

企业路由器

# 最佳实践

文档版本 01  
发布日期 2025-01-26



版权所有 © 华为云计算技术有限公司 2025。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

<b>1 企业路由器最佳实践汇总</b>	<b>1</b>
<b>2 通过企业路由器和云连接中心网络实现跨区域 VPC 互通</b>	<b>7</b>
2.1 方案概述	7
2.2 组网和资源规划	8
2.3 通过中心网络构建跨区域 VPC 互通组网流程	15
2.4 通过中心网络构建跨区域 VPC 互通组网步骤	16
2.4.1 创建云服务资源	16
2.4.2 在企业路由器中配置 VPC 连接	17
2.4.3 在中心网络内为跨区域连接配置带宽	17
2.4.4 验证跨区域网络的通信情况	18
<b>3 通过企业路由器实现同区域 VPC 隔离</b>	<b>19</b>
3.1 方案概述	19
3.2 规划组网和资源	21
3.3 创建资源	25
3.3.1 创建企业路由器	25
3.3.2 创建 VPC 和 ECS	25
3.4 配置网络	26
3.4.1 在企业路由器中配置 VPC 连接	26
3.5 验证网络互通情况	26
<b>4 通过企业路由器和第三方防火墙实现多 VPC 互访流量清洗</b>	<b>28</b>
4.1 方案概述	28
4.2 规划组网和资源	30
4.3 创建资源	35
4.3.1 创建企业路由器	35
4.3.2 创建 VPC 和 ECS	35
4.4 配置网络	36
4.4.1 在企业路由器中配置 VPC 连接	36
4.4.2 在 ECS 中配置内核参数及路由	37
4.5 验证网络互通情况	39
<b>5 通过企业路由器和中转 VPC 构建组网</b>	<b>41</b>
5.1 方案概述	41
5.2 组网和资源规划	42

5.3 通过企业路由器和中转 VPC 构建组网流程.....	49
5.4 通过企业路由器和中转 VPC 构建组网实施步骤.....	50
<b>6 通过企业路由器和云专线构建混合云组网（全域接入网关 DGW）.....</b>	<b>55</b>
6.1 方案概述.....	55
6.2 组网和资源规划.....	56
6.3 企业路由器和全域接入网关混合云组网构建流程.....	61
6.4 企业路由器和全域接入网关混合云组网构建步骤.....	63
<b>7 通过企业路由器构建 DC 双链路负载混合云组网（全域接入网关 DGW）.....</b>	<b>66</b>
7.1 DC 双链路负载混合云组网方案概述.....	66
7.2 DC 双链路负载混合云组网和资源规划.....	67
7.3 DC 双链路负载混合云组网构建流程.....	73
7.4 DC 双链路负载混合云组网构建步骤.....	75
<b>8 通过企业路由器构建 DC 双链路主备混合云组网（全域接入网关 DGW）.....</b>	<b>79</b>
8.1 DC 双链路主备混合云组网方案概述.....	79
8.2 DC 双链路主备混合云组网和资源规划.....	80
8.3 DC 双链路主备混合云组网构建流程.....	87
8.4 DC 双链路主备混合云组网构建步骤.....	88
<b>9 通过企业路由器构建 DC/VPN 双链路主备混合云组网（全域接入网关 DGW）.....</b>	<b>93</b>
9.1 DC/VPN 双链路互备混合云组网方案概述.....	93
9.2 DC/VPN 双链路互备混合云组网和资源规划.....	94
9.3 DC/VPN 双链路互备混合云组网构建流程.....	100
9.4 DC/VPN 双链路互备混合云组网构建步骤.....	101
<b>10 通过企业路由器和云专线实现线下 IDC 和云上 VPC 互通（虚拟网关 VGW）.....</b>	<b>106</b>
10.1 方案概述.....	106
10.2 规划组网和资源.....	108
10.3 创建资源.....	112
10.3.1 创建企业路由器.....	112
10.3.2 创建 VPC 和 ECS.....	112
10.3.3 创建云专线的物理连接.....	113
10.4 配置网络.....	113
10.4.1 在企业路由器中配置 VPC 连接.....	113
10.4.2 在企业路由器中配置 VGW 连接.....	113
10.5 验证网络互通情况.....	115
<b>11 通过企业路由器构建 DC 双链路负载混合云组网（虚拟网关 VGW）.....</b>	<b>116</b>
11.1 方案概述.....	116
11.2 组网和资源规划.....	117
11.3 DC 双链路负载混合云组网构建流程.....	123
11.4 DC 双链路负载混合云组网构建步骤.....	124
<b>12 通过企业路由器构建 DC/VPN 双链路主备混合云组网（虚拟网关 VGW）.....</b>	<b>129</b>
12.1 方案概述.....	129

12.2 组网和资源规划.....	130
12.3 DC/VPN 双链路互备混合云组网构建流程.....	136
12.4 DC/VPN 双链路互备混合云组网构建步骤.....	137
<b>13 通过企业路由器和 NAT 网关实现多个 VPC 共享 SNAT 访问公网.....</b>	<b>142</b>
13.1 方案概述.....	142
13.2 规划组网和资源.....	143
13.3 创建资源.....	148
13.3.1 创建企业路由器.....	148
13.3.2 创建 VPC 和 ECS.....	148
13.3.3 创建 EIP 和公网 NAT 网关.....	149
13.4 配置网络.....	149
13.4.1 在企业路由器中配置 VPC 连接.....	149
13.4.2 在 NAT 网关中配置 SNAT 规则.....	150
13.5 验证网络互通情况.....	150
<b>14 将 VPC 对等连接组网迁移至企业路由器.....</b>	<b>152</b>
14.1 VPC 对等连接组网迁移方案概述.....	152
14.2 VPC 对等连接组网迁移资源规划.....	153
14.3 VPC 对等连接组网迁移流程.....	163
14.4 VPC 对等连接组网迁移实施步骤.....	164
<b>15 将 DC 直连 VPC 组网迁移至企业路由器（全域接入网关 DGW）.....</b>	<b>169</b>
15.1 DC 直连 VPC 组网迁移方案概述.....	169
15.2 DC 直连 VPC 组网迁移资源规划.....	170
15.3 DC 直连 VPC 组网迁移流程.....	178
15.4 DC 直连 VPC 组网迁移实施步骤.....	180
<b>16 将云连接实例直连 VPC 组网迁移至中心网络和企业路由器.....</b>	<b>185</b>
16.1 云连接实例直连 VPC 组网迁移方案概述.....	185
16.2 云连接实例直连 VPC 组网迁移资源规划.....	186
16.3 云连接实例直连 VPC 组网迁移流程.....	196
16.4 云连接实例直连 VPC 组网迁移实施步骤.....	197

# 1 企业路由器最佳实践汇总

企业路由器（Enterprise Router, ER）可以连接虚拟私有云（Virtual Private Cloud, VPC）或本地网络来构建中心辐射型组网，是云上大规格，高带宽，高性能的集中路由器。企业路由器使用边界网关协议（Border Gateway Protocol, BGP），支持路由学习、动态选路以及链路切换，极大的提升网络的可扩展性及运维效率，从而保证业务的连续性。

