

企业交换机

# 产品介绍

文档版本 01  
发布日期 2023-11-17



版权所有 © 华为云计算技术有限公司 2024。保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

## 商标声明



HUAWEI和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

## 注意

您购买的产品、服务或特性等应受华为云计算技术有限公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为云计算技术有限公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

# 华为云计算技术有限公司

地址：贵州省贵安新区黔中大道交兴功路华为云数据中心 邮编：550029

网址：<https://www.huaweicloud.com/>

---

## 目录

---

1 什么是企业交换机.....	1
2 企业交换机工作原理.....	2
3 产品优势.....	6
4 约束与限制.....	9
5 权限管理.....	11
6 区域和可用区.....	13
7 与其他服务的关系.....	15
8 计费说明.....	16

# 1 什么是企业交换机

企业交换机（Enterprise Switch，简称ESW）可以在虚拟私有云（Virtual Private Cloud, VPC）内提供大二层互联等增强网络转发能力，助力企业灵活构建大规模、高性能、高可靠的云上/云下网络。

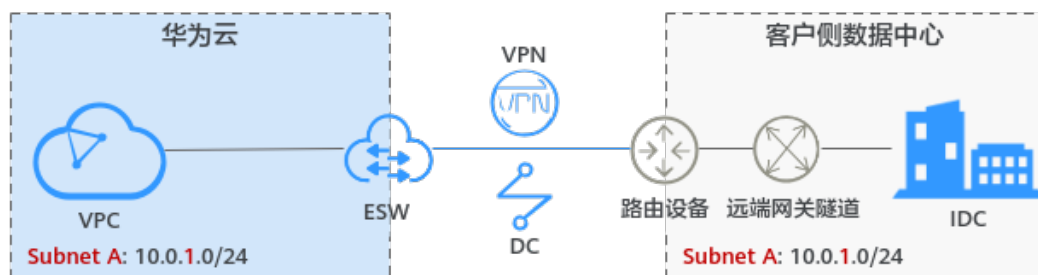
企业交换机当前仅支持二层连接网关特性，该特性提供一种虚拟隧道网关，可基于虚拟专用网络（Virtual Private Network, VPN）或者云专线（Direct Connect, DC）建立云上与云下之间的二层网络，解决云上和云下网络二层互通问题，允许您在不改变子网、IP规划的前提下将数据中心或私有云主机业务部分迁移上云。

您通过VPN或者云专线连接云上和云下互联网数据中心（Internet Data Center, IDC），此时建立的是三层网络，要求云上与云下子网网段不能重叠。

当云下IDC与云上VPC子网网段重叠，并且需要云上与云下服务器在该重叠子网网段内通信时，您需要建立二层网络，企业交换机可以帮助您实现该需求。

企业交换机作为VPC的隧道网关，与云下IDC侧隧道网关对应，基于VPN或者云专线三层网络，在VPC与云下IDC之间建立二层网络，组网示意图如图1-1所示，您需要将VPC子网接入到企业交换机中，并指定企业交换机与IDC侧的隧道网关建立连接，使VPC子网与IDC侧子网建立二层通信。

