企业交换机

最佳实践

文档版本 04

发布日期 2024-08-22

华为技术有限公司

商标声明


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。

安全声明

漏洞处理流程

华为公司对产品漏洞管理的规定以“漏洞处理流程”为准，该流程的详细内容请参见如下网址：
https://www.huawei.com/cn/psirt/vul-response-process
如企业客户须获取漏洞信息，请参见如下网址：
https://securitybulletin.huawei.com/enterprise/cn/security-advisory

目 录

1 使用企业交换机构建 IDC 和云上的大二层网络

1.1 方案概述

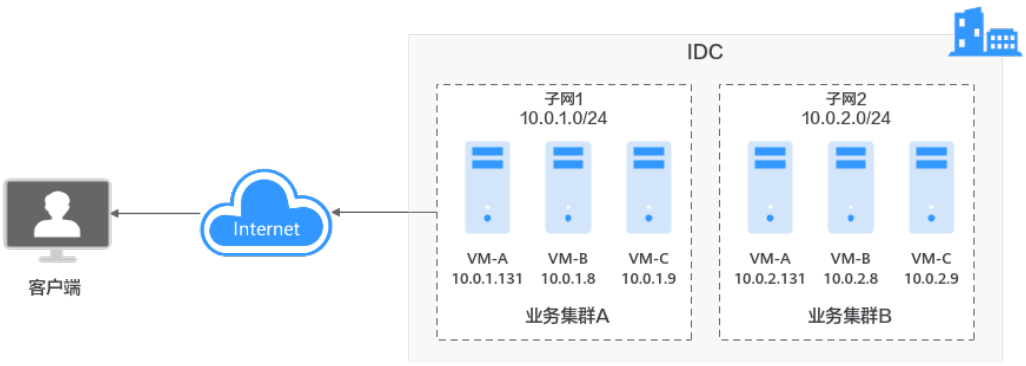
应用场景

某公司希望将云下IDC的部分业务迁移上云，在IDC内，业务主机采用集群部署，组网示意图如图1-1所示。

迁移上云过程中，该公司有以下诉求：

- 按主机粒度迁移上云，迁移中不能中断业务。
- 由于IDC内主机访问配置文件中记录的不是域名地址，而是真实的IP地址，迁移上云不改变原有主机IP地址。

图 1-1 IDC 内业务集群架构



方案架构

华为云支持通过企业交换机（Enterprise Switch，ESW）构建客户IDC和云上二层网络互通，在二层网络内，实现主机粒度迁移，助力客户IDC迁移上云期间业务不中断，不修改IP地址的诉求。

通过企业交换机迁移IDC的组网示例如图1-2所示，本示例中将IDC内的VM-B在不修改IP的前提下，迁移到云上。迁移过程说明如下：

1. 使用云专线或VPN建立云上与云下IDC隧道子网之间的三层网络通信。因为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。
2. 创建企业交换机、建立二层连接、配置VXLAN交换机，建立云上与云下IDC的二层网络通信。
3. 将主机VM-B（10.0.1.8）迁移到云上ECS-B（10.0.1.21），检查好VM-B和ECS-B的网络通信后，待业务低谷时期关闭IDC内的VM-B。

   短暂关闭VM-B时，业务主要由IDC内的VM-A（10.0.1.131）承载，因此不会中断业务。

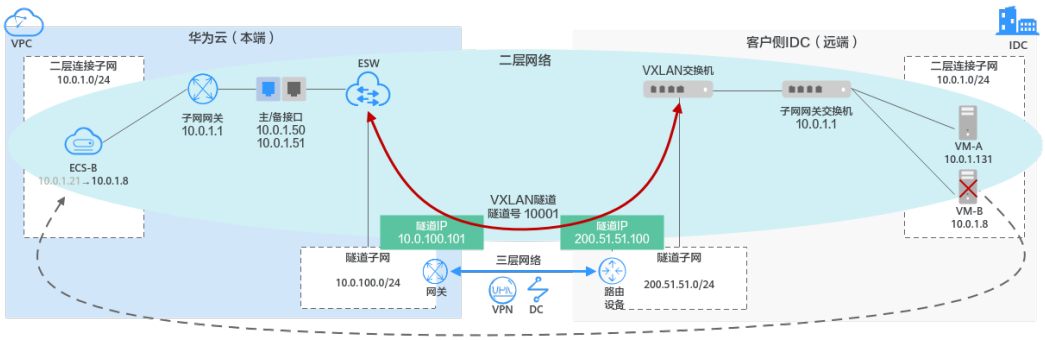
须知

此处为了验证VM-B和ECS-B之前的正常通信，刚迁移上云的ECS-B和VM-B的IP地址不能一样，否则无法正常通信。

4. 关闭IDC内的VM-B后，将云上的ECS-B地址由10.0.1.21改为10.0.1.8，此时业务流量会通过企业交换机转发到云上的ECS-B处理，确保迁移后不改变主机IP地址。

   同时，云上的ECS-B和IDC内的VM-A也可以自由互访，就像还位于同一个子网中。

图 1-2 企业交换机迁移组网



方案优势

- 云下IDC侧的业务网络互访很多是通过IP地址而非域名，上云前如果改造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。

  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。
- 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。

  使用企业交换机后，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。

约束与限制

- 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。

- 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。
- 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。