您可以通过企业路由器和华为云上的其他服务，灵活构建不同的组网，本文档提供典型组网的最佳实践供您参考。

表 1-1 场景说明

组网	场景示例	云服务	说明
云上跨区域组网	<a href="#">通过企业路由器和云连接中心网络实现跨区域VPC互通</a>	<ul style="list-style-type: none"><li>企业路由器ER</li><li>云连接中心网络</li><li>虚拟私有云VPC</li><li>弹性云服务器ECS</li></ul>	<p>为了实现业务的就近接入，XX企业在华为云区域A、区域B以及区域C内均部署了业务，承载业务的不同VPC之间需要网络互通。</p> <ol style="list-style-type: none"><li>在三个区域中，分别创建三个企业路由器ER，包括区域A的ER-A、区域B的ER-B以及区域C的ER-C。</li><li>创建云连接中心网络，并在云连接中心网络中加入ER-A、ER-B以及ER-C，连通不同区域的企业路由器。</li><li>在区域A内，将VPC-A01和VPC-A02接入ER内，实现同区域内VPC互通。在区域B和区域C进行同样的操作。最终，通过中心网络和企业路由器，实现不同区域的VPC网络互通。</li></ol>

组网	场景示例	云服务	说明
云上同区域组网	通过企业路由器实现同区域VPC隔离	<ul style="list-style-type: none"> <li>企业路由器ER</li> <li>虚拟私有云VPC</li> <li>弹性云服务器ECS</li> </ul>	<p>XX企业在华为云区域A内部署了4个虚拟私有云VPC，业务A、业务B、业务C分别部署在VPC1、VPC2、VPC3，公共业务部署在VPC4中，网络要求如下：</p> <ol style="list-style-type: none"> <li>业务A、业务B以及业务C所在的3个VPC需要隔离，不互通。</li> <li>业务A、业务B以及业务C都需要和公共业务所在的VPC4互通。</li> </ol>
云上同区域组网	通过企业路由器和第三方防火墙实现多VPC互访流量清洗	<ul style="list-style-type: none"> <li>企业路由器ER</li> <li>虚拟私有云VPC</li> <li>弹性云服务器ECS</li> </ul>	<p>XX企业在华为云区域A内部署了3个虚拟私有云VPC，其中业务A、业务B分别部署在VPC1、VPC2，VPC3部署有第三方防火墙软件。出于安全考虑，要求业务A和业务B互相访问的流量必须通过VPC3中防火墙软件的过滤清洗。</p>
混合云组网	通过企业路由器和中转VPC构建组网	<ul style="list-style-type: none"> <li>企业路由器ER</li> <li>云专线DC（虚拟网关VGW）</li> <li>虚拟专用网络VPN</li> <li>虚拟私有云VPC</li> <li>弹性云服务器ECS</li> </ul>	<p>您可以通过企业路由器构建中心辐射型组网，简化网络架构。当前为您提供两种典型组网方案，方案一是将业务VPC直接接入企业路由器，方案二是使用中转VPC，结合VPC对等连接和企业路由器共同构建组网。相比方案一，方案二可以降低成本，并且免去一些限制。</p>
混合云组网	通过企业路由器和云专线构建混合云组网（全域接入网关DGW）	<ul style="list-style-type: none"> <li>企业路由器ER</li> <li>云专线DC（全域接入网关DGW）</li> <li>虚拟私有云VPC</li> <li>弹性云服务器ECS</li> </ul>	<p>XX企业在华为云区域A内部署了2个虚拟私有云VPC，这2个VPC需要互相访问，并且通过DC全域接入网关和线下IDC网络互通。</p>

组网	场景示例	云服务	说明
混合云组网	<b>通过企业路由器构建DC双链路负载均衡混合云组网（全域接入网关DGW）</b>	<ul style="list-style-type: none"> <li>企业路由器ER</li> <li>云专线DC（全域接入网关DGW）</li> <li>虚拟私有云VPC</li> <li>弹性云服务器ECS</li> </ul>	<p>云专线（Direct Connect, DC）用于搭建线下IDC和云上虚拟私有云（Virtual Private Cloud, VPC）之间高速、低时延、稳定安全的专属连接通道，您可以通过企业路由器和云专线的全域接入网关，构建满足企业通信的大规模混合云组网。</p> <p>为了提升混合云组网的网络性能以及可靠性，XX企业同时部署了两条专线DC链路，均可以连通云上VPC和线下IDC的网络。两条DC链路形成负载均衡，当两条DC链路网络均正常，同时工作可提升网络传输能力。当其中一条DC链路故障时，另外一条DC链路可确保整个混合云组网的正常运行，避免了单点故障带来的业务中断。</p> <ul style="list-style-type: none"> <li>将VPC1、VPC2以及DC接入企业路由器中，VPC1和VPC2网络互通，并且均可以通过两条DC和线下IDC通信。</li> <li>当其中一条DC链路故障时，VPC1和VPC2可以通过另外一条DC链路和线下IDC通信。</li> </ul>
混合云组网	<b>通过企业路由器构建DC双链路主备混合云组网（全域接入网关DGW）</b>	<ul style="list-style-type: none"> <li>企业路由器ER</li> <li>云专线DC（全域接入网关DGW）</li> <li>虚拟私有云VPC</li> <li>弹性云服务器ECS</li> </ul>	<p>云专线（Direct Connect, DC）用于搭建线下IDC和云上虚拟私有云（Virtual Private Cloud, VPC）之间高速、低时延、稳定安全的专属连接通道，您可以通过企业路由器和云专线的全域接入网关，构建满足企业通信的大规模混合云组网。</p> <p>为了提升混合云组网的网络可靠性，并且控制成本费用，XX企业同时部署了两条DC链路，均可以连通云上VPC和线下IDC的网络。两条DC链路形成主备，当主链路故障后，可自动切换至备链路，降低了单链路故障导致的业务中断风险。</p>

组网	场景示例	云服务	说明
混合云组网	通过企业路由器构建DC/VPN双链路主备混合云组网（全域接入网关DGW）	<ul style="list-style-type: none"> <li>企业路由器ER</li> <li>云专线DC（全域接入网关DGW）</li> <li>虚拟专用网络VPN</li> <li>虚拟私有云VPC</li> <li>弹性云服务器ECS</li> </ul>	<p>云专线（Direct Connect, DC）用于搭建线下IDC和云上虚拟私有云（Virtual Private Cloud, VPC）之间高速、低时延、稳定安全的专属连接通道，您可以通过企业路由器和云专线的全域接入网关，构建满足企业通信的大规模混合云组网。</p> <p>虚拟专用网络（Virtual Private Network, VPN）用于在线下IDC和华为云上VPC之间建立一条安全加密的公网通信隧道。相比通过DC构建混合云，使用VPN更加快速，成本更低。</p> <p>为了提升混合云组网的可靠性，XX企业同时部署了DC和VPN两条网络链路，均可以连通云上VPC和线下IDC的网络。DC和VPN两条网络链路互为主备，主链路为DC，备链路为VPN，当DC链路故障时，可自动切换到VPN链路，降低网络中断对业务造成的影响。</p> <ul style="list-style-type: none"> <li>将VPC1、VPC2以及DC接入企业路由器中，VPC1和VPC2网络互通，并且均可以通过DC和线下IDC通信。</li> <li>将VPN接入企业路由器中，当主链路DC故障时，VPC1和VPC2可以通过备链路VPN和线下IDC通信。</li> </ul>
混合云组网	通过企业路由器和云专线实现线下IDC和云上VPC互通（虚拟网关VGW）	<ul style="list-style-type: none"> <li>企业路由器ER</li> <li>云专线DC（虚拟网关VGW）</li> <li>虚拟私有云VPC</li> <li>弹性云服务器ECS</li> </ul>	<p>XX企业在华为云区域A内部署了2个虚拟私有云VPC，这2个VPC需要互相访问，并且共享同一条云专线DC访问客户线下的IDC。</p> <p>在区域A内创建一个企业路由器ER，将VPC和DC的虚拟网关接入ER内，ER可以在接入的VPC和虚拟网关之间转发流量，实现2个VPC共享DC。</p>

