阿里云
云企业网

最佳实践

文档版本：20181129

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。
斜体	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

法律声明.....I
通用约定.....I
1 IDC通过BGP主备链路上云方案.....1
2 IDC双专线静态路由冗余上云方案.....5
3 IDC通过VPN网关上云方案.....9
4 IDC通过专线和智能接入网关主备方式上云方案.....16

1 IDC通过BGP主备链路上云方案

本教程介绍通过专线接入和云企业网组合的方式，实现客户IDC通过主备链路上云，并和云上不同地域VPC互通的场景。

方案概述

完成以下操作，配置主备选路（主链路优先）接入阿里云：

1. 搭建冗余物理专线

   创建冗余物理专线，将本地IDC接入阿里云。本地IDC和边界路由器之间配置BGP路由。详情参见*#unique_4*。

2. 配置健康检查

   设置健康检查，是保障等价冗余专线链路中一条链路中断后，流量可以切换到另外一条链路的前提。详情参见健康检查。

3. 加载网络实例将需要互通的VBR和VPC加载到已创建的云企业网实例中。详情参见*#unique_6/unique_6_Connect_42_section_s4y_4mh_tdb*。

4. 配置路由

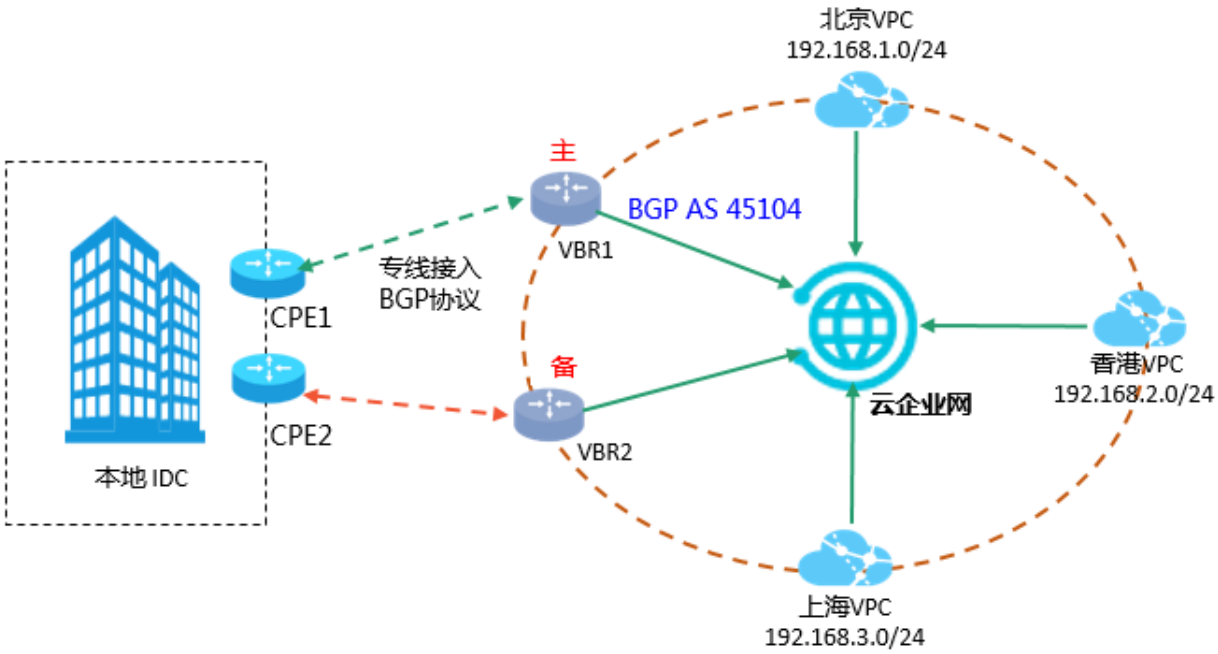
   您可以通过设置AS-Path的长度来确定路由选路的优先级。详情参见*IDC*侧宣告*BGP*路由并设置权重。

网络拓扑

本方案中使用的网络拓扑如下：

- 本地IDC已通过专线双冗余方式连接到阿里云的不同边界路由器（VBR）。IDC和VBR之间采用BGP路由协议。
- 分别在北京、香港和上海地域部署了VPC。
- 本方案中各网络的网段如下表所示。

网络	网段
本地IDC	10.1.1.0/24
北京VPC	192.168.1.0/24
上海VPC	192.168.2.0/24
香港VPC	192.168.3.0/24

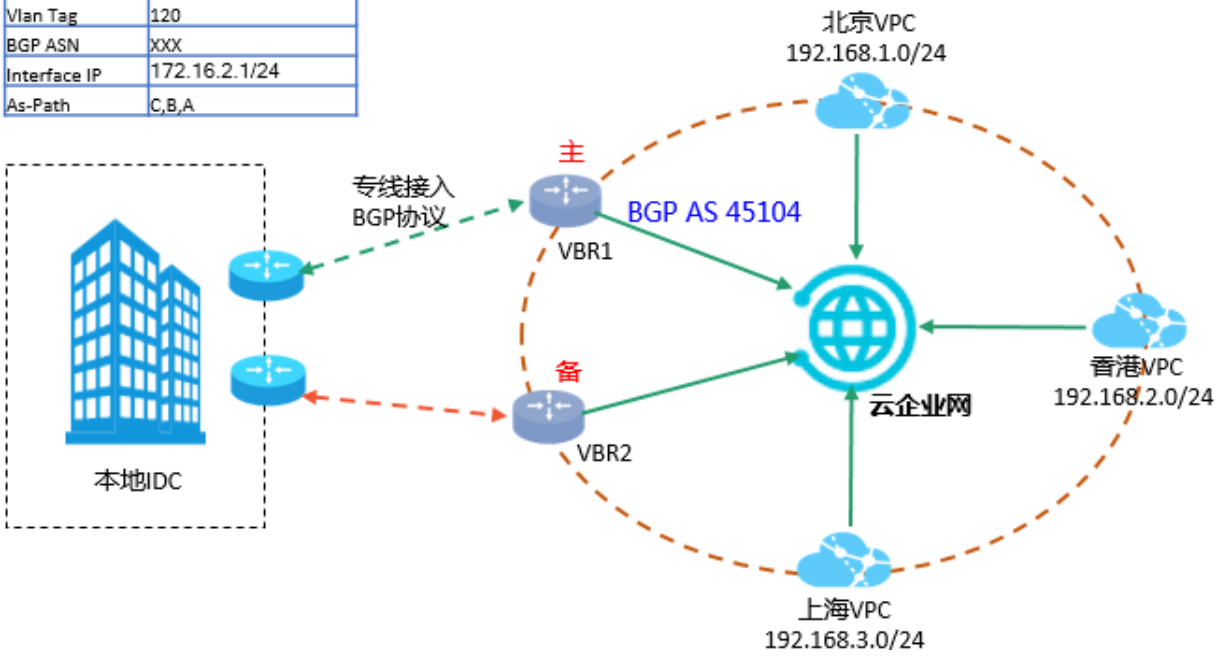


IDC侧宣告BGP路由并设置权重

假设IDC和边界路由器之间分别已经建立起BGP邻居关系（详情参见*创建BGP邻居*）。

现在需要在IDC侧配置向阿里云宣告的BGP路由（10.1.1.0/24），并通过设置AS-Path来确定选路权重，实现阿里云到IDC路由的主备模式。

CPE1	
Vlan Tag	110
BGP ASN	XXX
Interface IP	172.16.1.1/24
As-Path	B,A
CPE2	
Vlan Tag	120
BGP ASN	XXX
Interface IP	172.16.2.1/24
As-Path	C,B,A