1.2 主机粒度迁移，不中断业务上云（VPN+ESW）

方案架构

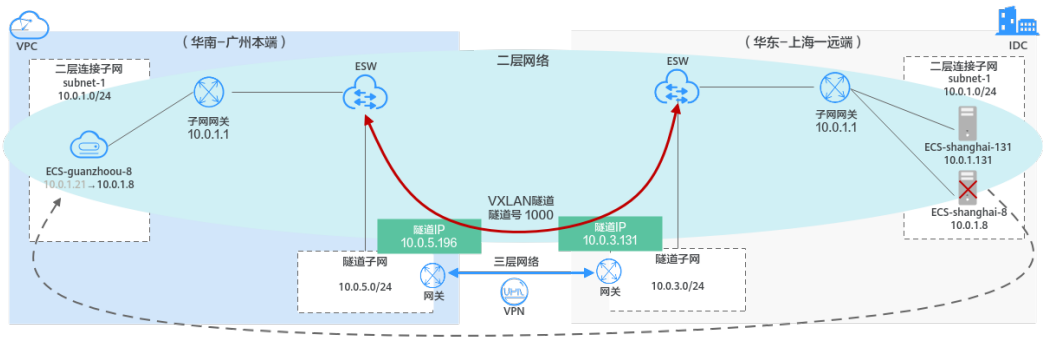
客户的模拟场景说明如下：

- 华东-上海一：用作模拟客户IDC，部门A的业务部署在subnet-1内的主机10.0.1.131和主机10.0.1.8上，两台主机组成集群对外提供服务。
- 华南-广州：用作模拟客户迁移上云的区域，部门A业务所在的主机10.0.1.8待迁移到华为云上。

本最佳实践提供的迁移方案说明如下：

1. 使用VPN和ESW打通“华东-上海一”和“华南-广州”两个子网之间的二层网络，将主机10.0.1.8迁移到云上子网内。
2. 迁移完成后，删除IDC内主机10.0.1.8，主机10.0.1.131能够和云上的主机10.0.1.8相互访问。

图 1-3 企业交换机迁移组网（VPN+ESW）



资源和成本规划

表 1-1 资源和成本规划

区域	资源	资源名称	资源说明	数量	每月费用（元）
华南-广州： 模拟华为云（本端）	虚拟私有云 VPC	vpc-guangzhou	VPC网段：10.0.0.0/16	1	00.00
	虚拟私有云子网	subnet-1	子网网段：10.0.1.0/24 本端二层连接子网，模拟华为云业务集群所在的子网，此处为迁移后的ECS所在子网	2	00.00
		subnet-5	子网网段：10.0.5.0/24 本端隧道子网，模拟华为云上的隧道子网，此处为VPN所在子网		
	弹性云服务器 ECS	ecs-guangzhou -8	私有IP地址：10.0.1.21 模拟华为云内的主机，此台主机为迁移后的主机，迁移前IP地址为10.0.1.21，迁移完成后，修改IP地址为10.0.1.8	1	263.90
	虚拟专用网络 VPN	vpn-guangzhou	• 本端子网：subnet-5 • 远端网关：119.3.121.173，此处填写华东-上海一VPN的本端网关 • 远端子网：10.0.3.0/24，此处填写华东-上海一VPN所在的子网	1	375.00
	企业交换机 ESW	l2cg-guangzhou	• 隧道连接方式：VPN • 关联网关：vpngw-guangzhou • 隧道子网：subnet-5	1	65000.00
	二层连接	l2conn-guangzhou	• 隧道IP：10.0.5.196 • 隧道号：1000	1	00.00
华东-上海一 模拟客户IDC（远端）	虚拟私有云 VPC	vpc-shanghai	VPC网段：10.0.0.0/16	1	00.00

区域	资源	资源名称	资源说明	数量	每月费用（元）
	虚拟私有云子网	subnet-1	子网网段：10.0.1.0/24 远端二层连接子网，模拟客户IDC业务集群所在的子网，此处为待迁移的主机所在子网	2	00.00
		subnet-3	子网网段：10.0.3.0/24 远端隧道子网，模拟客户IDC内的隧道子网，此处为VPN所在子网		
	弹性云服务器 ECS	ecs-shanghai -131	私有IP地址：10.0.1.131 模拟客户IDC内集群中的主机	2	527.80
		ecs-shanghai -8	私有IP地址：10.0.1.8 模拟客户IDC内的主机，此台主机待迁移		
	虚拟专用网络 VPN	vpn-shanghai	• 本端子网：subnet-3 • 远端网关：139.9.20.226，此处填写华南-广州VPN的本端网关 • 远端子网：10.0.5.0/24，此处填写华南-广州VPN所在的子网	1	375.00
	企业交换机 ESW	l2cg-shanghai	• 隧道连接方式：VPN • 关联网关：vpngw-shanghai • 隧道子网：subnet-3	1	65000.00
	二层连接	l2conn-shanghai	• 隧道IP：10.0.3.131 • 隧道号：1000	1	00.00

资源成本费用预估为131541.70元，该费用中，不包括迁移主机产生的费用，迁移费用详情请参见**计费说明**。

须知

本文提供的成本预估费用仅供参考，资源的实际费用以华为云管理控制台显示为准。

步骤一：创建 VPC 和子网

步骤1 登录华为云管理控制台，并选择“华东-上海一”区域。

步骤2 选择“网络 > 虚拟私有云”，单击“创建虚拟私有云”。

步骤3 根据资源和成本规划配置华东-上海一的VPC，完成后单击“立即创建”。

- 区域：选择华东-上海一
- 名称：vpc-shanghai
- IPv4网段：10.0.0.0/16
- 名称：subnet-1
- 子网IPv4网段：10.0.1.0/24
- 单击“添加子网”
  - 名称：subnet-3
  - 子网IPv4网段：10.0.3.0/24
- 未提及参数，保持默认或根据界面引导配置

步骤4 在VPC列表页查看创建结果。

步骤5 单击“创建虚拟私有云”，根据资源和成本规划配置华南-广州的VPC，完成后单击“立即创建”。

- 区域：选择华南-广州
- 名称：vpc-guangzhou
- IPv4网段：10.0.0.0/16
- 名称：subnet-1
- 子网IPv4网段：10.0.1.0/24
- 单击“添加子网”
  - 名称：subnet-5
  - 子网IPv4网段：10.0.5.0/24
- 未提及参数，保持默认或根据界面引导配置