组网	场景示例	云服务	说明
混合云组网	通过企业路由器构建DC双链路负载混合云组网（虚拟网关VGW）	<ul style="list-style-type: none"> <li>企业路由器ER</li> <li>云专线DC（虚拟网关VGW）</li> <li>虚拟私有云VPC</li> <li>弹性云服务器ECS</li> </ul>	<p>为了提升混合云组网的网络性能以及可靠性，XX企业同时部署了两条专线DC链路，均可以连通云上VPC和线下IDC的网络。两条DC链路形成负载均衡，当两条DC链路网络均正常，同时工作可提升网络传输能力。当其中一条DC链路故障时，另外一条DC链路可确保整个混合云组网的正常运行，避免了单点故障带来的业务中断。</p> <ul style="list-style-type: none"> <li>将VPC1、VPC2以及DC接入企业路由器中，VPC1和VPC2网络互通，并且均可以通过两条DC和线下IDC通信。</li> <li>当其中一条DC链路故障时，VPC1和VPC2可以通过另外一条DC链路和线下IDC通信。</li> </ul>
混合云组网	通过企业路由器构建DC/VPN双链路主备混合云组网（虚拟网关VGW）	<ul style="list-style-type: none"> <li>企业路由器ER</li> <li>云专线DC（虚拟网关VGW）</li> <li>虚拟专用网络VPN</li> <li>虚拟私有云VPC</li> <li>弹性云服务器ECS</li> </ul>	<p>为了提升混合云组网的可靠性，XX企业同时部署了DC和VPN两条网络链路，均可以连通云上VPC和线下IDC的网络。DC和VPN两条网络链路互为主备，主链路为DC，备链路为VPN，当DC链路故障时，可自动切换到VPN链路，降低网络中断对业务造成的影响。</p> <ul style="list-style-type: none"> <li>将VPC1、VPC2以及DC接入企业路由器中，VPC1和VPC2网络互通，并且均可以通过DC和线下IDC通信。</li> <li>将VPN接入企业路由器中，当主链路DC故障时，VPC1和VPC2可以通过备链路VPN和线下IDC通信。</li> </ul>
云内网络访问公网	通过企业路由器和NAT网关实现同区域VPC共享SNAT访问公网	<ul style="list-style-type: none"> <li>企业路由器ER</li> <li>NAT网关</li> <li>弹性公网IP</li> <li>虚拟私有云VPC</li> <li>弹性云服务器ECS</li> </ul>	<p>XX企业在华为云区域A内部署了4个虚拟私有云VPC，VPC1、VPC2、VPC3需要互相访问，并且可以共享VPC4的SNAT访问公网。</p>
组网迁移	将VPC对等连接组网迁移至企业路由器	<ul style="list-style-type: none"> <li>企业路由器ER</li> <li>虚拟私有云VPC</li> <li>弹性云服务器ECS</li> </ul>	<p>VPC-A、VPC-B、VPC-C位于区域A，通过对等连接连通三个VPC的网络，为了提升网络可扩展性、降低运维成本，现在需要将这三个VPC的网络迁移至企业路由器上。</p>

组网	场景示例	云服务	说明
组网迁移	将DC直连VPC组网迁移至企业路由器（全域接入网关DGW）	<ul style="list-style-type: none"> <li>企业路由器ER</li> <li>云专线DC（全域接入网关DGW）</li> <li>虚拟私有云VPC</li> <li>弹性云服务器ECS</li> </ul>	VPC-X和云专线DC的虚拟网关VGW-A、虚拟接口VIF-A01、虚拟接口VIF-A02位于区域A，通过DC连通VPC-X和线下IDC之间的网络，为了提升混合云组网可靠性并降低维护成本，现在需要将VPC-X和云专线网络迁移至企业路由器上，通过全域接入网关连通线下IDC网络。
组网迁移	将云连接实例直连VPC组网迁移至中心网络和企业路由器	<ul style="list-style-type: none"> <li>企业路由器ER</li> <li>云连接（云连接实例）</li> <li>云连接（中心网络）</li> <li>虚拟私有云VPC</li> <li>弹性云服务器ECS</li> </ul>	当前组网中，通过云连接实例连通区域A、区域B以及区域C内的VPC网络，为了提升组网的可扩展性，并降低维护难度，现在需要将VPC迁移到企业路由器中，并通过中心网络连通不同区域的企业路由器。