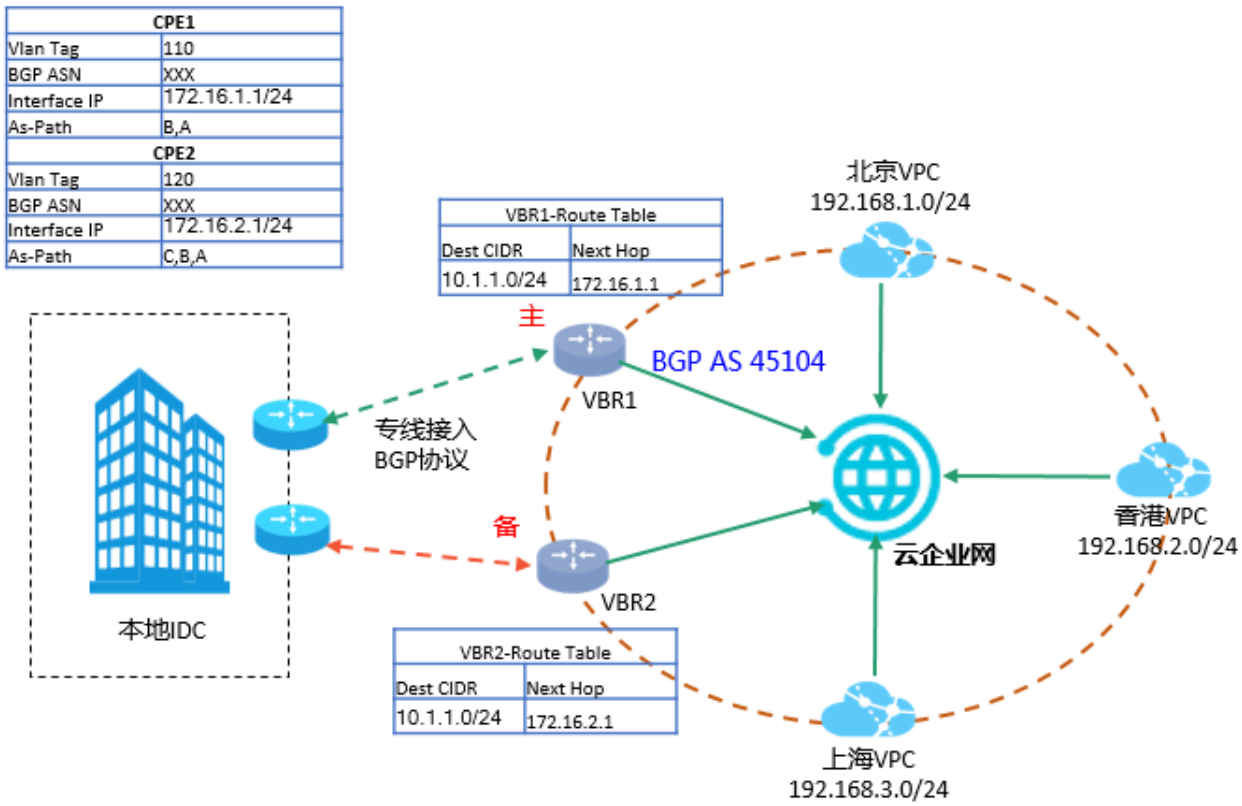
如上图所示绿色链路（CPE1）为主链路，红色链路（CPE2）为备份链路，则IDC侧分别在两个CPE的BGP配置如下表所示。

您可以通过设置AS-Path的长度来确定路由选路的优先级。As-Path长度越短，优先级越高。

配置	CPE1	CPE2
Vlan Tag	110	120
Network	10.1.1.0/24	10.1.1.0/24
BGP ASN	XXX	XXX
Interface IP	172.16.1.1/24	172.16.2.1/24
As-Path	B,A	C,B,A

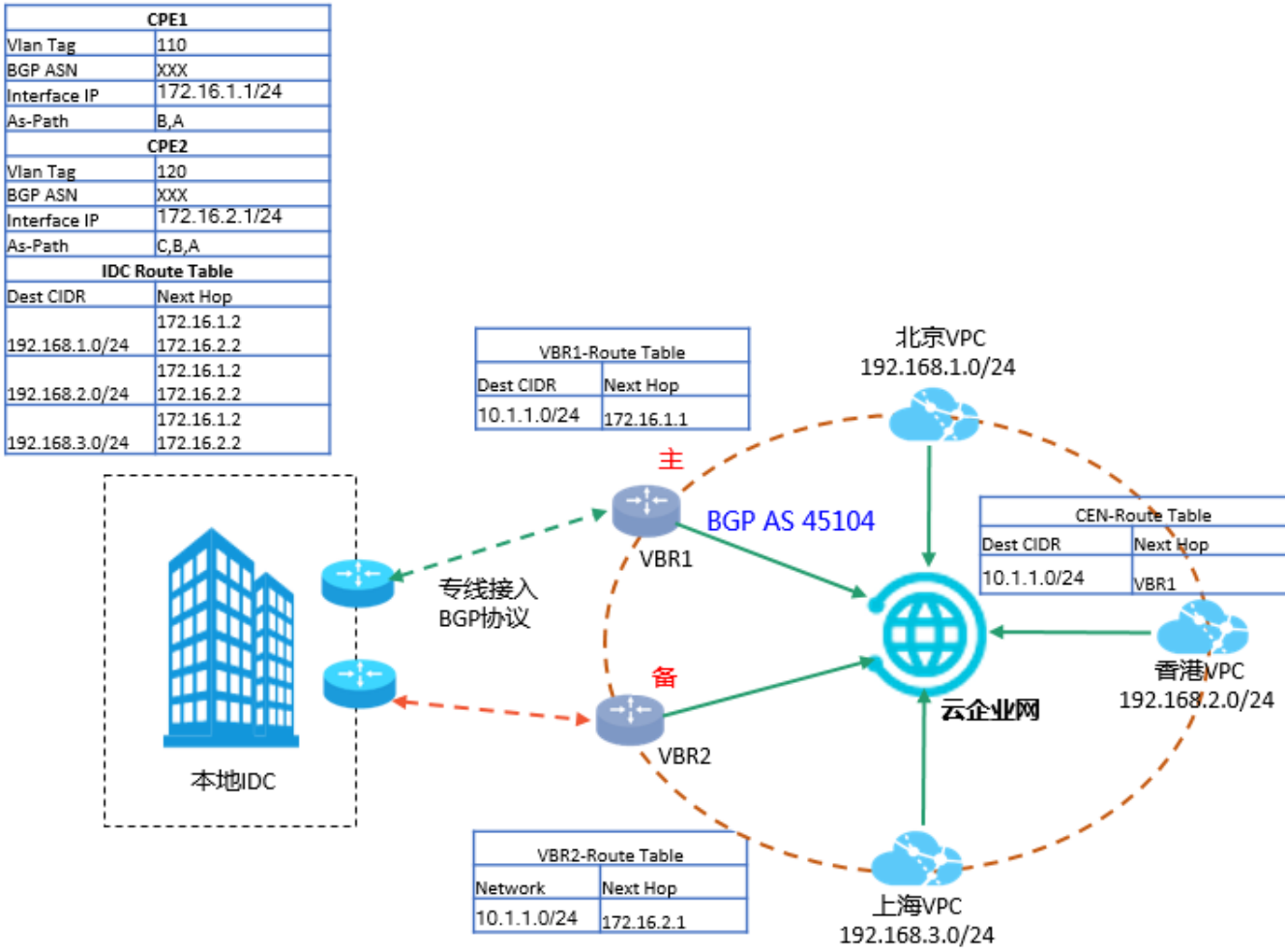
云企业网具备自动学习分发路由的能力，在配置好路由后，云企业网会基于选路权重等信息，将路由同步到云企业网内部。