步骤6 在VPC列表页查看创建结果。

----结束

步骤二：创建弹性云服务器

步骤1 选择“计算 > 弹性云服务器”，单击“购买弹性云服务器”。

步骤2 根据资源和成本规划配置华东-上海一的弹性云服务器的基础信息，完成后单击“下一步：网络配置”。

- 计费模式：按需计费。
- 区域：选择华东-上海一。
- 规格：用户自定义。本实践以c6.large.2举例。
- 镜像：公共镜像。具体镜像用户自定义，本实践以CentOS 8.0举例。
- 未提及参数，保持默认或根据界面引导配置。

步骤3 配置ECS的网络信息，完成后单击“下一步：高级配置”。

- 网络：选择“vpc-shanghai ”，并选择“手动分配IP地址”，指定IP地址。
- 安全组：Sys-FullAccess。本实践选择一个全部放通的安全组作为测试安全组，后期可以根据业务情况重新绑定业务所需的安全组，提升业务安全性。
- 弹性公网IP：暂不购买。
- 未提及参数，保持默认或根据界面引导配置。

步骤4 设置云服务器名称和密码等信息，完成后单击“下一步：确认配置”。

- 云服务器名称：ecs-shanghai -131。
- 登录凭证：密码；并输入密码。
- 未提及参数，保持默认或根据界面引导配置。

步骤5 确认ECS信息无误后，勾选“协议”并单击“立即购买”，完成ECS创建。

步骤6 单击弹性云服务器总览页面所在行的“远程登录”，选择VNC方式登录。

步骤7 使用root账号登录ECS，并执行如下命令查询ECS的私网IP地址是否为规划的IP地址。

ifconfig

```
[root@ecs-shanghai-131 ~]# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.1.131  netmask 255.255.255.0  broadcast 10.0.1.255
        inet6 fe80::f816:3eff:fe98:e592  prefixlen 64  scopeid 0x20<link>
        ether fa:16:3e:98:e5:92  txqueuelen 1000  (Ethernet)
        RX packets 158  bytes 29685 (28.9 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 245  bytes 25442 (24.8 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 2  bytes 168 (168.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2  bytes 168 (168.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

步骤8 重复**步骤1**~**步骤7**，完成华东-上海一ecs-shanghai -8（10.0.1.8）和华南-广州ecs-guangzhou -8（10.0.1.8）的ECS的创建。

步骤9 使用root账号登录ecs-shanghai -131，执行如下命令确认子网内的主机可以相互访问。

ping 10.0.1.8