### 须知

如果您需要连通云上VPC和线下IDC构建混合云组网，则推荐您使用企业路由器和云专线的全域接入网关DGW。

从2024年5月份开始，通过企业路由器和云专线的虚拟网关VGW构建混合云组网的功能不再支持新增组网，只针对存量组网进行维护。

# 2 通过企业路由器和云连接中心网络实现跨区域 VPC 互通

## 2.1 方案概述

### 应用场景

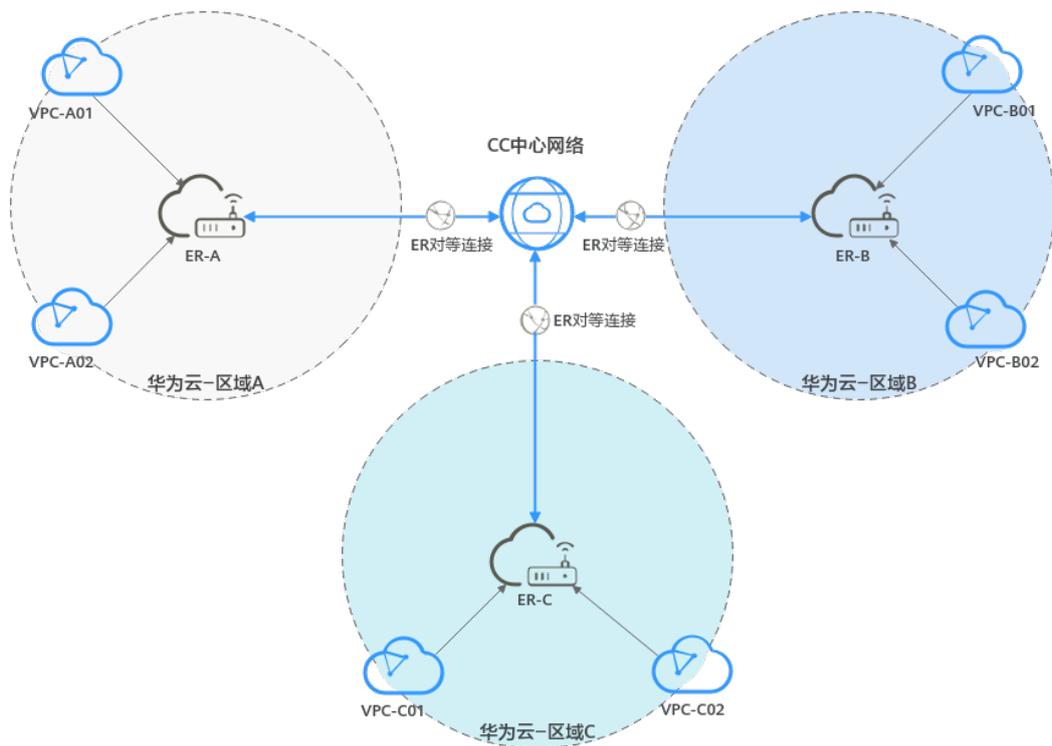
云连接中心网络基于华为云骨干网络面向客户提供全球网络编排能力，帮助用户便捷、安全的创建和管理云上、云下的全球网络资源。您可以将两个及以上不同区域的企业路由器接入中心网络，构成ER对等连接，实现云上跨区域网络互通。

### 方案架构

为了实现业务的就近接入，XX企业在华为云区域A、区域B以及区域C内均部署了业务，承载业务的不同VPC之间需要网络互通。

1. 在三个区域中，分别创建三个企业路由器ER，包括区域A的ER-A、区域B的ER-B以及区域C的ER-C。
2. 创建云连接中心网络，并在云连接中心网络中加入ER-A、ER-B以及ER-C，连通不同区域的企业路由器。
3. 在区域A内，将VPC-A01和VPC-A02接入ER内，实现同区域内VPC互通。在区域B和区域C进行同样的操作。最终，通过中心网络和企业路由器，实现不同区域的VPC网络互通。

图 2-1 跨区域 VPC 互通组网



### 说明

您可以使用[企业路由器的共享功能](#)，将不同账号下的虚拟私有云添加至同一个企业路由器中构建组网。

## 约束与限制

不同VPC的子网网段不能重复，否则可能出现无法通信的情况。

## 2.2 组网和资源规划

通过企业路由器和云连接中心网络构建跨区域VPC互通组网，您需要规划组网和资源：

- **网络规划说明：**规划云连接中心网络、VPC及其子网的网段、VPC路由表和ER路由表信息等。
- **资源规划说明：**规划云上资源的数量、名称以及主要参数等信息，云上资源包括VPC、CC中心网络、ECS以及ER等。

### 网络规划说明

跨区域VPC互通组网规划如[图2-2](#)所示，将3个不同区域的ER接入云连接中心网络中，组网规划说明如[表2-2](#)所示。

### 说明

本示例中，每个区域内创建一个VPC接入企业路由器ER内，仅供您参考配置，实际网络规划请以您的业务需求为准。

图 2-2 跨区域 VPC 互通组网规划

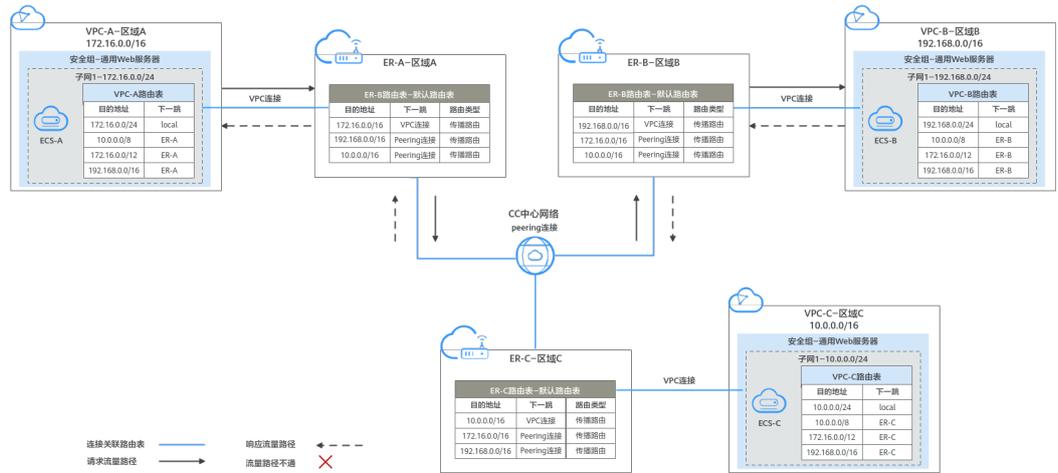


表 2-1 网络流量路径说明

路径	说明
请求路径: VPC-A → VPC-B	<ol style="list-style-type: none"> <li>在VPC-A路由表中，通过下一跳为ER-A的路由将流量转送到ER-A。</li> <li>在ER-A路由表中，通过云连接中心网络和下一跳为Peering连接，目的地址为192.168.0.0/16的路由将流量转送到ER-B。</li> <li>在ER-B路由表中，通过下一跳为VPC连接的路由将流量送达VPC-B。</li> </ol>
响应路径: VPC-B → VPC-A	<ol style="list-style-type: none"> <li>在VPC-B路由表中，通过下一跳为ER-B的路由将流量转送到ER-B。</li> <li>在ER-B路由表中，通过云连接中心网络和下一跳为Peering连接，目的地址为172.16.0.0/16的路由将流量转送到ER-A。</li> <li>在ER-A路由表中，通过下一跳为VPC连接的路由将流量送达VPC-A。</li> </ol>

表 2-2 跨区域 VPC 互通组网规划说明

资源	说明
VPC	<ul style="list-style-type: none"> <li>VPC网段（CIDR）不能重叠。 本示例中，ER路由表使用的是“虚拟私有云（VPC）”连接的传播路由，由ER自动学习VPC网段作为目的地址，不支持修改，因此重叠的VPC网段会导致路由冲突。</li> <li>如果您已有的VPC存在网段重叠，则不建议您使用传播路由，请在ER路由表中手动添加静态路由，目的地址可以为VPC子网网段或者范围更小的网段。</li> <li>VPC有一个默认路由表。</li> <li>VPC默认路由表中的路由说明如下： <ul style="list-style-type: none"> <li>local：表示VPC本地IPv4的默认路由条目，用于VPC内子网通信，系统自动配置。</li> <li>ER：表示将VPC子网流量路由至ER，本示例中系统自动在VPC路由表中增加三个VPC的网段10.0.0.0/8、172.16.0.0/12、192.168.0.0/16，路由信息如表2-3所示。</li> </ul> </li> </ul>
中心网络	<ul style="list-style-type: none"> <li>将不同区域的ER添加在云连接中心网络中。</li> <li>购买全域互联带宽，配置连通不同区域的全域互联带宽值。</li> </ul>
ER	<p>区域A、区域B和区域C下的ER组网配置相同，路由信息如表2-4所示。</p> <p>当使用中心网络连通ER时，必须开启ER的“默认路由表关联”和“默认路由表传播”功能，那么在ER中添加连接时，系统会自动添加ER指向连接的路由，无需手动添加。</p>
ECS	<p>ECS分别位于不同的VPC内，VPC中的ECS如果位于不同的安全组，需要在安全组中添加规则放通其他安全组的网络。</p>