- 边界路由器BGP路由



如下图所示，在VBR1和VBR2可以看到从对端邻居学到的路由信息和下一跳。由于VBR已经加载到云企业网中，所以VBR会将从IDC侧学来的BGP路由信息发送到云企业网，包括AS-Path。

- 全量路由配置



由于VBR和VPC均已加载到云企业网中，那么从VBR上学来的BGP路由也会发布到云企业网中，云企业网会基于选路权重等信息，将路由同步到云企业网内部。

两个VBR从IDC侧学习到的BGP路由目标网段一致，但是路由权重不同，VBR1作为主选路（AS-Path短），VBR2是备选（AS-Path长），那么云企业网会将该路由的属性通知到云企业网中的其他网络实例比如VPC。从VPC的路由表中就可以看到去往10.1.1.0/24的路由均指向VBR1。

云企业网也会将云企业网内系统路由重发布到BGP中，所以在IDC的BGP路由表中就可以看到学习到的云企业网中的路由信息，并且下一跳分别指向与IDC建立邻居的两个VBR的接口IP。

同理，如果想从IDC侧设置到阿里云业务地址（192.168.X.0/24）的主备链路，同样可以通过BGP选路属性，在IDC侧分别设置从不同邻居（VBR1，VBR2）学习到的路由192.168.X.0/24的权重，便可实现从IDC到阿里云的主备选路。

2 IDC双专线静态路由冗余上云方案

本教程介绍通过专线接入和云企业网组合的方式，实现客户IDC冗余专线上云，并和云上不同地域VPC互通的场景。

方案概述

完成以下操作，将本地IDC接入阿里云：

1. 搭建冗余物理专线

   创建冗余物理专线，将本地IDC接入阿里云。本地IDC和边界路由器之间配置静态路由。详情参见*#unique_4*。

2. 配置健康检查（必须配置）

   设置健康检查，是保障等价冗余专线链路中一条链路中断后，流量可以切换到另外一条链路的前提。在配置健康检查时，您可以将CEN中加载的VPC中任何一个未被使用的私网IP配置为源IP，将和VBR互联的CPE接口IP配置为目标IP。详情参见健康检查。

3. 加载网络实例

   将需要互通的VBR和VPC加载到已创建的云企业网实例中。详情参见*#unique_6/unique_6_Connect_42_section_s4y_4mh_tdb*。

4. 配置和发布路由

   在本地IDC和VPC中分别配置路由，详情参见*IDC*和*VBR*静态路由配置。

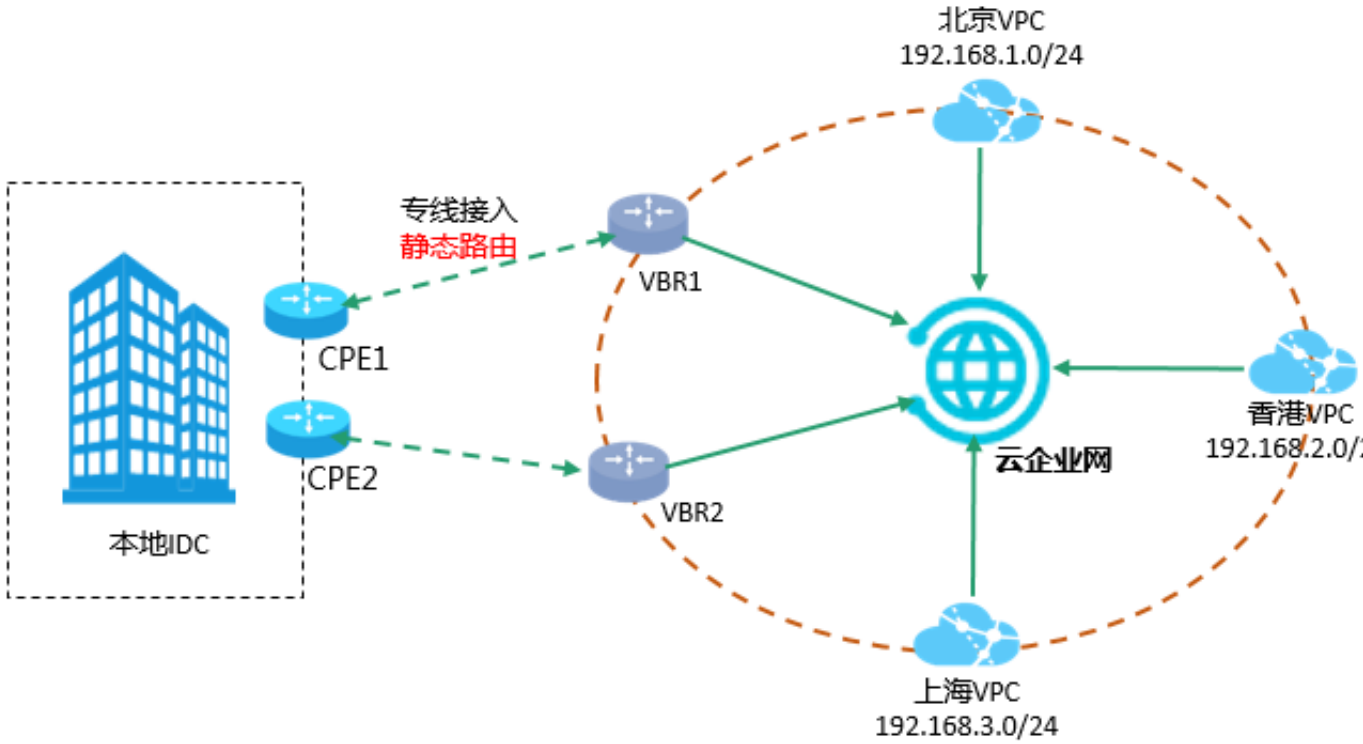
网络拓扑

本方案中使用的网络拓扑如下：

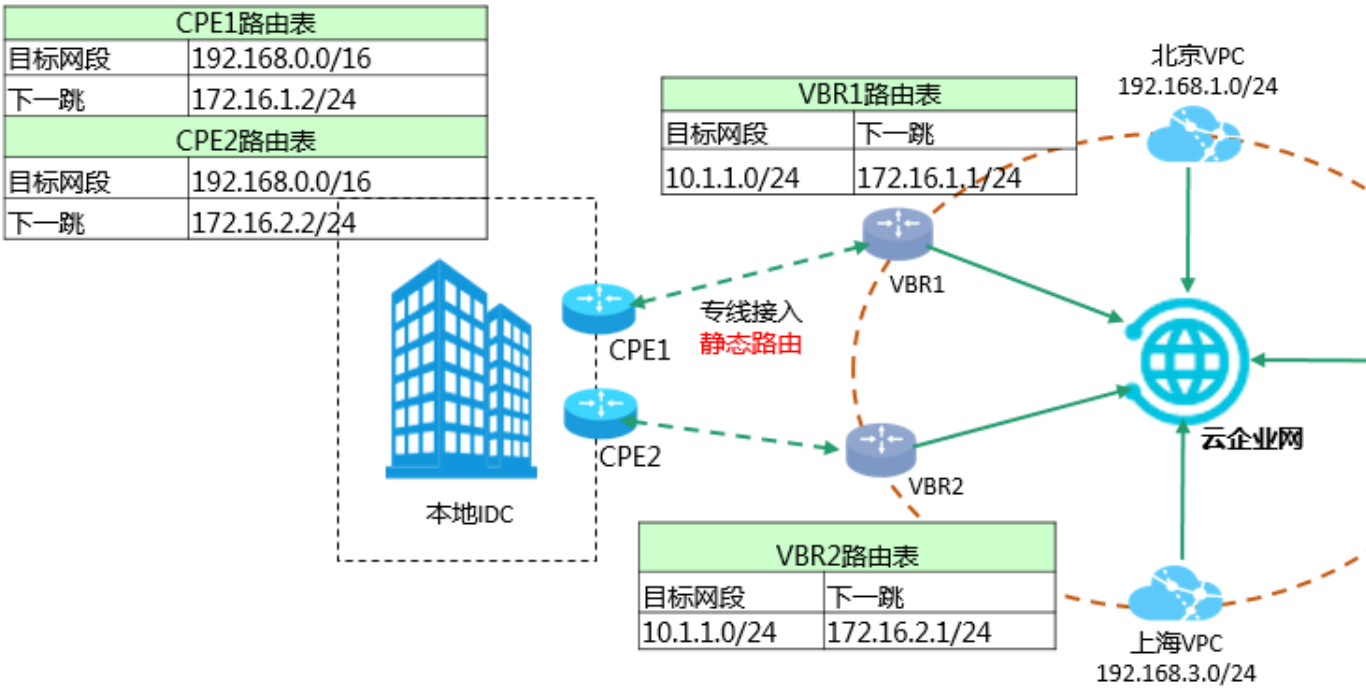
- 本地IDC已通过专线双冗余方式连接到阿里云的不同边界路由器（VBR）。IDC和VBR之间配置静态路由。
- 分别在北京、香港和上海地域部署了VPC。
- 本方案中各网络的网段如下表所示。