图 1-1 云下和云上二层网络组网



# 2 企业交换机工作原理

企业交换机的工作原理如图2-1所示，详细说明请参见表2-1。

图 2-1 企业交换机工作原理

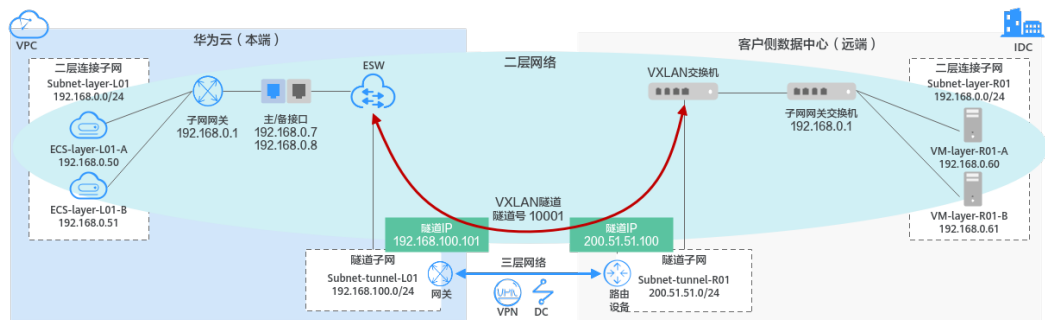


表 2-1 企业交换机工作原理说明

序号	原理	网络实例说明
1	建立本端和远端隧道子网之间的三层网络通信	<ul style="list-style-type: none"> <li>使用企业交换机之前，需要规划云下和云上所需的资源，本示例中的资源规划详情请参见表2-2。</li> <li>企业交换机建立二层通信网络时，依赖隧道子网之间的三层网络，需要使用云专线或VPN建立本端隧道子网Subnet-tunnel-L01和远端隧道子网Subnet-tunnel-R01之间的三层网络通信。</li> </ul>
2	基于隧道子网创建企业交换机	基于本端隧道子网Subnet-tunnel-L01创建企业交换机，并配置本端隧道IP（192.168.100.101），支持自动生成或手动配置。

序号	原理	网络实例说明
3	创建企业交换机的 <a href="#">二层连接</a>	<p>企业交换机创建完成后，您还需要创建二层连接，建立本端二层连接子网Subnet-layer-L01和远端VXLAN交换机之间的二层网络通信。</p> <p>创建二层连接时，需要配置以下信息：</p> <ul style="list-style-type: none"> <li>配置<a href="#">主接口IP/备接口IP</a>，支持自动生成或手动配置，该接口用来连接本端二层连接子网Subnet-layer-L01和企业交换机。</li> <li>配置<a href="#">远端隧道IP</a>（200.51.51.100）和<a href="#">隧道号</a>（10001），连通本端二层连接子网Subnet-layer-L01和远端VXLAN交换机。</li> </ul>
4	配置远端隧道网关	在远端VXLAN隧道交换机上配置隧道网关，建立远端二层连接子网Subnet-layer-R01在IDC侧的VXLAN隧道。

表 2-2 资源规划详情

网络资源名称	本端		远端	
	<a href="#">二层连接子网</a>	VPC子网	Subnet-layer-L01: 192.168.0.0/24	IDC子网
	ECS	<ul style="list-style-type: none"> <li>ECS-layer-L01-A: 192.168.0.50</li> <li>ECS-layer-L01-B: 192.168.0.51</li> </ul>	IDC服务器	<ul style="list-style-type: none"> <li>VM-layer-R01-A: 192.168.0.60</li> <li>VM-layer-R01-B: 192.168.0.61</li> </ul>
	<a href="#">主接口IP/备接口IP</a>	<ul style="list-style-type: none"> <li>主接口: 192.168.0.7</li> <li>备接口: 192.168.0.8</li> </ul>	-	-
<a href="#">隧道子网</a>	VPC子网	Subnet-tunnel-L01: 192.168.100.0/24	IDC子网	Subnet-tunnel-R01: 200.51.51.0/24
	<a href="#">隧道IP</a>	192.168.100.101	<a href="#">隧道IP</a>	200.51.51.100
<a href="#">隧道号</a>	10001			

## 二层连接子网

二层连接子网是云上VPC与云下IDC准备建立二层互通的子网，包括本端二层连接子网和远端二层连接子网。

- 本端二层连接子网：VPC的子网，该子网需要和IDC子网建立二层网络通信，例如Subnet-layer-L01。

- 远端二层连接子网：IDC的子网，该子网需要和VPC子网建立二层网络通信，例如 Subnet-layer-R01。

约束说明：

- 本端和远端二层连接子网网段可以重叠，但是本端和远端子网内需要通信的服务器地址不能相同，否则无法正常通信。
- 已被企业交换机二层连接绑定的VPC子网，不能再被其他二层连接或者企业交换机使用。

## 隧道子网

隧道子网基于云专线或者VPN实现三层网络通信，包括本端隧道子网和远端隧道子网。企业交换机需要基于隧道子网之间的三层网络，为需要互通的云上和云下子网提供二层连接通道。