```
[root@ecs-shanghai-131 ~]# ping 10.0.1.8
PING 10.0.1.8 (10.0.1.8) 56(84) bytes of data.
64 bytes from 10.0.1.8: icmp_seq=1 ttl=64 time=0.361 ms
64 bytes from 10.0.1.8: icmp_seq=2 ttl=64 time=0.395 ms
64 bytes from 10.0.1.8: icmp_seq=3 ttl=64 time=0.331 ms
64 bytes from 10.0.1.8: icmp_seq=4 ttl=64 time=0.258 ms
^C
--- 10.0.1.8 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 79ms
rtt min/avg/max/mdev = 0.258/0.336/0.395/0.052 ms
```


----结束

步骤三：创建 VPN

步骤1 选择“网络 > 虚拟专用网络”，选择“VPN网关”，并单击“创建VPN网关”。

步骤2 根据**资源和成本规划**配置VPN参数，完成后单击“立即购买”。

- VPN网关
  - 计费模式：按需计费。
  - 区域：华东-上海一。
  - 虚拟私有云：vpc-shanghai 。
  - 计费方式：按流量计费。
- VPN连接
  - 名称：vpn-shanghai 。
  - 本端子网：subnet-3。
  - 远端网关：1.1.1.1。这里随意填写一个临时的网关，待远端VPN网关（华南-广州）创建成功后，再修改为正确的远端网关。
  - 远端子网：10.0.5.0/24，填写华南-广州的子网。
  - 输入密钥。请记录此密钥，目标端VPN（华南-广州）创建时，需要与此处的密钥相同。
- 未提及参数，保持默认或根据界面引导配置。

步骤3 确认信息无误后，单击“提交”。

步骤4 在“VPN连接”页签，记录“本端网关”和“本端子网”信息，以便创建华南-广州的VPN网关时使用。

步骤5 重复**步骤1**~**步骤4**，创建华南-广州的VPN，其中关键参数信息如下。

- VPN网关
  - 计费模式：按需计费。
  - 区域：华南-广州。
  - 虚拟私有云：vpngw-guangzhou 。
  - 计费方式：按流量计费。
- VPN连接
  - 名称：vpn-guangzhou 。
  - 本端子网：subnet-5。
  - 远端网关：填写华东-上海一的“本端网关”，具体IP从**步骤4**中获取，例如119.3.121.173。
  - 远端子网：10.0.3.0/24，填写华东-上海一的“本端子网”。
  - 输入密钥，与华东-上海一VPN网关创建时输入的相同。
- 未提及参数，保持默认或根据界面引导配置。

步骤6 在“VPN连接”页签，记录“本端网关”信息，以便修改华东-上海一的VPN网关参数。

步骤7 切换到华东-上海一的VPN控制台，单击vpn-shanghai 所在行的“更多 > 修改”，修改“远端网关”参数为vpn-guangzhou 的“本端网关”，完成后单击“确定”。

步骤8 请**提交工单**给VPN服务，确认您的VPN是否支持和企业交换机对接（VXLAN），如果不支持则需要VPN服务开通对接。

至此华东-上海一和华南-广州的两个子网的VPN已配置成功，VPN的状态为“未连接”，待两个子网间有流量请求时VPN网关才正式生效。

----结束

步骤四：配置企业交换机

步骤1 在系统首页，选择“网络>企业交换机”。

进入企业交换机页面。

步骤2 在界面右上角，单击“购买”。

进入企业交换机购买页面。

步骤3 根据**资源和成本规划**配置参数，购买华东-上海一的企业交换机，完成后单击“立即购买”。

- 区域：华东-上海一
- 隧道连接方式：VPN
- 关联网关：vpngw-shanghai
- 隧道子网：subnet-3
- 名称：l2cg-shanghai
- 未提及参数，保持默认或根据界面引导配置

步骤4 创建过程大约需要6分钟，记录l2cg-shanghai 的“本端隧道IP”地址（10.0.3.131）。

创建过程中，请手动单击页面刷新按钮刷新页面。

步骤5 重复**步骤1**~**步骤3**，创建购买华南-广州的企业交换机，关键参数如下。

- 区域：华南-广州
- 隧道连接方式：VPN
- 关联网关：vpngw-guangzhou
- 隧道子网：subnet-5
- 名称：l2cg-guangzhou
- 未提及参数，保持默认或根据界面引导配置

步骤6 创建过程大约需要6分钟，记录l2cg-guangzhou 的“本端隧道IP”地址（10.0.5.196）。

创建过程中，请手动单击页面刷新按钮刷新页面。

步骤7 单击“l2cg-guangzhou ”页面的“创建连接”，配置源端接入信息，完成后单击“创建”。

- 隧道号：1000

- 隧道IP：填写l2cg-shanghai 的“本端隧道IP”地址（ 10.0.3.131 ）
- 名称：l2conn-guangzhou
- 未提及参数，保持默认或根据界面引导配置

步骤8 创建过程大约需要2分钟，状态变为“已连接”表示华南-广州Region的二层连接创建成功。

创建过程中，请手动单击页面刷新按钮刷新页面。

步骤9 切换到l2cg-shanghai ，并单击“l2cg-shanghai ”页面的“创建连接”，配置源端接入信息，完成后单击“创建”。

- 隧道号：1000
- 隧道IP：填写l2cg-guangzhou 的“本端隧道IP”地址（ 10.0.5.196 ）
- 名称：l2conn-shanghai
- 未提及参数，保持默认或根据界面引导配置

步骤10 创建过程大约需要2分钟，状态变为“已连接”表示华东-上海一Region的二层连接创建成功。

创建过程中，请手动单击页面刷新按钮刷新页面。

----结束

步骤五：迁移云下主机至云上

步骤1 将华东-上海一的ecs-shanghai -8（ 10.0.1.8 ）迁移到华南-广州的ecs-guangzhou -8（ 10.0.1.21 ）。

迁移具体操作，请参见**主机迁移服务快速入门**。

步骤2 迁移完成后，验证华东-上海一的ecs-shanghai -131（ 10.0.1.131 ）和华南-广州的ecs-guangzhou -8（ 10.0.1.21 ）之间二层网络通信。

1. 选择“计算 > 弹性云服务器”，切换为“华东-上海一”区域。
2. 登录ecs-shanghai -131。

   弹性云服务器有多种登录方法，具体请参见**登录弹性云服务器**。

   本示例是通过管理控制台远程登录（ VNC方式 ）。
3. 执行以下命令，验证ecs-shanghai -131访问ecs-guangzhou -8。

   ping 10.0.1.21
4. 选择“计算 > 弹性云服务器”，切换为“华南-广州”区域。
5. 登录ecs-guangzhou -8。

   弹性云服务器有多种登录方法，具体请参见**登录弹性云服务器**。

   本示例是通过管理控制台远程登录（ VNC方式 ）。
6. 执行以下命令，验证ecs-guangzhou -8访问ecs-shanghai -131。

   ping 10.0.1.131

----结束

步骤六：修改云上主机 IP 地址

步骤1 选择“计算 > 弹性云服务器”，切换为“华东-上海一”区域。

步骤2 在ecs-shanghai -8（10.0.1.8）所在行的操作列下，选择“更多 > 关机”，关闭ecs-shanghai -8。

步骤3 选择“计算 > 弹性云服务器”，切换为“华南-广州”区域。

步骤4 在ecs-guangzhou -8（10.0.1.21）所在行的操作列下，选择“更多 > 关机”，关闭ecs-guangzhou -8。

步骤5 关闭ecs-guangzhou -8，继续选择“更多 > 网络设置 > 修改私有IP”。

根据界面提示，将ecs-guangzhou -8的私有IP由10.0.1.21改为10.0.1.8。

----结束

步骤七：验证云上和云下主机网络通信

步骤1 选择“计算 > 弹性云服务器”，切换为“华东-上海一”区域。

步骤2 在ecs-shanghai -8（10.0.1.8）所在行的操作列下，选择“更多 > 删除”，并释放弹性公网IP和数据盘。

模拟IDC内主机业务完全迁移上云后、删除主机。

步骤3 登录ecs-shanghai -131（10.0.1.131）。

弹性云服务器有多种登录方法，具体请参见**登录弹性云服务器**。

本示例是通过管理控制台远程登录（VNC方式）。

步骤4 执行以下命令，验证ecs-shanghai -131访问ecs-guangzhou -8。

ping 10.0.1.8

回显类似如下信息，表示网络通信正常。