网络	网段
本地IDC	10.1.1.0/24
北京VPC	192.168.1.0/24
上海VPC	192.168.2.0/24

网络	网段
香港VPC	192.168.3.0/24



IDC和VBR静态路由配置



本方案中的路由配置如下：

- IDC路由配置

  分别在CPE1和CPE2上配置指向阿里云的静态路由，实现IDC到云上的路由。

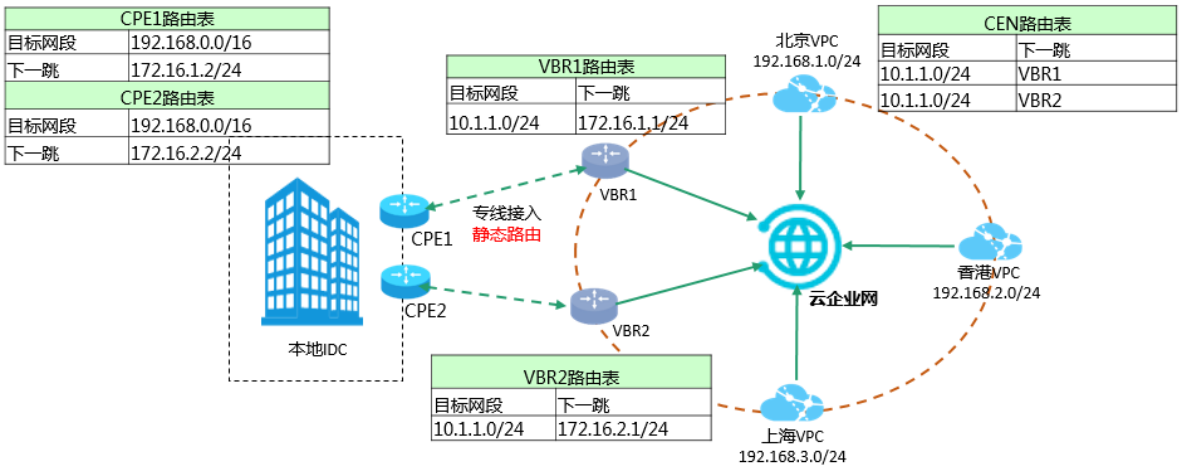
配置	CPE1	CPE2
目标网段	192.168.0.0/16	192.168.0.0/16
下一跳	172.16.1.2/24 (VBR1)	172.16.2.2/24 (VBR2)

- VBR路由配置

  分别在VBR1和VBR2上配置指向本地IDC的静态路由，实现云上到IDC的路由。

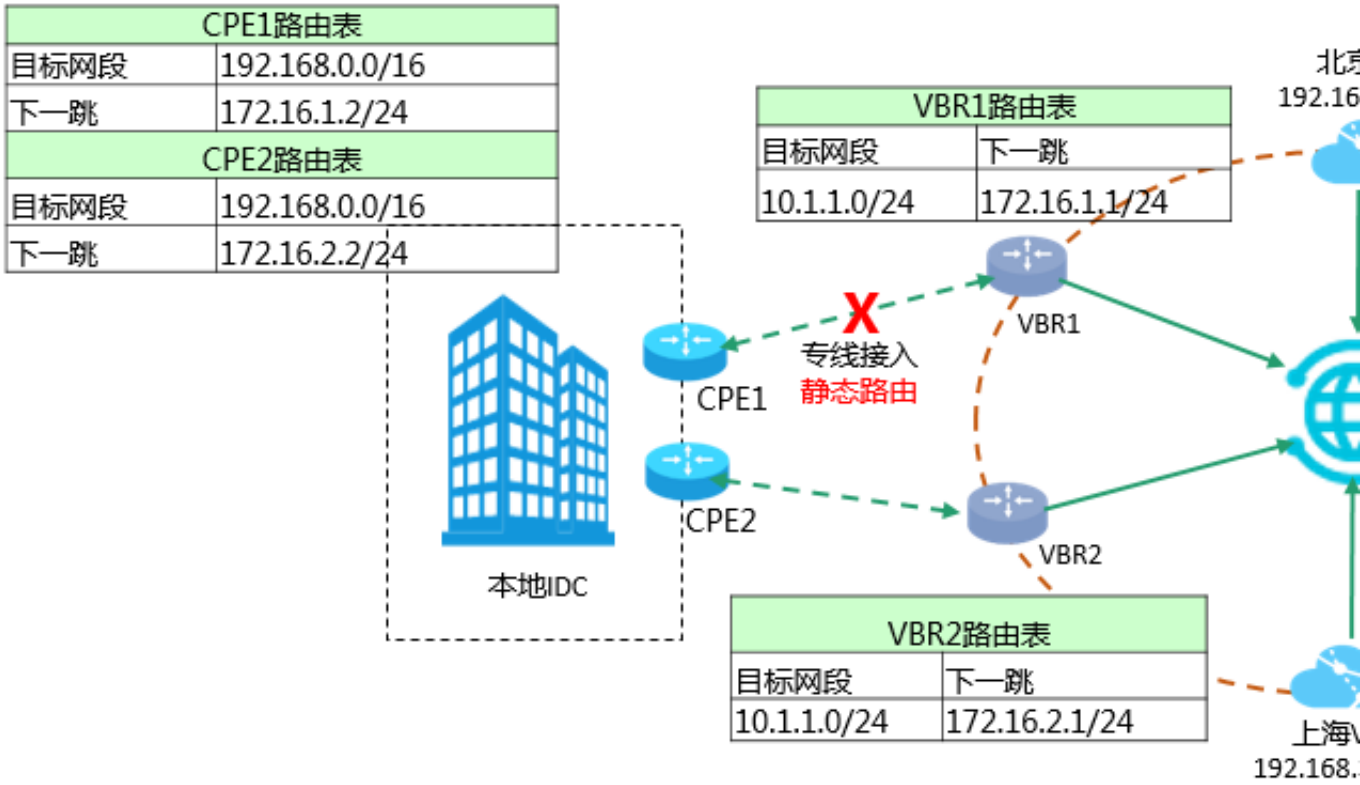
配置	VBR1	VBR2
目标网段	10.1.1.0/24	10.1.1.0/24
下一跳	172.16.1.1/24	172.16.2.1/24