表 2-3 VPC 路由表

目的地址	下一跳	路由类型
10.0.0.0/8	企业路由器	静态路由：自定义
172.16.0.0/12	企业路由器	静态路由：自定义
192.168.0.0/16	企业路由器	静态路由：自定义

### 📖 说明

- 如果您在创建连接时开启“配置连接侧路由”选项，则不用手动在VPC路由表中配置静态路由，系统会在VPC的所有路由表中自动添加指向ER的路由，目的地址固定为10.0.0.0/8，172.16.0.0/12，192.168.0.0/16。
- 如果VPC路由表中的路由与这三个固定网段冲突，则会添加失败。此时建议您不要开启“配置连接侧路由”选项，并在连接创建完成后，手动添加路由。
- 不建议在VPC路由表中将ER的路由配置为默认路由网段0.0.0.0/0，如果VPC内的ECS绑定了EIP，会在ECS内增加默认网段的策略路由，并且优先级高于ER路由，此时会导致流量转发至EIP，无法抵达ER。

表 2-4 ER 路由表

企业路由器	目的地址	下一跳	路由类型
区域A: ER-A	VPC-A网段: 172.16.0.0/16	VPC连接: er-attach-VPC-A	传播路由
	VPC-B网段: 192.168.0.0/16	Peering连接: region-A-region-B	传播路由
	VPC-C网段: 10.0.0.0/16	Peering连接: region-A-region-C	传播路由
区域B: ER-B	VPC-B网段: 192.168.0.0/16	VPC-B连接: er-attach-VPC-B	传播路由
	VPC-A网段: 172.16.0.0/16	Peering连接: region-B-region-A	传播路由
	VPC-C网段: 10.0.0.0/16	Peering连接: region-B-region-C	传播路由
区域C: ER-C	VPC-C网段: 10.0.0.0/16	VPC-C连接: er-attach-VPC-C	传播路由
	VPC-A网段: 172.16.0.0/16	Peering连接: region-C-region-A	传播路由
	VPC-B网段: 192.168.0.0/16	Peering连接: region-C-region-B	传播路由

## 资源规划说明

企业路由器ER、虚拟私有云VPC、弹性云服务器ECS只要位于同一个区域内即可，可用区可以任意选择，不用保持一致。

### 📖 说明

以下资源规划详情仅为示例，实际情况请根据您的业务需求规划。

表 2-5 跨区域 VPC 互通组网资源规划总体说明

资源类型	资源数量	说明
VPC	3	<p>业务VPC，实际运行客户业务的VPC，需要接入ER，本示例中需要在3个不同区域内各创建一个VPC。</p> <ul style="list-style-type: none"><li>● VPC名称：请根据实际情况填写，本示例如下。<ul style="list-style-type: none"><li>- 区域A：VPC-A</li><li>- 区域B：VPC-B</li><li>- 区域C：VPC-C</li></ul></li><li>● IPv4网段：建议不同的VPC网段不能重复，请根据实际情况填写，本示例如下。<ul style="list-style-type: none"><li>- VPC-A：172.16.0.0/16</li><li>- VPC-B：192.168.0.0/16</li><li>- VPC-C：10.0.0.0/16</li></ul></li><li>● 子网名称和IPv4网段：需要互通的VPC子网网段不能重复，否则无法通信。请根据实际情况规划，本示例如下。<ul style="list-style-type: none"><li>- subnet-A01：172.16.0.0/24</li><li>- subnet-B01：192.168.0.0/24</li><li>- subnet-C01：10.0.0.0/24</li></ul></li></ul>

资源类型	资源数量	说明
ER	3	<p>本示例中需要在3个不同区域内各创建一个ER，并接入“对等连接（Peering）”连接和“虚拟私有云（VPC）”连接。</p> <ul style="list-style-type: none"> <li>名称：请根据实际情况填写， <ul style="list-style-type: none"> <li>区域A：ER-A</li> <li>区域B：ER-B</li> <li>区域C：ER-C</li> </ul> </li> <li>ASN：此处建议不同区域企业路由器的ASN号不同，本示例如下。 <ul style="list-style-type: none"> <li>ER-A：64512</li> <li>ER-B：64513</li> <li>ER-C：64514</li> </ul> </li> <li>默认路由表关联：开启</li> <li>默认路由表传播：开启</li> <li>自动接受共享连接：请根据实际情况选择，本示例选择“开启”。</li> <li>连接：本示例需要在不同区域的企业路由器中分别添加3个连接，本示例如下。 <p><b>ER-A:</b></p> <ul style="list-style-type: none"> <li>VPC连接：连通VPC-A和ER-A之间的网络，名称为er-attach-VPC-A</li> <li>Peering连接：连通ER-A和ER-B之间的网络，名称为region-A-region-B</li> <li>Peering连接：连通ER-A和ER-C之间的网络，名称为region-A-region-C</li> </ul> <p><b>ER-B:</b></p> <ul style="list-style-type: none"> <li>VPC连接：连通VPC-B和ER-B之间的网络，名称为er-attach-VPC-B</li> <li>Peering连接：连通ER-B和ER-A之间的网络，名称为region-B-region-A</li> <li>Peering连接：连通ER-B和ER-C之间的网络，名称为region-B-region-C</li> </ul> <p><b>ER-C:</b></p> <ul style="list-style-type: none"> <li>VPC连接：连通VPC-C和ER-C之间的网络，名称为er-attach-VPC-C</li> <li>Peering连接：连通ER-C和ER-A之间的网络，名称为region-C-region-A</li> <li>Peering连接：连通ER-C和ER-B之间的网络，名称为region-C-region-B</li> </ul> </li> </ul> <p><b>须知</b> 当使用中心网络连通ER时，必须开启ER的“默认路由表关联”和“默认路由表传播”功能。</p>

资源类型	资源数量	说明
CC中心网络	1	<p>本示例中，需要创建一个中心网络，并在中心网络中加入需要网络互通的ER。</p> <ul style="list-style-type: none"> <li>● 名称：请根据实际情况填写，本示例为gcn-A-B-C。</li> <li>● 策略： <ul style="list-style-type: none"> <li>- 区域：区域A；企业路由器：ER-A</li> <li>- 区域：区域B；企业路由器：ER-B</li> <li>- 区域：区域C；企业路由器：ER-C</li> </ul> </li> <li>● 跨地域连接带宽： <ul style="list-style-type: none"> <li>- 区域A-区域B：10 Mbit/s</li> <li>- 区域A-区域C：5 Mbit/s</li> <li>- 区域B-区域C：20 Mbit/s</li> </ul> </li> </ul>
全域互联带宽	3	<p>本示例中，需要创建3个全域互联带宽，用来连通不同区域的云内骨干网络。</p> <ul style="list-style-type: none"> <li>● 名称：请根据实际情况填写，本示例如下。 <ul style="list-style-type: none"> <li>- 连通区域A和区域B：bandwidth-A-B。</li> <li>- 连通区域A和区域C：bandwidth-A-C。</li> <li>- 连通区域B和区域C：bandwidth-B-C。</li> </ul> </li> <li>● 带宽类型：请根据组网实际情况选择，本示例中区域A、区域B以及区域C位于同一个大区，因此选择“大区带宽”。</li> <li>● 互联大区：请根据组网实际情况选择，本示例中区域A、区域B以及区域C均位于中国大陆，因此选择“中国大陆”。</li> <li>● 指定互通区域：请根据组网实际情况选择。</li> </ul>