```
[root@ecs-shanghai-131 ~]# ping 10.0.1.8
PING 10.0.1.8 (10.0.1.8) 56(84) bytes of data.
64 bytes from 10.0.1.8: icmp_seq=1 ttl=64 time=34.7 ms
64 bytes from 10.0.1.8: icmp_seq=2 ttl=64 time=34.2 ms
64 bytes from 10.0.1.8: icmp_seq=3 ttl=64 time=34.2 ms
64 bytes from 10.0.1.8: icmp_seq=4 ttl=64 time=34.0 ms
64 bytes from 10.0.1.8: icmp_seq=5 ttl=64 time=34.3 ms
64 bytes from 10.0.1.8: icmp_seq=6 ttl=64 time=34.0 ms
64 bytes from 10.0.1.8: icmp_seq=7 ttl=64 time=33.9 ms
64 bytes from 10.0.1.8: icmp_seq=8 ttl=64 time=34.2 ms
^C
--- 10.0.1.8 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 17ms
rtt min/avg/max/mdev = 33.933/34.176/34.677/0.297 ms
[root@ecs-shanghai-131 ~]# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.1.131  netmask 255.255.255.0  broadcast 10.0.1.255
        inet6 fe80::f816:3eff:fe98:e592  prefixlen 64  scopeid 0x20<link>
        ether fa:16:3e:98:e5:92  txqueuelen 1000  (Ethernet)
        RX packets 4417  bytes 1537165 (1.4 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4632  bytes 1005171 (981.6 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```


