
目标IP	本地IDC网络设备的接口IP地址。 如果需要从IDC向VPC做ICMP健康检查，建议将目标地址设置为VPC健康检查源地址，并配置指向新的健康检查目的地址的路由。

6. 单击确定。
7. 重复上述步骤，完成另一个对等连接的健康检查配置。

说明:

第二个对等连接的健康检查源IP不能跟第一个重复。

步骤二 配置路由权重

本次操作以配置负载路由为例。

1. 在左侧导航栏，单击路由表。
2. 单击需要配置负载路由和权重的VPC实例ID，然后单击目标路由表ID。

3. 在路由表页面，单击添加路由条目，配置负载路由。

   根据以下信息配置负载路由：

   - 目标网段：要转发到的目标网段。
   - 下一跳类型：此处选择路由器接口（边界路由器方向），表示将目的地址在目标网段范围内的流量路由至边界路由器关联的路由器接口。

     路由方式选择负载路由，选择VPC对接的两个边界路由器作为下一跳。实例权重的有效范围为1-255的整数，默认值为100。每个实例的权重必须相同，系统会将流量平均分配给下一跳实例。

4. 继续单击添加路由条目，配置第一个边界路由器到本地IDC的互联地址网段的路由。

   根据以下信息配置负载路由：

   - 目标网段：要转发到的目标网段。
   - 下一跳类型：此处选择路由器接口（边界路由器方向），表示将目的地址在目标网段范围内的流量路由至边界路由器关联的路由器接口。

     路由方式选择普通路由，选择第一个边界路由器接口。

5. 继续单击添加路由条目，配置第二个边界路由器到本地IDC的互联地址网段的路由。

   根据以下信息配置负载路由：

   - 目标网段：要转发到的目标网段。
   - 下一跳类型：此处选择路由器接口（边界路由器方向），表示将目的地址在目标网段范围内的流量路由至边界路由器关联的路由器接口。

     路由方式选择普通路由，选择第二个边界路由器接口。

   路由配置完成后如下图所示。

步骤三 本地机房CPE设备配置云上健康检查源IP的静态路由

边界路由器和本地IDC之间配置的是静态路由配置，未使用BGP时，本地机房CPE设备需要配置以下静态路由：

- 本地机房CPE设备，配置到第一个对等连接健康检查源IP的下一跳为云上第一个边界路由器的IP地址（新建VBR配置的云上互联IP地址）。
- 本地机房CPE设备，配置到第二个对等连接健康检查源IP的下一跳为云上第二个边界路由器的IP地址。

步骤四 测试网络连通性

当一条物理专线出现故障时，尝试ping云上VPC中的实例，确认是否能够通过冗余专线访问云上资源。

补充说明

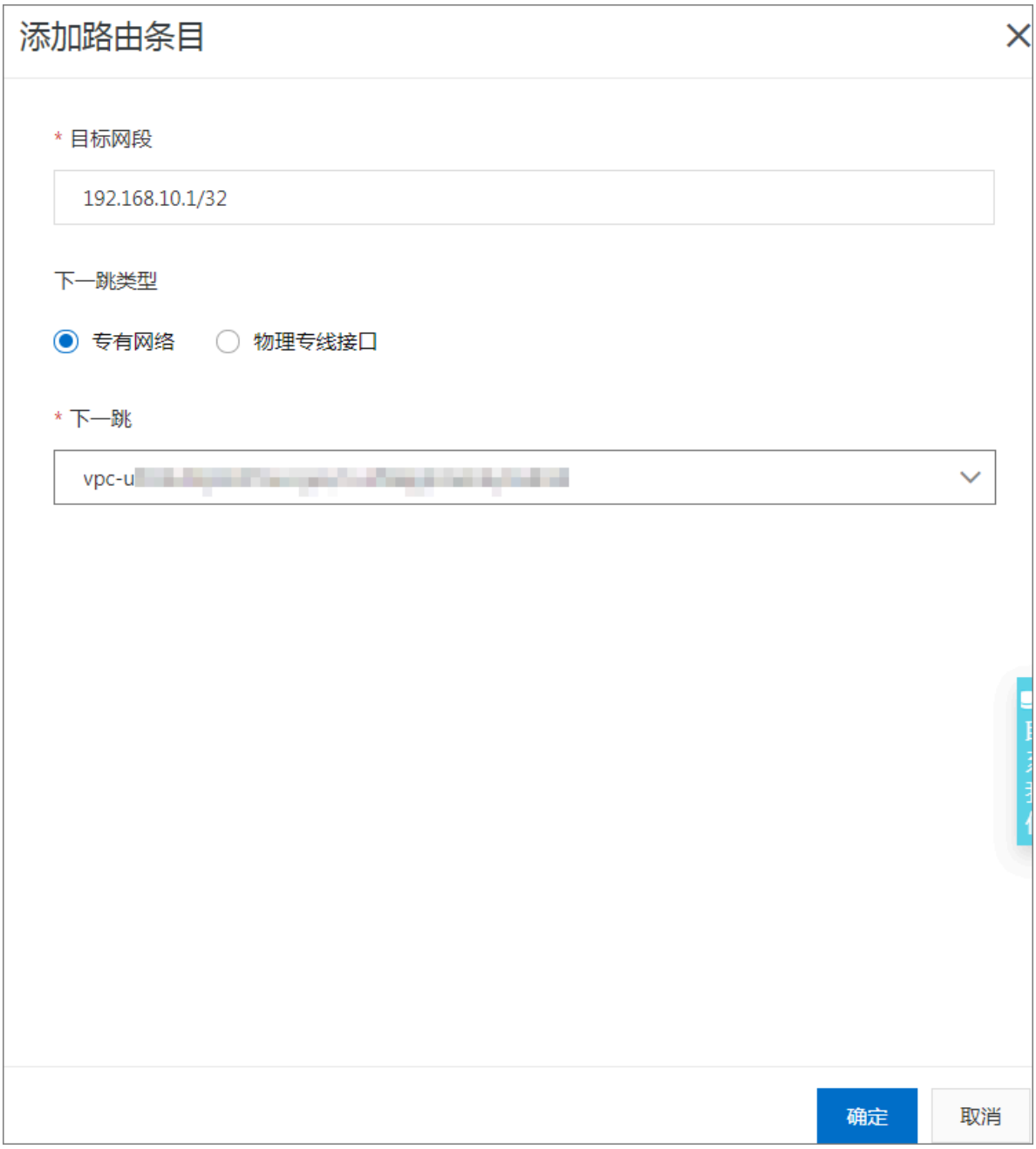
若您的边界路由器和本地机房CPE配置了BGP，边界路由器对健康检查地址需要进行BGP网段的宣告。

1. 登录高速通道管理控制台。
2. 在左侧导航栏，选择物理专线连接 > 边界路由器（VBR）。
3. 单击第一个VBR实例ID，在路由条目页签下，单击添加路由条目。

4. 在添加路由条目页面，配置健康检查源地址路由信息。

   相关参数说明如下：

   - 目标网段：健康检查源IP，本次配置为192.168.10.1/32。
   - 下一跳类型：此处选择专有网络，选择对接的VPC实例。



5. 在宣告BGP网段页签下，单击宣告BGP网段。

6. 在宣告BGP网段页面，配置健康检查的源IP。

7. 重复上述步骤，给第二个边界路由器的健康检查地址需要进行BGP网段的宣告。