- 云企业网路由



通过在VBR上进行以上路由配置，云企业网会分别将VBR1和VBR2上配置的静态路由同步到云企业网内部。从云企业网内部看，两条专线已形成等价路由（ECMP），并且处于双活状态。

冗余容灾



当某条专线断掉后（如VBR1到CPE1），云企业网会对路由进行切换，云上所有到IDC的数据会走VBR2，从而实现了链路的切换和容灾效果。

3 IDC通过VPN网关上云方案

本教程介绍通过VPN网关和云企业网组合的方式，实现客户IDC上云，并和云上不同地域VPC互通的场景。

方案概述

完成以下操作，将本地IDC接入阿里云：

1. 配置VPN网关

   创建IPSec-VPN连接，将本地IDC接入阿里云。详情参见配置站点到站点连接。

2. 加载网络实例

   将需要互通的VBR和VPC加载到已创建的云企业网实例中。详情参见*#unique_6/unique_6_Connect_42_section_s4y_4mh_tdb*。

3. 配置和发布路由

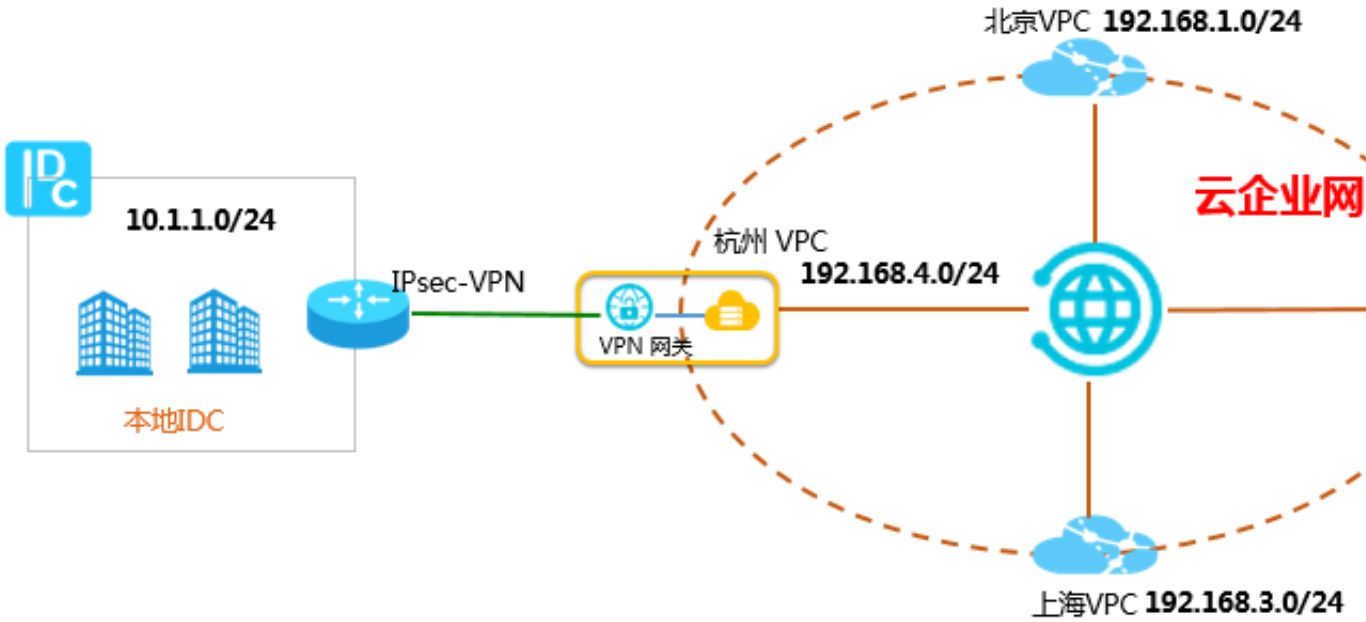
   您可以将VPC中指向VPN网关的路由发布到CEN中，CEN中其他加载的网络实例便可以学习到该条路由。

网络拓扑

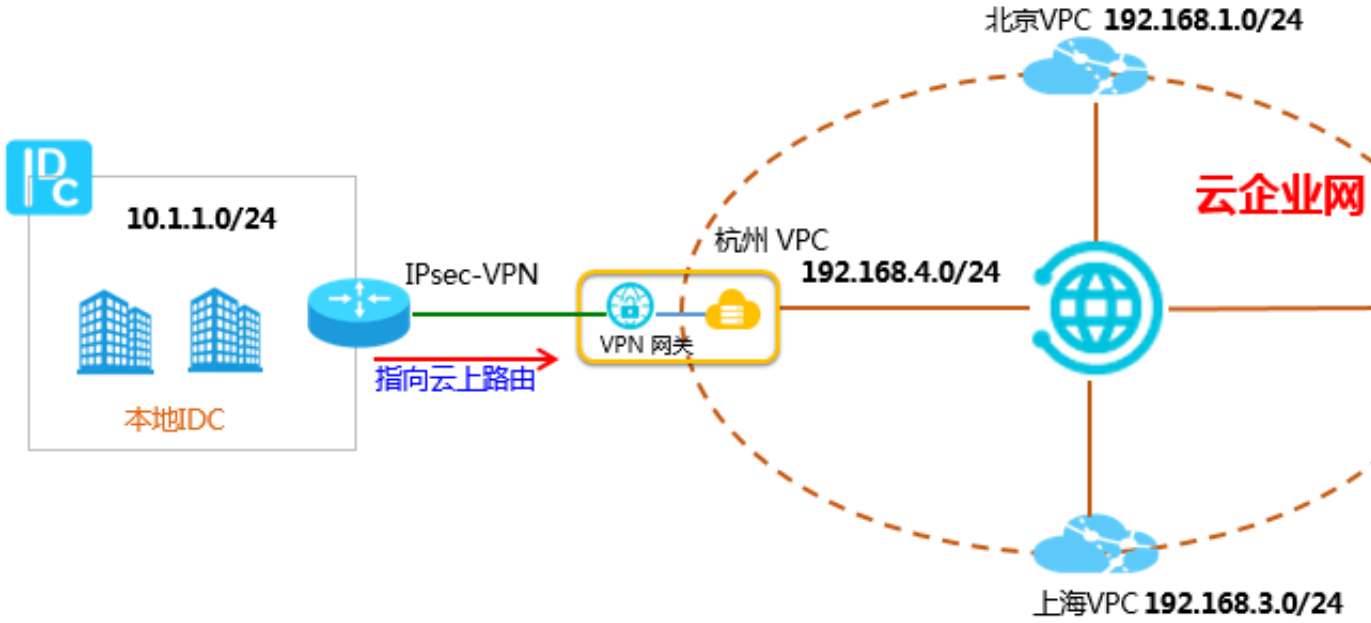
本方案中使用的网络拓扑如下：

- 本地IDC已通过VPN网关连接到阿里云。
- 分别在杭州、北京、香港和上海地域部署了VPC。
- 本方案中各网络的网段如下表所示，确保各VPC的地址段不冲突。

网络	网段
本地IDC	10.1.1.0/24
北京VPC	192.168.1.0/24
上海VPC	192.168.2.0/24
香港VPC	192.168.3.0/24
杭州VPC	192.168.4.0/24