步骤5 选择“计算 > 弹性云服务器”，切换为“华南-广州”区域。

步骤6 登录ecs-guangzhou -8（10.0.1.8）。

弹性云服务器有多种登录方法，具体请参见**登录弹性云服务器**。

本示例是通过管理控制台远程登录（VNC方式）。

步骤7 执行以下命令，验证ecs-guangzhou -8访问ecs-shanghai -131。

ping 10.0.1.131

回显类似如下信息，表示网络通信正常。

```
[root@ecs-guangzhou-8 ~]# ping 10.0.1.131
PING 10.0.1.131 (10.0.1.131) 56(84) bytes of data.
64 bytes from 10.0.1.131: icmp_seq=1 ttl=64 time=34.3 ms
64 bytes from 10.0.1.131: icmp_seq=2 ttl=64 time=34.1 ms
64 bytes from 10.0.1.131: icmp_seq=3 ttl=64 time=34.1 ms
^C
--- 10.0.1.131 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 5ms
rtt min/avg/max/mdev = 34.082/34.162/34.314/0.238 ms
[root@ecs-guangzhou-8 ~]# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.1.8  netmask 255.255.255.0  broadcast 10.0.1.255
        inet6 fe80::f816:3eff:fe07:c73  prefixlen 64  scopeid 0x20<link>
        ether fa:16:3e:07:0c:73  txqueuelen 1000  (Ethernet)
        RX packets 355  bytes 58529 (57.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 441  bytes 52031 (50.8 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

步骤8 选择“网络 > 虚拟专用网络”，切换为“华东-上海一”或“华南-广州”区域，可以看到VPN连接的状态已经变为“正常”。

至此IDC和云上构建二层网络，实现主机粒度的不中断业务迁移上云的最佳实践配置完成。

----结束

1.3 主机粒度迁移，不中断业务上云（云专线+ESW）

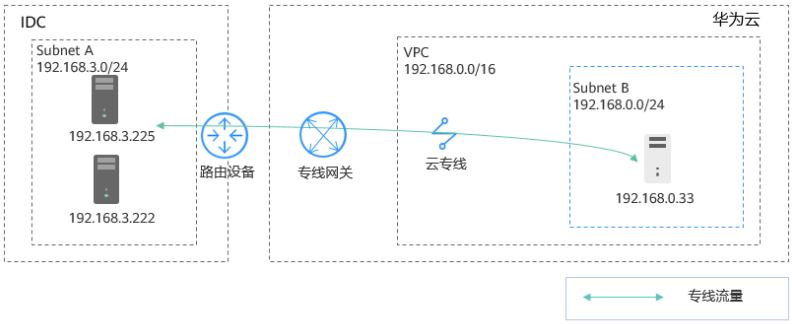
方案架构

用户云下IDC已有子网A，通过云专线连接到云上的子网B，如**图1-4**所示。用户希望将子网A内的部分业务迁移上云，迁移的具体要求如下：

- 扩展上云后的部分主机与同网段云下主机二层互通。
- 扩展上云的二层网段与IDC三层互通能力继续保持。

- IDC内改造的二层网络与云上三层互通能力继续保持。

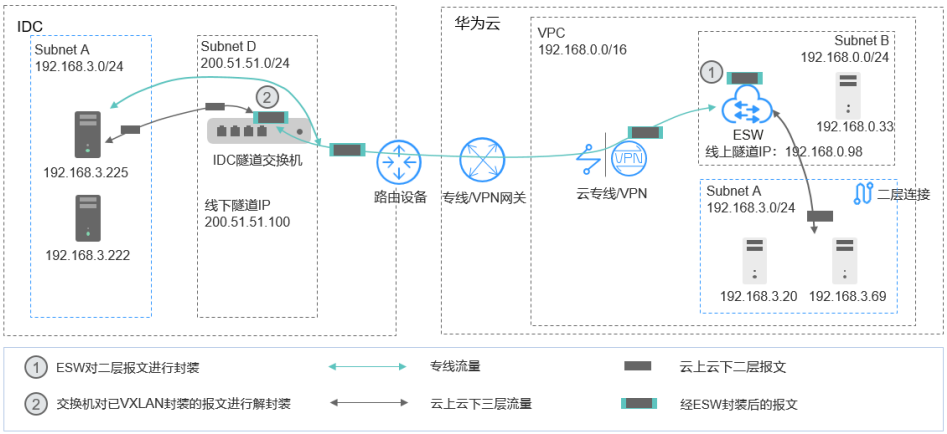
图 1-4 用户业务场景组网图



基于客户当前的业务场景，需要进行两个阶段的网络部署，详细说明如下：

1. 将子网Subnet A二层迁移上云，通过ESW实现云下和云上Subnet A之间二层网络互通，组网图如图1-5所示，迁移方案说明如下：
   a. 在云下IDC新增一个子网Subnet D，作为云下VXLAN交换机所需的隧道子网。
   b. 在云上VPC内新增一个子网Subnet A，用作云下Subnet A的上云目标子网。
   c. 将云上原有的Subnet B作为隧道子网，基于该子网创建企业交换机和二层连接，并关联云专线，即可以连通云上云下二层网络。

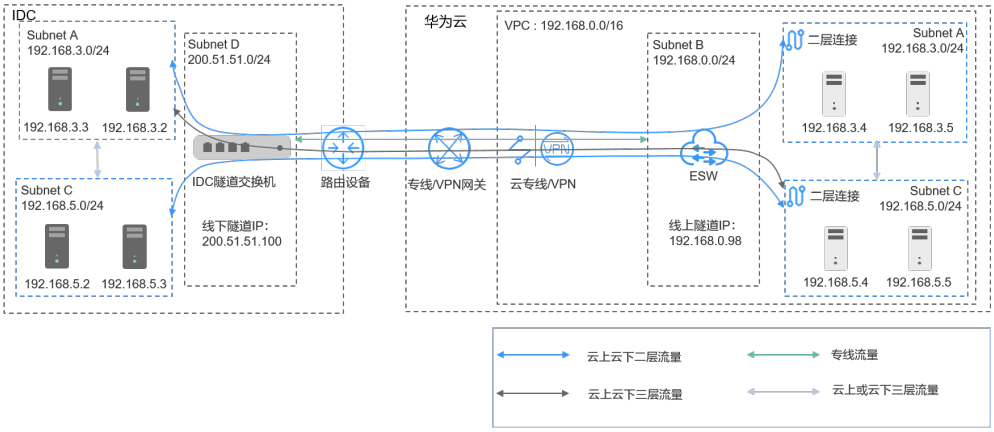
   图 1-5 云下和云上 Subnet A 之间二层网络互通



2. 在云上和云下新增子网Subnet C，通过ESW实现云下和云上Subnet C之间二层网络互通，并且基于云专线，实现云下IDC内Subnet A和云上Subnet C、云上Subnet A和云下Subnet C之间三层互通，组网图如图1-6所示，部署方案说明如下：
   a. 在云上和云下分别新增子网Subnet C。