资源类型	资源数量	说明
ECS	3	<p>本示例中需要在3个不同区域内各创建一个ECS，主要用来验证网络互通情况。</p> <ul style="list-style-type: none"><li>名称：根据实际情况填写，本示例如下。<ul style="list-style-type: none"><li>区域A：ECS-A</li><li>区域B：ECS-B</li><li>区域C：ECS-C</li></ul></li><li>镜像：请根据实际情况选择，本示例为公共镜像（CentOS 8.2 64bit）。</li><li>网络：请根据实际情况选择虚拟私有云和子网，本示例如下。<ul style="list-style-type: none"><li>ECS-A：VPC-A、subnet-A01</li><li>ECS-B：VPC-B、subnet-B01</li><li>ECS-C：VPC-C、subnet-C01</li></ul></li><li>安全组：请根据实际情况选择，本示例安全组模板选择“通用Web服务器”，名称为sg-demo。</li><li>私有IP地址：<ul style="list-style-type: none"><li>ECS-A：172.16.0.91</li><li>ECS-B：192.168.0.5</li><li>ECS-C：10.0.0.29</li></ul></li></ul>

## 2.3 通过中心网络构建跨区域 VPC 互通组网流程

本章节介绍通过企业路由器和云连接中心网络构建跨区域VPC互通组网，流程如表2-6所示。

表 2-6 构建跨区域 VPC 组网流程说明

序号	步骤	说明
1	创建云服务资源	<ol style="list-style-type: none"><li>创建3个企业路由器，每个区域内需要1个企业路由器。</li><li>创建业务VPC和其子网，本示例中在每个区域下各创建1个VPC和1子网。</li><li>在每个业务VPC子网内创建ECS，本示例中共创建3个ECS。</li><li>创建1个云连接中心网络，创建中心网络时需要配置策略，此时需要将不同区域的企业路由器添加到策略中。</li><li>创建全域互联带宽，本示例中创建3个全域互联带宽连通不同区域网络。</li></ol>

序号	步骤	说明
2	<a href="#">在企业路由器中配置VPC连接</a>	针对每个区域的企业路由器，分别在企业路由器中添加“虚拟私有云（VPC）”连接，即将VPC接入企业路由器中。
3	<a href="#">在中心网络内为跨区域网络链路配置带宽</a>	为中心网络内的跨区域连接配置带宽，根据业务的实际需要配置，确保带宽满足业务需求。
4	<a href="#">验证跨区域网络的通信情况</a>	分别登录不同区域的ECS，执行ping命令，验证网络互通情况。

## 2.4 通过中心网络构建跨区域 VPC 互通组网步骤

### 2.4.1 创建云服务资源

本示例中，您需要创建企业路由器，虚拟私有云、云连接中心网络等资源，资源规划详情请参见[表2-5](#)。

**步骤1** 在3个区域内，各创建1个企业路由器。

创建企业路由器，具体方法请参见[创建企业路由器](#)。

#### 📖 说明

不同区域内的企业路由器，建议您使用不同的AS号。

**步骤2** 在3个区域内，各创建1个VPC。

创建VPC及子网，具体方法请参见[创建虚拟私有云和子网](#)。

**步骤3** 在3个区域内，各创建1个ECS。

创建ECS，具体方法请参见[自定义购买ECS](#)。

**步骤4** 创建云连接中心网络，并在策略中添加需要连通的企业路由器。

1. 创建1个云连接中心网络，并在策略中添加企业路由器。

创建中心网络，具体方法请参见[创建中心网络](#)。

2. 在企业路由器控制台，查看“对等连接（Peering）”连接的添加情况。

具体方法请参见[查看连接](#)。

“对等连接（Peering）”连接的状态“正常”，表示已成功接入企业路由器中。

由于本示例创建ER时，开启“默认路由表关联”和“默认路由表传播”，因此配置策略，即添加完“对等连接（Peering）”连接后，以下均为系统自动配置：

- 在ER的默认路由表中创建关联
- 在ER默认路由表中创建传播，并自动学习对方路由表中的路由信息。

**步骤5** 创建3个全域互联带宽，连通不同区域的网络链路。

创建全域互联带宽，具体方法请参见[购买全域互联带宽](#)。

----结束

## 2.4.2 在企业路由器中配置 VPC 连接

在企业路由器中配置“虚拟私有云（VPC）”连接，即将VPC接入企业路由器中，资源规划详情请参见[表2-5](#)。

**步骤1** 在区域A内，在企业路由器ER-A中添加“虚拟私有云（VPC）”连接。

1. 将VPC接入企业路由器中。

本示例添加“虚拟私有云（VPC）”连接时开启“配置连接侧路由”，免去手工在VPC路由表中配置路由。

添加“虚拟私有云（VPC）”连接，具体方法请参见[在企业路由器中添加VPC连接](#)。

由于本示例创建ER时，开启“默认路由表关联”和“默认路由表传播”，因此添加完“虚拟私有云（VPC）”连接后，以下均为系统自动配置：

- 在默认路由表中创建关联
- 在默认路由表中创建传播，并自动学习VPC网段路由信息。

2. （可选）在VPC路由表中配置ER的路由信息。

如果您添加“虚拟私有云（VPC）”连接时开启“配置连接侧路由”，则无需执行该操作，系统会自动在VPC路由表中添加路由，路由详情请参见[表2-3](#)。

配置路由信息，具体方法请参见[在VPC路由表中配置路由](#)。

**步骤2** 在区域B内，参考[步骤1](#)，在企业路由器ER-B中添加“虚拟私有云（VPC）”连接。

**步骤3** 在区域C内，参考[步骤1](#)，在企业路由器ER-C中添加“虚拟私有云（VPC）”连接。

----结束

## 2.4.3 在中心网络内为跨区域连接配置带宽

为中心网络内的跨区域连接配置带宽，根据业务的实际需要配置，确保带宽满足业务需求，跨地域连接带宽的详细规划请参见[表2-5](#)。

### 📖 说明

云连接服务默认您在各个区域之间分配了10kbps的域间带宽，用来支撑连通性测试。“对等连接（Peering）”连接添加完成后，您就可以验证网络连通性，具体方法请参见[验证跨区域网络的通信情况](#)。