- 本端隧道子网：VPC的子网，该子网需要与IDC子网建立三层网络通信，例如 Subnet-tunnel-L01。
- 远端隧道子网：IDC的子网，该子网需要与VPC子网建立三层网络通信，例如 Subnet-tunnel-R01。

约束说明：

- 企业交换机建立二层通信网络时，依赖隧道子网之间的三层网络，因此使用企业交换机前，请确保已通过VPN或者云专线打通本端和远端隧道子网的三层网络。
- 企业交换机建立二层网络通信时，需要和IDC侧建立VXLAN隧道，IDC侧交换机必须支持VXLAN功能。
- 企业交换机会占用本端隧道子网的三个IP地址，用来做企业交换机实例主备节点的负载均衡，请您规划隧道子网的时候预留足够的IP地址。

## 二层连接

企业交换机创建完成后，您还需要创建二层连接，建立本端二层连接子网和远端VXLAN交换机之间的二层网络通信。

约束说明：

- 一个二层连接可以连通一对本端和远端二层连接子网，一个企业交换机最多支持建立6个二层连接，即同时连接6对二层连接子网。
- 基于同一个企业交换机建立二层连接时，这些二层连接可以共用隧道IP，但是隧道号不能相同，隧道号是隧道的标识。
- 通过二层连接连通本端二层连接子网和企业交换机时，需要占用本端二层连接子网中的两个IP地址，用作主接口IP与备接口IP。这两个IP地址不能被本端资源占用，也不能与远端二层连接子网内的其他IP地址冲突。

## 主接口 IP/备接口 IP

通过二层连接连通本端二层连接子网和企业交换机时，需要占用本端二层连接子网中的两个IP地址，用作主接口IP与备接口IP。

## 隧道 IP

企业交换机需要和云下IDC建立VXLAN隧道实现二层网络通信，VXLAN隧道两端各需要一个隧道IP，包括本端隧道IP和远端隧道IP，两个IP地址不能冲突。

- 本端隧道IP: 属于本端隧道子网, 例如Subnet-tunnel-L01, 隧道IP为192.168.100.101。
- 远端隧道IP: 属于远端隧道子网, 例如Subnet-tunnel-R01, 隧道IP为200.51.51.100。

## 隧道号

云下IDC连接企业交换机所需要的VXLAN隧道号, 即VXLAN网络标识号(VNI), 是VXLAN隧道的标识, 用于区分不同的VXLAN隧道。

对于同一个VXLAN隧道, 云下IDC和云上隧道号一致, 即本端和远端隧道号一致。



# 3 产品优势

通常情况下，企业客户通过VPN或者云专线建立云下IDC和云上VPC之间的三层网络通信。由于三层网络通信本身限制，往往让客户上云面临IDC网络改造、上云周期延长、部分业务中断等种种困难，具体请参见[云下和云上三层网络的约束](#)。

企业交换机致力于解决客户上云面临的困难，通过建立云下IDC和云上VPC之间的二层网络通信，帮助您实现业务动态、平滑迁移上云，具体请参见[云下和云上二层网络的优势](#)。