   b. 在云上和云下基于已有的隧道子网，新建一个二层连接，连通云下和云上Subnet C之间二层网络。

      并且，同一个VPC内的子网网络三层互通，此时云下IDC内Subnet A和云上Subnet C、云上Subnet A和云下Subnet C之间三层互通。

图 1-6 云上和云下三层网络互通



资源和成本规划

表 1-2 资源和成本规划

区域	资源	资源说明	数量	每月费用（元）
华为云（本端）	虚拟私有云子网	子网名称：Subnet A 子网网段：192.168.3.0/24 第一个二层连接：二层连接A内的本端二层连接子网，此处为云上ECS所在子网	3	00.00
		子网名称：Subnet C 子网网段：192.168.5.0/24 第二个二层连接：二层连接C内的二层连接子网，此处为云上ECS所在子网		
		子网名称：Subnet B 子网网段：192.168.0.0/24 本端隧道子网，华为云上的隧道子网，此处为DC和ESW所在子网		
	弹性云服务器ECS	• Subnet A内地ECS，此处两台主机为IDC业务上云后扩展的两台主机。 – 私有IP地址：192.168.3.4 – 私有IP地址：192.168.3.5 • Subnet C内地ECS： – 私有IP地址：192.168.5.4 – 私有IP地址：192.168.5.5	4	1055.60

区域	资源	资源说明	数量	每月费用（元）
	企业交换机 ESW	• 隧道连接方式：云专线 • 隧道子网：Subnet B	1	65000.00
	二层连接	• 二层连接A，连接云上和云下Subnet A – 隧道IP：192.168.0.98 – 隧道号：5530 • 二层连接C，连接云上和云下Subnet C – 隧道IP：192.168.0.98 – 隧道号：5540 基于同一个企业交换机的两个二层连接，隧道IP地址保持一致，但是隧道号不能重复。	2	00.00
客户IDC（远端）	客户IDC内子网	子网名称：Subnet A 子网网段：192.168.3.0/24 第一个二层连接：二层连接A内的远端二层连接子网，客户IDC业务集群所在的子网	3	-
		子网名称：Subnet C 子网网段：192.168.5.0/24 第二个二层连接：二层连接C内的远端二层连接子网，客户IDC业务集群所在的子网		
		子网名称：Subnet D 子网网段：200.51.51.0/24 远端隧道子网：客户IDC内的隧道子网		
	二层连接对应的IDC内VXLAN隧道	• 二层连接A，连接云上和云下Subnet A – 隧道IP：200.51.51.100 – 隧道号：5530 • 二层连接C，连接云上和云下Subnet C – 隧道IP：200.51.51.100 – 隧道号：5540	2	-

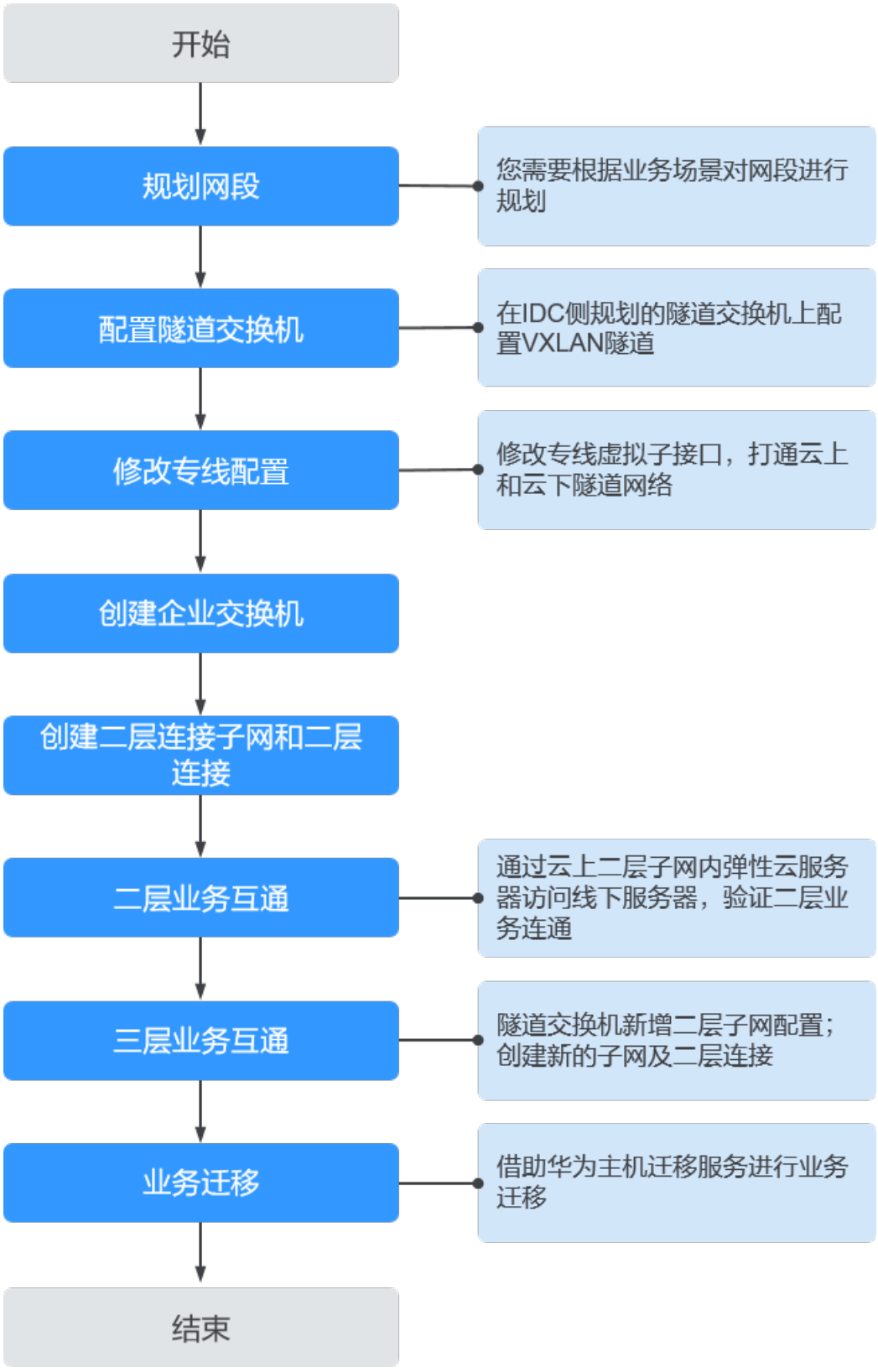
资源成本费用预估为66055.60元，该费用中，不包括迁移主机产生的费用，迁移费用详情请参见**计费说明**。

须知

本文提供的成本预估费用仅供参考，资源的实际费用以华为云管理控制台显示为准。

通过云专线和企业交换机迁移 IDC 子网上云流程

图 1-7 通过云专线和企业交换机迁移 IDC 子网上云流程



1. 根据业务场景需求，规划资源和网段。

   网络规划详情，请参见**表1-2**。

   说明

   - 上述网段仅供参考，具体以用户网段为准。
   - 隧道网段不建议范围很大，此隧道网段是用来规划一个隧道IP和华为云上的企业交换机建立VXLAN隧道。参考**图 云下和云上Subnet A之间二层网络互通**。

2. 在云下IDC侧的隧道交换机上配置VXLAN隧道。

   本文中子网Subnet D作为配置在交换机上的隧道网段，配置信息如下：

   - 源地址：为云下隧道IP（200.51.51.100）。
   - 目的地址：为云上隧道IP（192.168.0.98）。
   - 隧道号：5530

   配置线下交换机存在两种主要场景，不同的场景使用的配置方式不同，详情请参考**配置远端隧道网关**。

3. 修改专线的虚拟子接口配置，增加隧道子网Subnet D网段（200.51.51.0/24），以打通云上和云下隧道网络。

   具体操作请参考**修改虚拟接口**。

4. 请**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对接（VXLAN），如果不支持则需要云专线服务开通对接。

5. 创建企业交换机。

   创建方法请参见**购买企业交换机**，参数说明如下：