为了业务正常使用，您需要继续执行以下操作购买全域互联带宽，并为跨区域连接配置带宽。

**步骤1** 为连通区域A和区域B的连接配置带宽。

基于购买的全域互联带宽为两个互通的区域配置带宽，具体方法请参见[配置跨地域连接带宽](#)。

**步骤2** 为连通区域A和区域C的连接配置带宽。

**步骤3** 为连通区域B和区域C的连接配置带宽。

----结束

## 2.4.4 验证跨区域网络的通信情况

**步骤1** 登录弹性云服务器。

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）。

**步骤2** 在弹性云服务器的远程登录窗口，执行以下命令，验证网络互通情况。

1. 执行以下命令，验证跨区域VPC网络互通情况。

**ping 弹性云服务器IP地址**

以登录ECS-A，验证VPC-A与VPC-B的网络互通情况为例：

**ping 192.168.0.5**

回显类似如下信息，表示VPC-A与VPC-B通信正常。

```
[root@ECS-A ~]# ping 192.168.0.5
PING 192.168.0.5 (192.168.0.5) 56(84) bytes of data.
64 bytes from 192.168.0.5: icmp_seq=1 ttl=62 time=30.6 ms
64 bytes from 192.168.0.5: icmp_seq=2 ttl=62 time=30.2 ms
64 bytes from 192.168.0.5: icmp_seq=3 ttl=62 time=30.1 ms
64 bytes from 192.168.0.5: icmp_seq=4 ttl=62 time=30.1 ms
...
--- 192.168.0.5 ping statistics ---
```

2. 执行以下命令，验证跨区域VPC网络互通情况。

**ping 弹性云服务器IP地址**

以登录ECS-A，验证VPC-A与VPC-C的网络互通情况为例：

**ping 10.0.0.29**

回显类似如下信息，表示VPC-A与VPC-C通信正常。

```
[root@ECS-A ~]# ping 10.0.0.29
PING 10.0.0.29 (10.0.0.29) 56(84) bytes of data.
64 bytes from 10.0.0.29: icmp_seq=1 ttl=62 time=27.4 ms
64 bytes from 10.0.0.29: icmp_seq=2 ttl=62 time=27.0 ms
64 bytes from 10.0.0.29: icmp_seq=3 ttl=62 time=26.10 ms
64 bytes from 10.0.0.29: icmp_seq=4 ttl=62 time=26.9 ms
...
--- 10.0.0.29 ping statistics ---
```