## 云下和云上三层网络的约束

通过VPN或者云专线建立云下IDC和云上VPC之间的三层网络，组网示意请参见图3-1，客户痛点请参见表3-1。

图 3-1 云下和云上三层网络组网

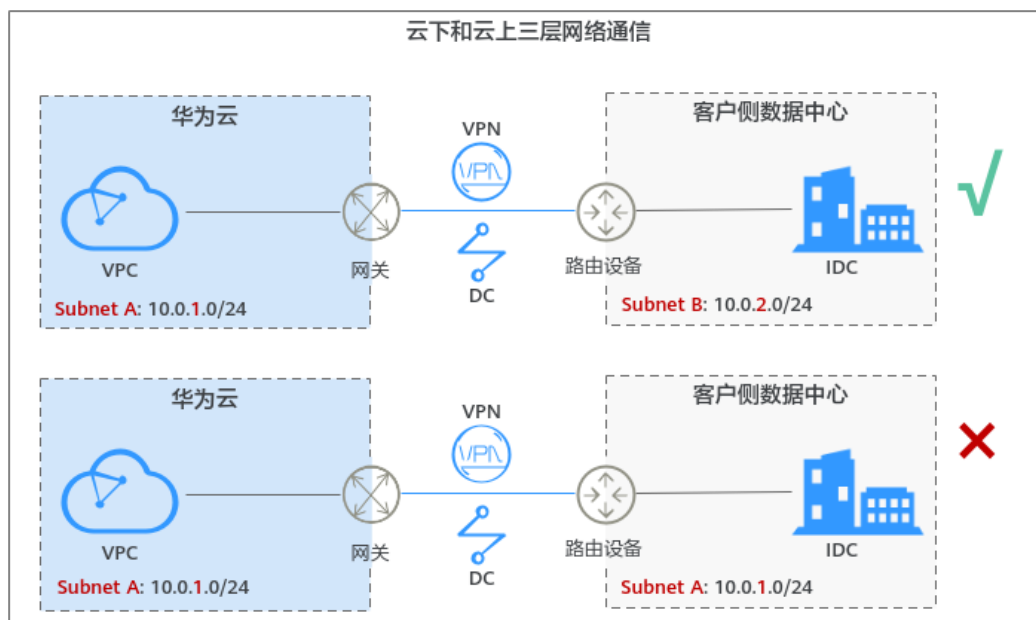


表 3-1 云下和云上三层网络说明

网络说明	云下IDC和云上VPC通过VPN或者云专线建立三层网络，通过路由通信。
客户痛点	<ul style="list-style-type: none"> <li>云下IDC子网和云上VPC子网网段不能重叠。云下IDC侧的业务网络互访很多是通过IP地址而非域名，如果IDC子网和VPC子网网段存在重叠，上云前需要改造IDC侧网络，会导致上云周期延长、迁移期间业务中断，并且网络改造往往增加运维成本。</li> <li>网络迁移最小的粒度是“子网”，并且同一个子网无法实现跨云上和云下通信。云下IDC侧的每个子网通常承载几十种不同的业务，如果按照子网粒度进行迁移，几十种业务一次性上云存在较大风险，无法满足业务连续性需求。</li> </ul>