   - 隧道连接方式：选择云专线。
   - 关联网关：选择已有云专线网关。
   - 隧道子网：选择子网Subnet B（192.168.0.0/24）。
   - 隧道IP：配置为云上本端隧道IP（192.168.0.98）。

   单击“立即购买”及“提交”后，开始创建企业交换机。企业交换机的创建过程一般需要3~6分钟。

6. 创建第一个二层连接子网和二层连接，实现二层连接子网Subnet A云上和云下二层互通。

   注意

   创建二层连接子网后，由于两个子网网段相同，导致专线到云下和云上的路由冲突，因此专线原有三层业务中断。在创建完二层连接之后，三层业务会恢复。

   a. 在VPC中创建二层连接子网，对应**图1-5**中云上的子网Subnet A（192.168.3.0/24），子网网段与线下二层互通网段相同。

      创建子网请参考**为虚拟私有云创建新的子网**。

      说明

      - 子网 Subnet A、Subnet B、Subnet C、Subnet D网段不允许重叠。
      - Subnet D作为隧道子网，不需过大的网段范围，建议最大28位掩码。
      - 云上VPC的掩码规划，取决于用户创建企业交换机的个数，每个企业交换机会占用隧道子网的三个IP。

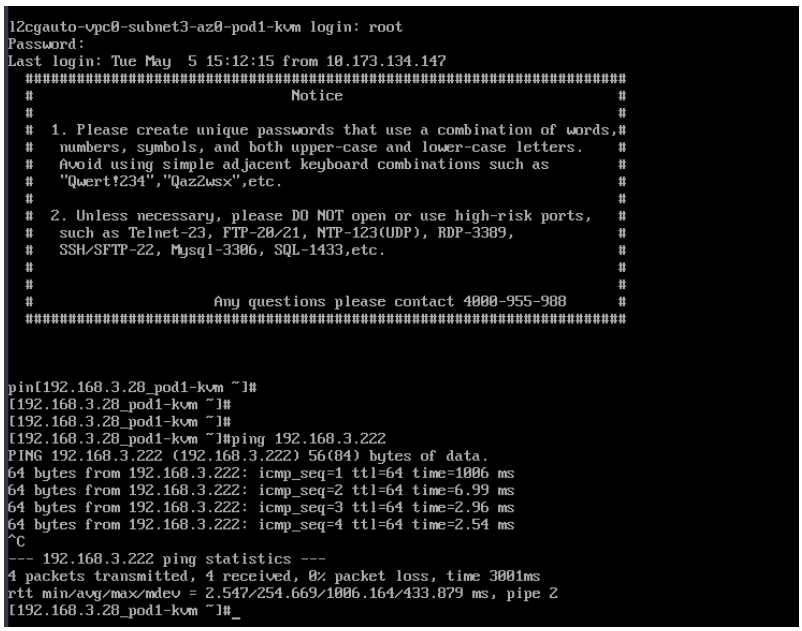
b. 创建云下和云上的二层连接子网Subnet A之间的二层连接A。
详情请参考**创建二层连接**。

- 二层连接子网：选择云上二层连接子网 Subnet A（192.168.3.0/24）。
- 远端接入信息：
  - 隧道号：5530
  - 对端隧道IP：200.51.51.100

c. 单击“创建”，等待连接状态为“已连接”，表示二层连接已创建成功。

7. 验证二层连接子网Subnet A之间的二层网络通信。
   a. 在云上二层连接子网 Subnet A内创建两台弹性云服务器。
   此处两台ECS的私有IP地址分别为192.168.3.20和192.168.3.69。
   b. 分别登录两台创建的弹性云服务器。
   弹性云服务器有多种登录方法，具体请参见**登录弹性云服务器**。
   本示例是通过管理控制台远程登录（VNC方式）。
   c. 执行以下命令，验证是否可正常访问云下主机。
   ping *云下二层连接子网Subnet A内的主机IP地址*
   命令示例：
   - **ping 192.168.3.255**
   - **ping 192.168.3.222**

   回显类似如下信息，表示二层云下和云上二层通信正常。



8. 创建新的二层连接子网和二层连接，实现云下和云上三层互通。
   a. 在VPC中创建二层连接子网，对应**图1-6**中云上的子网Subnet C（192.168.5.0/24），子网网段与线下二层互通网段相同。
   创建子网请参考**为虚拟私有云创建新的子网**。
   b. 创建云下和云上的二层连接子网Subnet C之间的二层连接C。
   详情请参考**创建二层连接**。

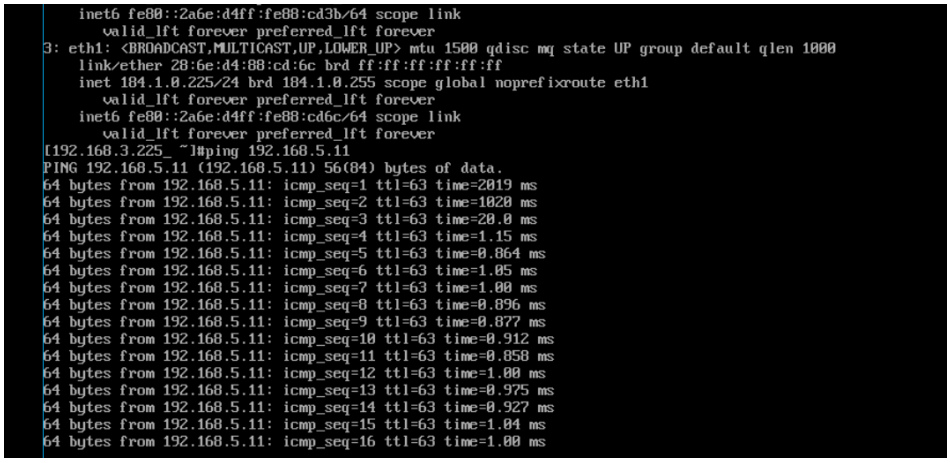
- 二层连接子网：选择云上二层连接子网Subnet C（192.168.5.0/24）。
- 远端接入信息：
  - 隧道号：5540
  - 对端隧道IP：200.51.51.100

c. 单击“创建”，等待连接状态为“已连接”，表示二层连接已创建成功。此时云下和云上可实现三层互通。

d. 参考**7**，验证二层连接子网Subnet C之间的二层网络通信。

e. 参考**7**，验证云下IDC内Subnet A和云上Subnet C、云上Subnet A和云下SubnetC之间三层网络通信。

回显类似如下信息，表示三层网络通信正常。



9. **业务迁移**

a. 二层业务互通后，将IDC内的部分主机迁移到云上。

迁移具体操作，请参见**主机迁移服务快速入门**。

b. 验证IDC和云上主机之间网络通信。

c. 网络通信验证成功后，将IDC内已迁移的主机进行关机。

d. 将云上的主机IP地址修改为云下IDC内的主机的IP地址。

修改IP地址具体操作，请参见**修改私有IP地址**。

e. 验证云下IDC内主机和云上主机网络通信。

常见问题

大二层互通的多个子网如果不属于同一个网段，需要云上企业交换机所在的VPC支持多CIDR能力，此时需借助工具创建跨CIDR的子网。请**提交工单**进行解决。