IDC路由配置



本地IDC已与阿里云VPN网关之间建立起IPsec-VPN连接，并且已配置指向云上的明细路由或默认路由：

表 3-1: IDC明细路由配置

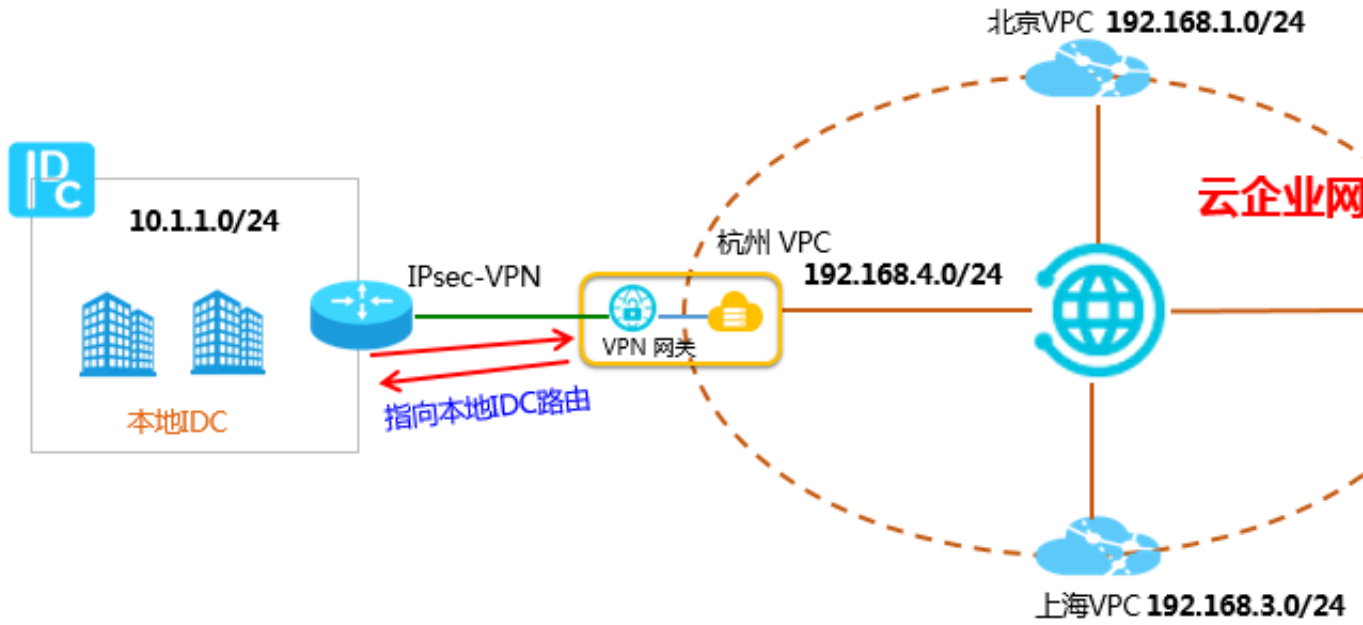
目标网段	下一跳
192.168.1.0/24	VPN网关
192.168.2.0/24	VPN网关

目标网段	下一跳
192.168.3.0/24	VPN网关
192.168.4.0/24	VPN网关

表 **3-2: IDC默认路由配置**

目标网段	下一跳
0.0.0.0/0	VPN网关

VPC路由配置

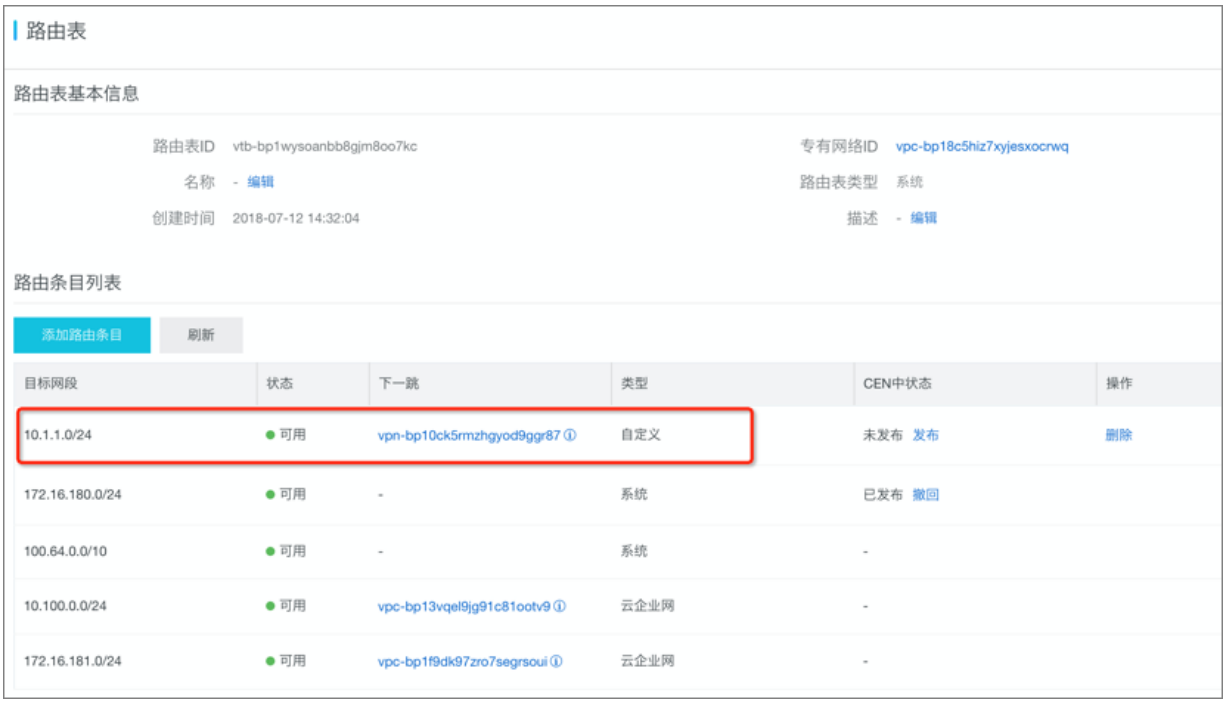


为了能够让IDC和云上的VPC之间互相通信，需要在连接VPN网关的VPC内，配置一条指向IDC侧（VPN网关）的路由，并且宣告到CEN。

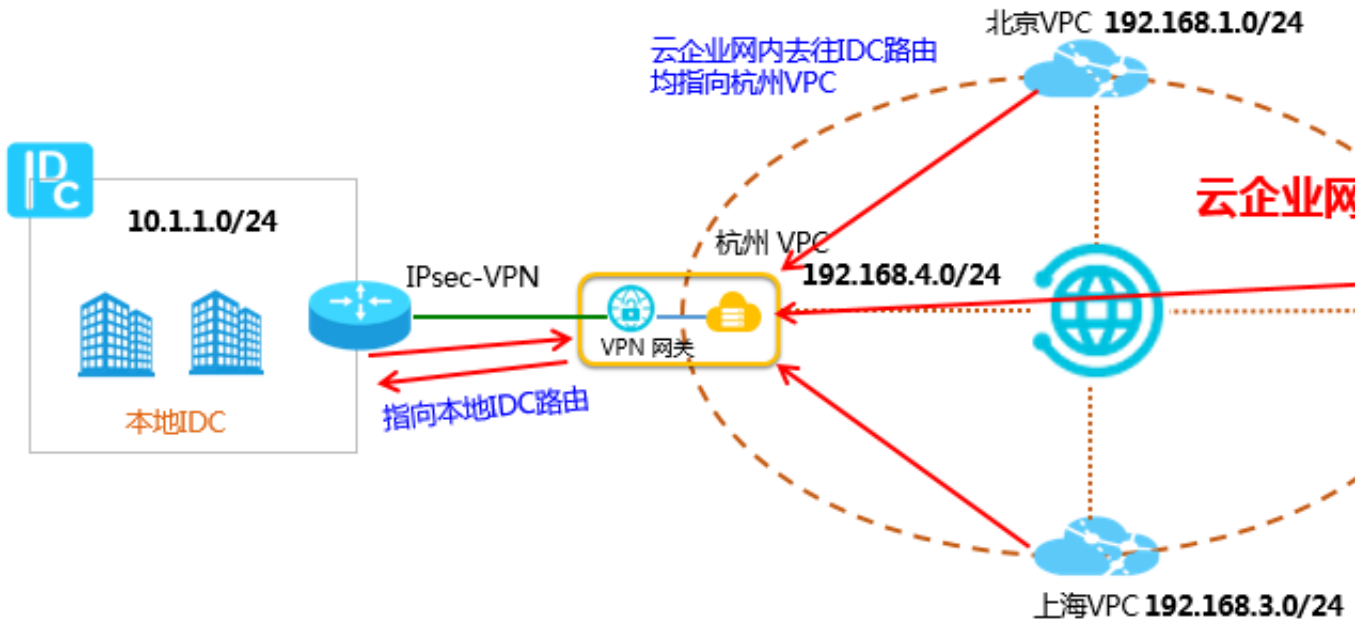
IDC侧已经配置了指向云上的路由，那么数据流量便可从云下到达云上；在杭州VPC内，配置一条回程路由指向VPN网关，便可实现流量从杭州VPC到达云下IDC。