### 云下和云上二层网络的优势

为了应对当前上云的种种痛点，推荐您使用企业交换机，建立云下IDC和云上VPC二层网络，实现轻松上云。企业交换机优势请参见表3-2。

图 3-2 云下和云上二层网络组网

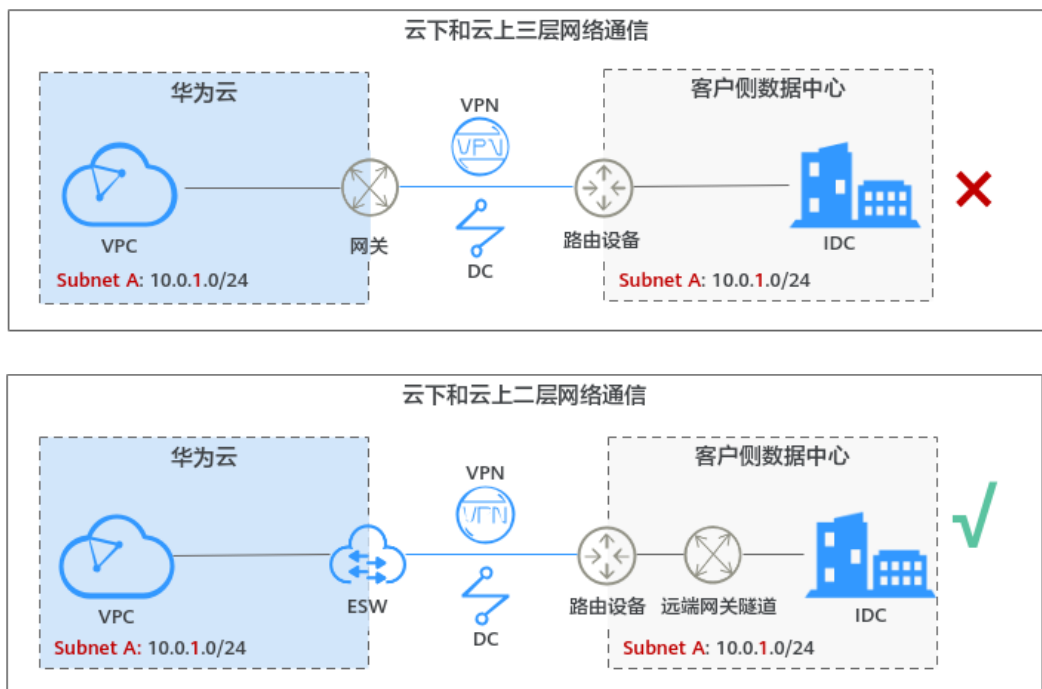


表 3-2 云下和云上二层网络说明

网络说明	企业交换机基于VPN或者云专线网络，在云下IDC和云上VPC之间建立二层网络。
------	---

<b>企业交换机优势</b>	<ul style="list-style-type: none"><li>● 云下IDC子网和云上VPC子网网段可以重叠。如果客户IDC子网和VPC子网网段存在重叠，使用企业交换机后，上云不用修改IDC侧IP地址，减少业务对环境感知，加快上云进度。</li><li>● 网络迁移粒度由“子网”变为“虚拟机”，同时支持同一个子网跨云上和云下互通。按照“虚拟机”粒度迁移上云，支持业务系统灰度上云，应对核心业务分批上云，避免业务在迁移过程中受损，减少上云风险。</li></ul>
----------------	---

# 4 约束与限制

## 配额限制

表 4-1 企业交换机配额限制

规格项	默认配额	申请更多配额
每个租户支持创建的企业交换机数量	5个	申请更多配额，请参见 <a href="#">提交工单</a>
每个企业交换机支持绑定的VPC数量	1个	不支持修改
每个VPC的子网支持连通的二层连接数量	1个	不支持修改
每个“基础型”企业交换机支持建立的二层连接数量	1个	不支持修改
每个“标准型”企业交换机支持建立的二层连接数量	3个	不支持修改
每个“增强型”企业交换机支持建立的二层连接数量	6个	不支持修改

## 使用限制

- ESW不支持IPv6报文，且不支持云下往云上转发未知单播、广播、组播（除VRRP协议外）的IP报文。
- 不支持云下服务器访问云上的高级网络功能，如VPC对等连接、VPC路由表、ELB以及NAT网关等。
- 对于使用云专线（DC）对接企业交换机的场景，请您先[提交工单](#)给云专线服务，确认您的云专线是否支持和企业交换机进行对接，如果不支持，需要联系客服开通云专线的对接企业交换机能力。
- 对于使用虚拟专用网络（VPN）对接企业交换机的场景，请您先[提交工单](#)给虚拟专用网络服务，确认您的虚拟专用网络是否支持和企业交换机进行VXLAN对接，如果不支持，需要联系客服开通虚拟专用网络的对接企业交换机能力。

- ESW支持对接VPN场景是指经典型VPN，不支持对接专业版VPN和共享型VPN。
- 云上和云下二层网络互通后，云下子网网关地址要和云上子网网关地址保持一致，否则可能导致云下子网网关地址和云上虚拟机的IP地址冲突，引发通信异常。
- 每个企业交换机最多支持10000个IP二层互通（即包含通过该企业交换机打通的所有二层网段IP），且最多同时支持连接1000个云下二层网段IP。
- 使用企业交换机建立云上与云下之间的二层网络时，客户侧负责建设IDC机房的VXLAN网络，包括VXLAN交换机准备、物理网络连通、对接云专线或者虚拟专用网络等。
- ESW支持MAC Proxy转发能力，通过ARP报文代理，使云上和云下主机相互不可见对端的实际MAC地址。在业务报文转发时，云上主机收到的云下报文源MAC是二层连接主接口的MAC，云下主机收到的云上报文源MAC是实例隧道口的MAC。如果您的业务场景需要感知实际主机MAC或者有基于MAC的安全策略等，不支持使用ESW。
- 通常，服务器端会通过ARP学习确定回复报文的的目的MAC地址，但是某些主机或硬件设备（如F5负载均衡器）配置了原路径返回能力，回复报文的的目的MAC地址取自请求报文的源MAC地址，当通过ESW实现云上云下三层访问场景时，可能会出现网络不通问题，请提前排查。  
例如，先通过ESW打通云上和云下192.168.3.0/24网段，当云上主机192.168.2.2/24需要跨网段访问云下主机192.168.3.3/24时，云上请求报文会先通过VPC路由，再经过ESW送往云下主机，云下对应回复报文走路由发回云上，可以经过云专线/VPN。如果云下主机配置了原路径返回，云下回复报文的的目的MAC地址不是192.168.3.0/24的网关MAC地址，是取对应请求报文的源MAC地址，即ESW的MAC地址。这样云下回复报文的的目的MAC地址错误，导致网络不通。
- ESW使用VXLAN协议时，VXLAN协议头占用50个字节，报文长度会增加。请您确保VXLAN报文经过的线下网络设备支持大帧（Jumbo Frames，即MTU大于1500字节的以太网帧）通过，否则会导致大包不通。

#### 📖 说明

- 不同设备厂商处理大帧的方式不同，其中部分厂商默认大帧放通，例如华为。部分厂商默认大帧不放通，例如思科。
- 如果您的IDC需要与华为云企业交换机对接来建立云下和云上二层网络通信，那么IDC侧的交换机需要支持VXLAN功能。以下为您列举部分支持VXLAN功能的交换机，仅供参考。
    - 华为交换机：Huawei CE58、CE68、CE78、CE88系列支持VXLAN，例如CE6870、CE6875、CE6881、CE6863、CE12800。
    - 其他厂商交换机：例如Cisco Nexus 9300、锐捷RG-S6250、H3C S6520。

# 5 权限管理

如果您需要对华为云上购买的ESW资源，为企业中的员工设置不同的访问权限，以达到不同员工之间的权限隔离，您可以使用统一身份认证服务（Identity and Access Management，简称IAM）进行精细的权限管理。该服务提供用户身份认证、权限分配、访问控制等功能，可以帮助您安全的控制华为云资源的访问。

通过IAM，您可以在账号中给员工创建IAM用户，并授权控制员工对华为云资源的访问范围。

如果华为账号已经能满足您的要求，不需要创建独立的IAM用户进行权限管理，您可以跳过本章节，不影响您使用ESW服务的其它功能。

IAM是华为云提供权限管理的基础服务，无需付费即可使用，您只需要为您账号中的资源进行付费。关于IAM的详细介绍，请参见《[IAM产品介绍](#)》。

## ESW 权限

默认情况下，管理员创建的IAM用户没有任何权限，需要将其加入用户组，并给用户组授予角色，才能使得用户组中的用户获得对应的权限，这一过程称为授权。授权后，用户就可以基于被授予的权限对云服务进行操作。

ESW部署时通过物理区域划分，为项目级服务。授权时，“作用范围”需要选择“区域级项目”，然后在指定区域（如亚太-曼谷）对应的项目（ap-southeast-2）中设置相关权限，并且该权限仅对此项目生效；如果在“所有项目”中设置权限，则该权限在所有区域项目中都生效。访问ESW时，需要先切换至授权区域。

ESW服务没有独立的系统权限，和VPC共用一套系统权限，VPC系统权限如表1所示，包括了VPC的所有系统角色。由于华为云各服务之间存在业务交互关系，VPC的角色依赖其他服务的角色实现功能。因此给用户授予VPC的角色时，需要同时授予依赖的角色，VPC的权限才能生效。

表 5-1 VPC 系统权限

策略名称	描述	策略类别	依赖关系
VPC FullAccess	虚拟私有云的所有执行权限。	系统策略	如果您需要使用VPC流日志功能，则依赖云日志服务的只读权限LTS ReadOnlyAccess。