如下图所示，您需要在杭州VPC内配置指向VPN网关（IDC）的自定义路由：

在杭州VPC路由表中可以看到该条指向VPN网关的路由：



在CEN中宣告路由

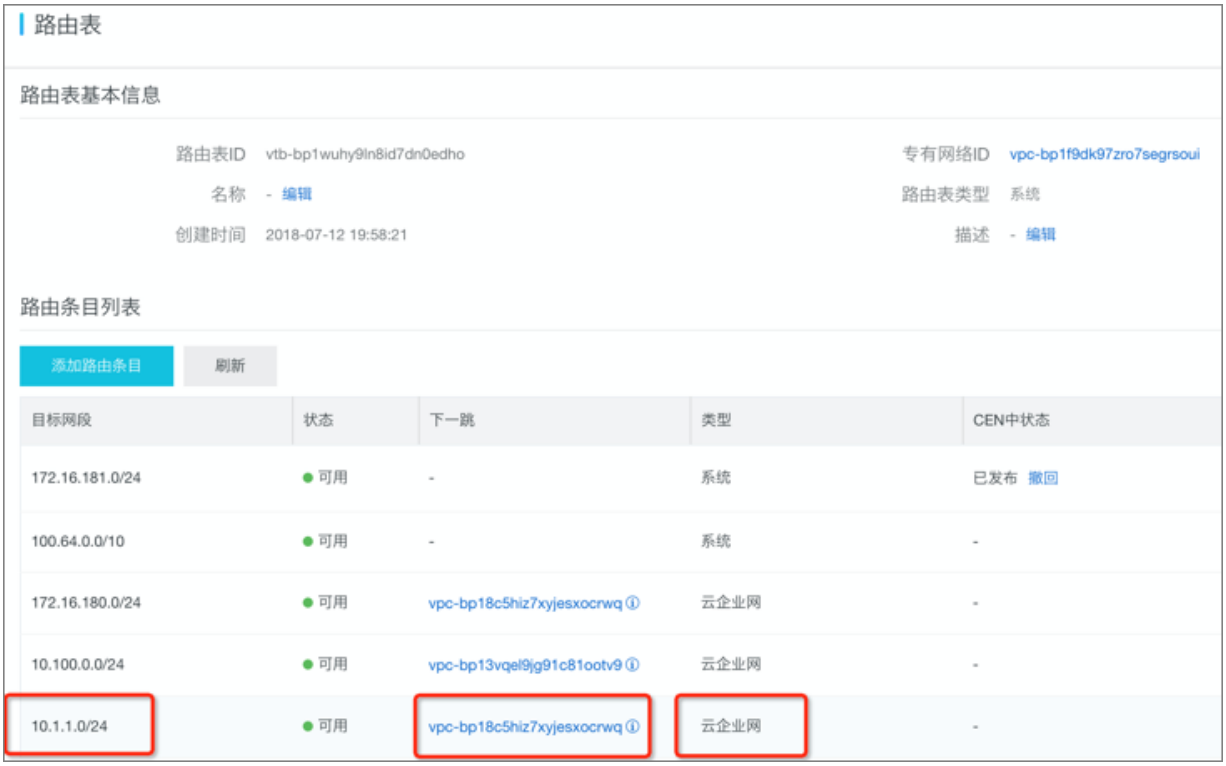


为了能够让CEN内其他VPC学习到指向IDC的路由，需要在杭州VPC将指向VPN网关的路由发布到CEN内，其他VPC便可学习到该条路由。

路由发布前

路由发布后

CEN内其他VPC路由表如下图所示。



通过以上操作，可以看到加载到CEN中的其他VPC已经学习到了该条指向IDC的路由，本地IDC便可和CEN内的任意VPC之间进行通信。

CEN发布路由功能说明

以上方案只是对加载到CEN中的网络实例向CEN发布或撤销路由的一种场景，对于加载到CEN中的VPC/VBR，支持如下的路由发布或撤销操作：

路由类型	路由所属实例	是否默认发布到CEN
指向ECS实例的路由	VPC	否
指向VPN网关的路由	VPC	否
指向高可用虚拟IP的路由	VPC	否
VPC系统路由	VPC	是
指向IDC的路由	VBR	是
BGP路由	VBR	是

以上发布到CEN中的路由，均可进行撤销操作。路由撤销后，CEN中将不再存在该路由条目。

对于各条自定义路由，如果已发布到CEN中，在VPC上删除该自定义路由后，该路由也将从CEN中删除。

说明：

目前控制台只支持VPC的路由发布和撤销，VBR路由的发布和撤销操作暂不支持，您可以通过调用Open API*PublishRouteEntries*发布、撤销VBR路由条目。

4 IDC通过专线和智能接入网关主备方式上云方案

本方案指导您如何使用云企业网、高速通道专线和智能接入网关，使本地IDC通过专线和智能接入网关以主备链路的方式接入阿里云，并和云上不同地域VPC互通。

本地IDC通过专线和智能接入网关两种方式连接到阿里云，实现主备冗余链路。其中，专线作为主链路使用BGP路由协议连接边界路由器（VBR）；智能接入网关通过云连接网（CCN）接入云企业网作为备用链路。当专线出现故障时，自动切换至智能接入网关的链路，实现高可用。