策略名称	描述	策略类别	依赖关系
VPC ReadOnlyAccess	虚拟私有云的只读权限。	系统策略	无
VPC Administrator	虚拟私有云的大部分操作权限， 不包括创建、修改、删除、查看 安全组以及安全组规则。 拥有该权限的用户必须同时拥有 Tenant Guest权限。	系统角色	依赖Tenant Guest策略，在同项目中勾选依赖的策略。

## 相关链接

- [IAM产品介绍](#)
- [创建用户组并授权使用ESW](#)

# 6 区域和可用区

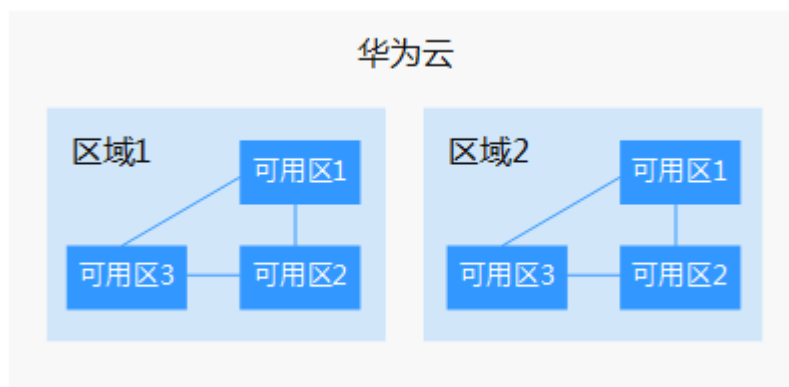
## 什么是区域、可用区？

区域和可用区用来描述数据中心的位置，您可以在特定的区域、可用区创建资源。

- 区域（Region）：从地理位置和网络时延维度划分，同一个Region内共享弹性计算、块存储、对象存储、VPC网络、弹性公网IP、镜像等公共服务。Region分为通用Region和专属Region，通用Region指面向公共租户提供通用云服务的Region；专属Region指只承载同一类业务或只面向特定租户提供业务服务的专用Region。
- 可用区（AZ，Availability Zone）：一个AZ是一个或多个物理数据中心的集合，有独立的风火水电，AZ内逻辑上再将计算、网络、存储等资源划分成多个集群。一个Region中的多个AZ间通过高速光纤相连，以满足用户跨AZ构建高可用性系统的需求。

图6-1阐明了区域和可用区之间的关系。

图 6-1 区域和可用区



目前，华为云已在全球多个地域开放云服务，您可以根据需求选择适合自己的区域和可用区。更多信息请参见[华为云全球站点](#)。

## 如何选择区域？

选择区域时，您需要考虑以下几个因素：



- 地理位置

一般情况下，建议就近选择靠近您或者您的目标用户的区域，这样可以减少网络时延，提高访问速度。

- 在除中国大陆以外的亚太地区有业务的用户，可以选择“中国-香港”、“亚太-曼谷”或“亚太-新加坡”区域。
- 在非洲地区有业务的用户，可以选择“非洲-约翰内斯堡”区域。
- 在拉丁美洲地区有业务的用户，可以选择“拉美-圣地亚哥”区域。