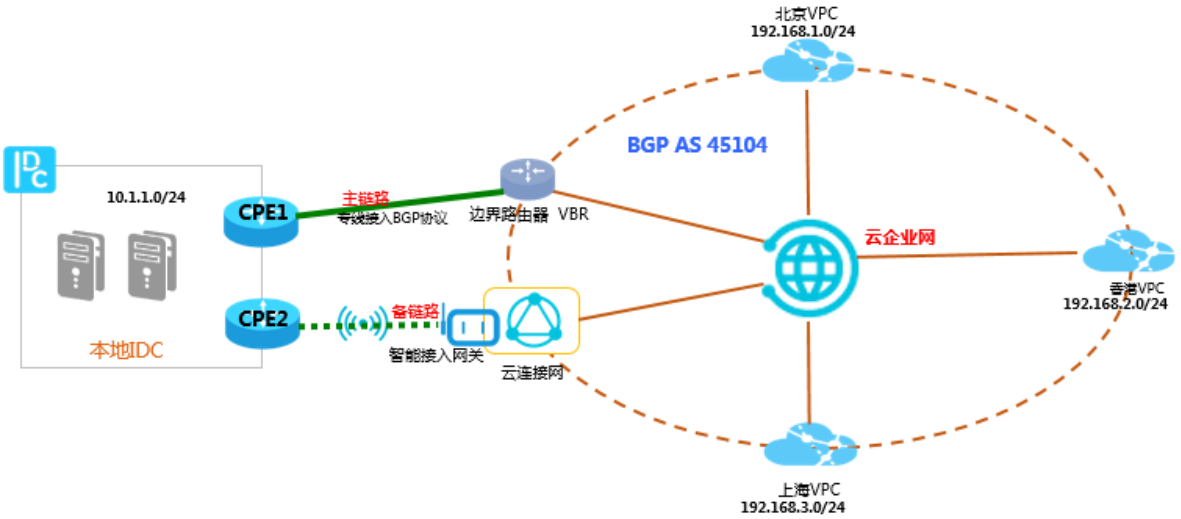
网络拓扑

本方案的网络架构如下：

- 本地IDC通过专线和智能接入网关连接到阿里云，实现冗余链路。专线上使用BGP路由协议。
- 分别在北京、香港和上海地域部署了云服务。
- 确保各地域的VPC网段和本地数据中心的网段都不冲突。本教程中各VPC和本地数据中心的IP地址段如下表所示。

网络	IP地址段
华北1（北京）VPC	192.168.1.0/24
华东2（上海）VPC	192.168.2.0/24
香港VPC	192.168.3.0/24
本地数据中心	10.1.1.0/24

- 智能接入网关和专线侧的边界路由器已经加载到云企业网中。



方案概述

云企业网内的路由优先级

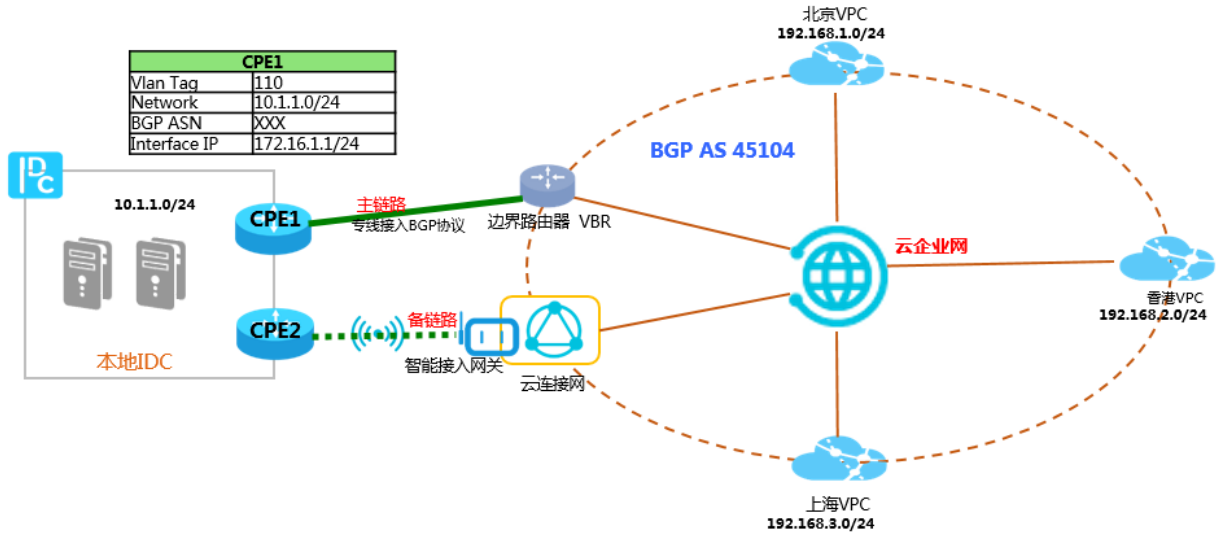
当连接相同目标网段的专线和智能接入网关同时接入云企业网时，在云企业网内对两者路由的处理优先级为：专线优于智能接入网关。

1. 专线方向宣告**BGP**路由

假设IDC和边界路由器之间，分别已经建立起BGP邻居关系。

现在需要在IDC侧配置向阿里云宣告的BGP网段10.1.1.0/24，IDC的CPE1配置如下表所示。

配置	示例值
Vlan Tag	110
Network	10.1.1.0/24
BGP ASN	xxx
Interface IP	172.16.1.1/24



2. 智能接入网关配置

1. 在智能接入网关控制台，选择和智能接入网关做主备的专线（专线永远是主链路）。

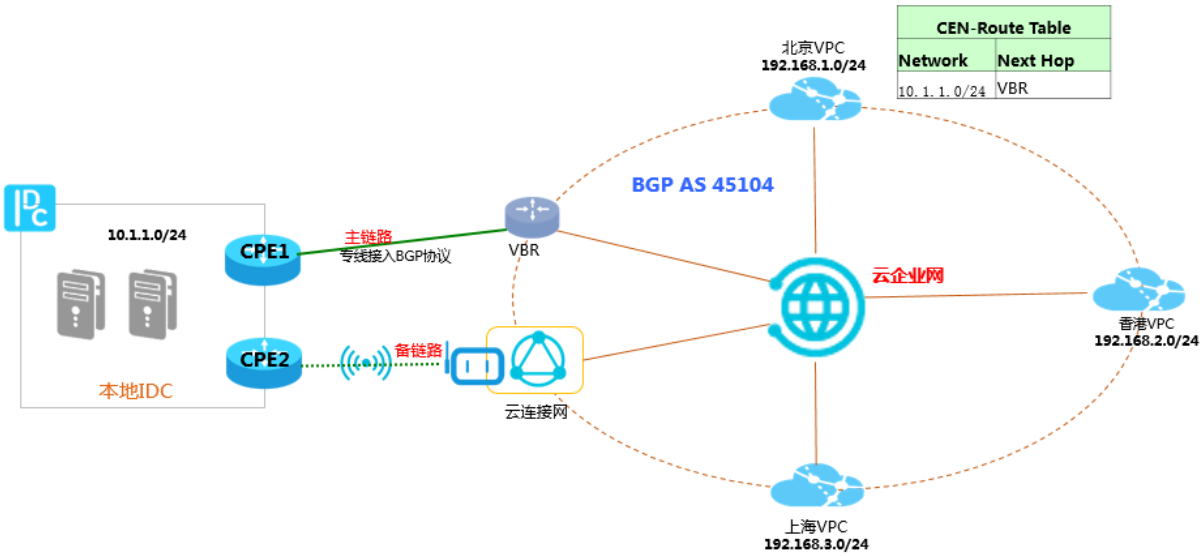
2. 在智能接入网关控制台，配置智能接入网关所连接的IDC业务地址。

   智能接入网关已经加载到云企业网中，需要在智能接入网关中配置IDC的业务地址段10.1.1.0/24。

说明：

在配置专线和智能接入网关的主备链路时，必须按照以上顺序操作。先配置主备专线，再配置智能接入网关的业务地址。如果配置顺序相反，例如先配置IP地址，由于智能接入网关已经加载到云企业网中，会出现地址冲突而不能添加IP地址的问题。配置详情参见主备链路配置教程。

3. 云企业网内路由处理



本教程中专线侧通过BGP路由协议向云企业网宣告了10.1.1.0/24网段 ，智能接入网关配置了业务地址10.1.1.0/24，由于VBR和CCN分别已加载到了云企业网内，那么该地址10.1.1.0/24也会同步到云企业网内。由于云企业网对相同网段的专线路由和智能接入网关路由处理优先级是：专线路由优先处理。那么从云企业网内的其他网络实例看到达10.1.1.0/24目标地址的下一跳是专线方向的VBR。当专线出现故障，备用链路便生效，从云上到IDC的路径会切换到智能接入网关的链路。