 说明

“拉美-圣地亚哥”区域位于智利。

- 资源的价格

不同区域的资源价格可能有差异，请参见[华为云服务价格详情](#)。

## 如何选择可用区？

是否将资源放在同一可用区内，主要取决于您对容灾能力和网络时延的要求。

- 如果您的应用需要较高的容灾能力，建议您将资源部署在同一区域的不同可用区内。
- 如果您的应用要求实例之间的网络延时较低，则建议您将资源创建在同一可用区内。

## 区域和终端节点

当您通过API使用资源时，您必须指定其区域终端节点。有关华为云的区域和终端节点的更多信息，请参阅[地区和终端节点](#)。

# 7 与其他服务的关系

企业交换机与华为云上多个云服务之间存在交互关系，如图7-1所示。

图 7-1 企业交换机与其他服务的关系

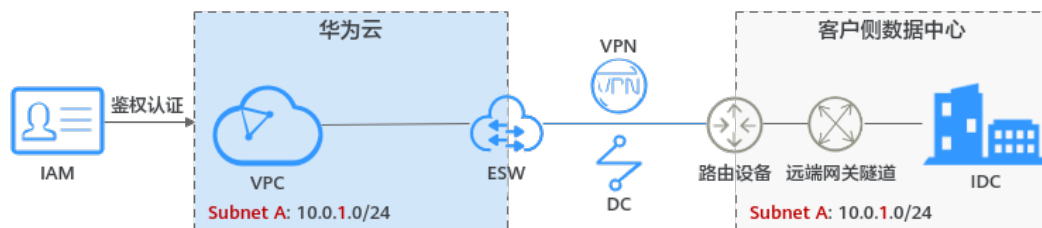


表 7-1 企业交换机与其他服务的关系

服务名称	交互功能
虚拟私有云 ( Virtual Private Cloud, VPC )	您通过企业交换机可以建立云下IDC和云上VPC之间的二层网络。
云专线 ( Direct Connect, DC )	通过VPN或云专线在云下IDC和云上VPC之间实现三层网络通信，基于三层网络，企业交换机建立云下和云上之间的二层网络。
虚拟专用网络 ( Virtual Private Network, VPN )	
统一身份认证服务 ( Identity and Access Management, IAM )	针对位于华为云上的企业交换机资源，您可以通过IAM进行权限管理，即为不同的用户设置不同的使用权限，权限管理有助于实现资源的安全管控。

# 8 计费说明

## 计费项

企业交换机根据您选择的规格进行计费，当前支持“基础型”、“标准型”和“增强型”规格。

详细的价格说明请参考[企业交换机价格计算器](#)。

## 计费模式

企业交换机支持包年/包月、按需付费两种计费方式。企业交换机的计费情况详细介绍见[表8-1](#)：

表 8-1 企业交换机计费情况说明

计费模式	计费说明	操作ESW对计费项的影响
包年/包月	<p>购买包年/包月ESW时，需要一次性支付选定周期内企业交换机实例的费用，不同规格包周期费用不同，具体以页面实际结算为准。包周期计费企业交换机规格如下：</p> <ul style="list-style-type: none"><li>“基础型”规格</li><li>“标准型”规格</li><li>“增强型”规格</li></ul> <p><b>说明</b> ESW包年/包月计费模式当前仅在“拉美-圣地亚哥”和“非洲-约翰内斯堡”区域上线。</p>	<p>购买后支持退订，扣除实际使用的费用和部分优惠费用，请以实际扣费为准。</p>

计费模式	计费说明	操作ESW对计费项的影响
按需计费	按需计费的企业交换机：后付费。创建企业交换机实例成功后即开始计费。按秒计费，按小时结算，不足一小时以实际使用时长为准。按需计费企业交换机规格如下： <ul style="list-style-type: none"><li>“基础型”规格</li><li>“标准型”规格</li><li>“增强型”规格</li></ul>	-

### 📖 说明

当前支持的企业交换机规格如下：

- 基础型
  - 最大带宽：3 Gbit/s
  - 最大发包数：500000 pps
  - 连接子网数：1
- 标准型
  - 最大带宽：5 Gbit/s
  - 最大发包数：1000000 pps
  - 连接子网数：3
- 增强型
  - 最大带宽：10 Gbit/s
  - 最大发包数：2000000 pps
  - 连接子网数：6

## 如何为企业交换机续费，账号欠费后会有什么影响？

当您的账号欠费后，会对您的资源使用产生如下影响：

- 包年/包月资源：当您的包年/包月资源到期未续费，首先会进入宽限期。如果您在宽限期内仍未续订包年/包月资源，那么就会进入保留期。  
您无法对处于宽限期或者保留期的包年/包月资源执行任何操作，因此，为了确保您的业务不受影响，请您在资源到期前，及时续费，详细操作请参考[续费管理](#)。
- 按需计费资源：当您的按需资源欠费时，首先会进入宽限期。如果您在宽限期内仍未缴清按需资源的欠费，那么就会进入保留期。  
您可以对处于宽限期的按需计费资源正常执行操作，当进入保留期后，您无法对该资源执行任何操作。