**步骤3** 重复执行**步骤1~步骤2**，验证其他VPC之间的网络互通情况。

----结束

# 3 通过企业路由器实现同区域 VPC 隔离

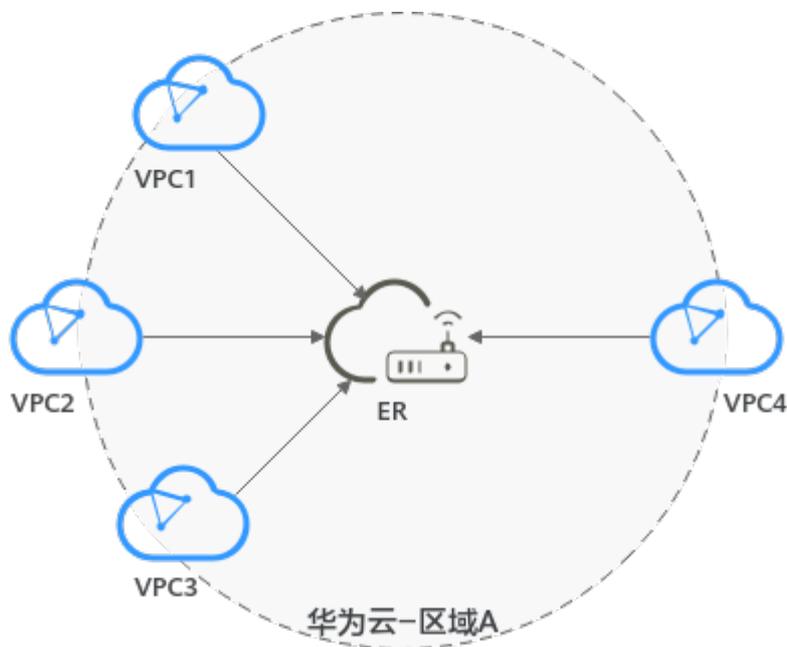
## 3.1 方案概述

### 背景信息

XX企业在华为云区域A内部署了4个虚拟私有云VPC，业务A、业务B、业务C分别部署在VPC1、VPC2、VPC3，公共业务部署在VPC4中，网络要求如下：

1. 业务A、业务B以及业务C所在的3个VPC需要隔离，不互通。
2. 业务A、业务B以及业务C都需要和公共业务所在的VPC4互通。

图 3-1 同区域 VPC 隔离



### 说明

您可以使用[企业路由器的共享功能](#)，将不同账号下的虚拟私有云添加至同一个企业路由器中构建组网。

## 操作流程

本文档介绍如何通过企业路由器构建同区域VPC隔离组网，流程如图3-2所示。

图 3-2 构建同区域 VPC 隔离组网流程图

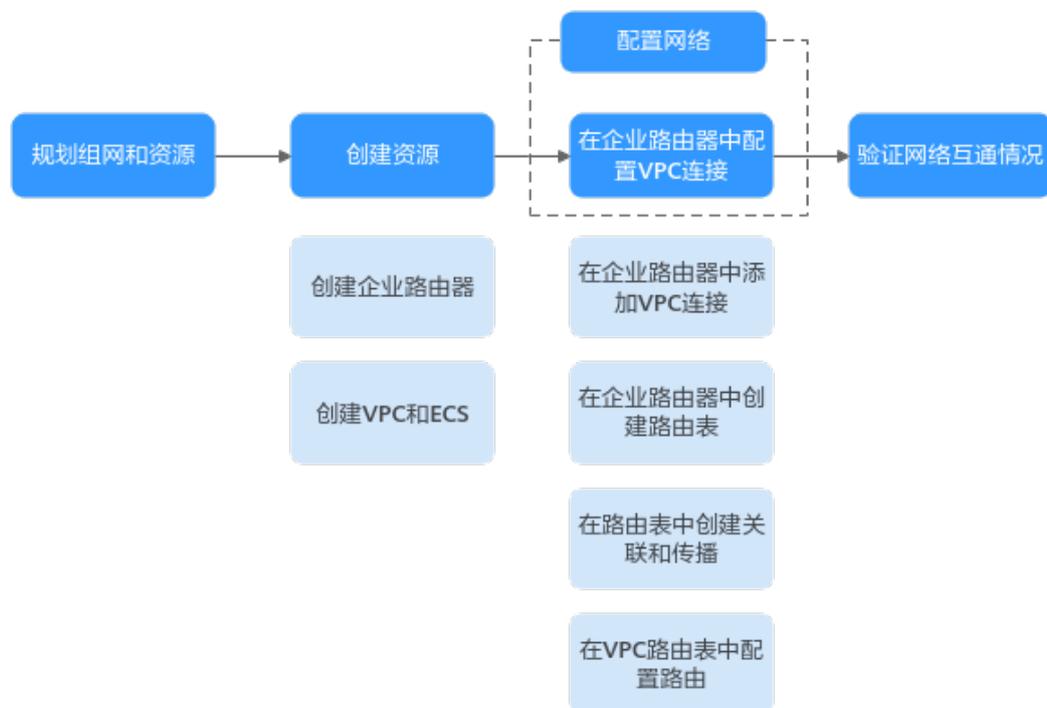


表 3-1 构建同区域 VPC 隔离组网流程说明

序号	路径	说明
1	规划组网和资源	规划组网和资源，包括资源数量及网段信息等。
2	创建资源	1. <b>创建企业路由器</b> ：创建1个企业路由器，构建一个同区域组网只需要1个企业路由器。 2. <b>创建VPC和ECS</b> ：创建4个虚拟私有云VPC和4个弹性云服务器ECS。
3	配置网络	1. <b>在企业路由器中配置VPC连接</b> ： <ol style="list-style-type: none"> <li>在企业路由器中添加“虚拟私有云（VPC）”连接：将4个VPC分别接入企业路由器中。</li> <li>在企业路由器中创建路由表；创建2个自定义路由表。</li> <li>在路由表中创建关联和传播：根据网络规划，在两个路由表中分别创建“虚拟私有云（VPC）”连接的关联和传播。</li> <li>在VPC路由表中配置路由：在VPC路由表中配置到企业路由器的路由信息。</li> </ol>

序号	路径	说明
4	验证网络互通情况	登录ECS，执行ping命令，验证网络互通情况。

### 3.2 规划组网和资源

通过企业路由器构建同区域VPC隔离组网，您需要规划组网和资源：

- **规划组网：**规划VPC及其子网的网段、VPC路由表和ER路由表信息。
- **规划资源：**规划云上资源的数量、名称以及主要参数等信息，云上资源包括VPC、ECS以及ER。

#### 规划组网

同区域VPC隔离组网规划如图3-3所示，将4个VPC接入ER中，组网规划说明如表3-3所示。

图 3-3 同区域 VPC 隔离组网规划

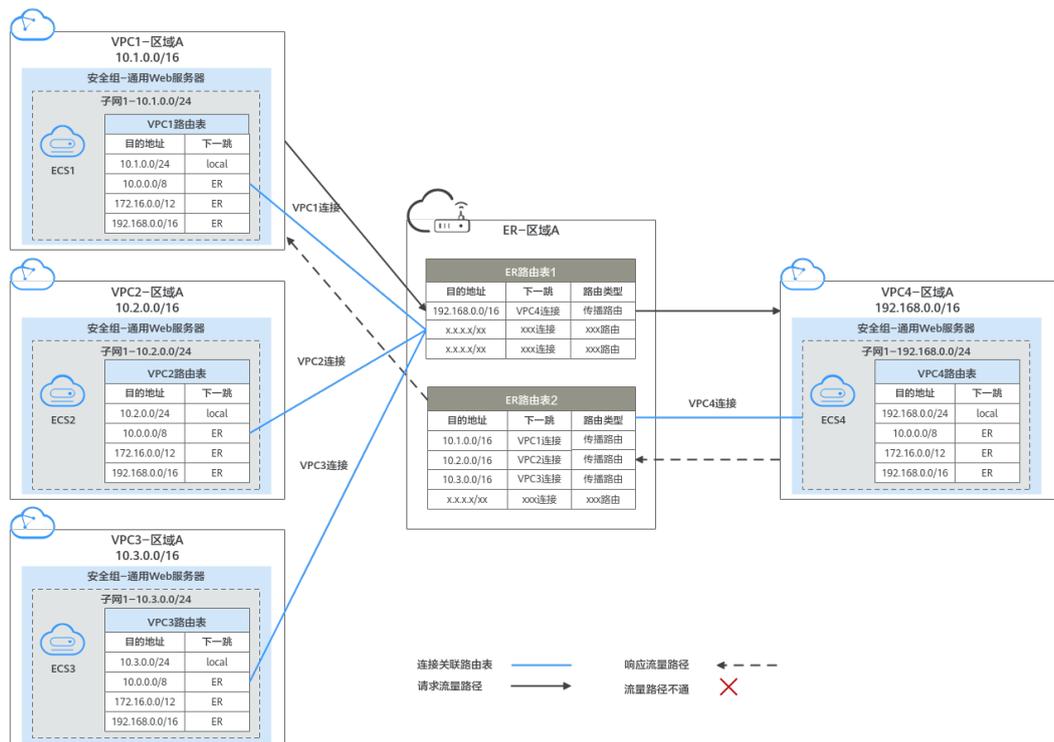


表 3-2 网络流量路径说明

路径	说明
请求路径： VPC1 → VPC4	<ol style="list-style-type: none"> <li>1. 在VPC1路由表中，通过下一跳为ER的路由将流量转送到ER。</li> <li>2. VPC1关联的是ER路由表1，在ER路由表1中，通过下一跳为VPC4连接的路由将流量送达VPC4。</li> </ol>
响应路径： VPC4 → VPC1	<ol style="list-style-type: none"> <li>1. 在VPC4路由表中，通过下一跳为ER的路由将流量转送到ER。</li> <li>2. VPC4关联的是ER路由表2，在ER路由表2中，通过下一跳为VPC1连接的路由将流量送达VPC1。</li> </ol>

表 3-3 同区域 VPC 隔离组网规划说明

资源	说明
VPC	<ul style="list-style-type: none"> <li>• VPC1、VPC2、VPC3隔离，这3个VPC和VPC4互通。</li> <li>• VPC网段（CIDR）不能重叠。 本示例中，ER路由表使用的是“虚拟私有云（VPC）”连接的传播路由，由ER自动学习VPC网段作为目的地址，不支持修改，因此重叠的VPC网段会导致路由冲突。 如果您已有的VPC存在网段重叠，则不建议您使用传播路由，请在ER路由表中手动添加静态路由，目的地址可以为VPC子网网段或者范围更小的网段。</li> <li>• VPC有一个默认路由表。</li> <li>• VPC默认路由表中的路由说明如下： <ul style="list-style-type: none"> <li>- local：表示VPC本地IPv4的默认路由条目，用于VPC内子网通信，系统自动配置。</li> <li>- ER：表示将VPC子网流量路由至ER，建议您在VPC路由表中增加三个VPC的网段10.0.0.0/8、172.16.0.0/12、192.168.0.0/16，路由信息如表3-4所示。</li> </ul> </li> </ul>
ER	<p>不开启“默认路由表关联”和“默认路由表传播”功能，手动创建两个路由表，并添加4个“虚拟私有云（VPC）”连接，路由表作如下配置：</p> <ul style="list-style-type: none"> <li>• 路由表1：关联VPC1连接、VPC2连接、VPC3连接，并在路由表1中创建VPC4连接的传播，路由自动学习VPC网段，路由信息如表3-5所示。</li> <li>• 路由表2：关联VPC4连接，并在路由表2中创建VPC1连接、VPC2连接、VPC3连接的传播，路由自动学习VPC网段，路由信息如表3-6所示。</li> </ul>
ECS	<p>4个ECS分别位于不同的VPC内，VPC中的ECS如果位于不同的安全组，需要在安全组中添加规则放通对端安全组的网络。</p>

表 3-4 VPC 路由表

目的地址	下一跳	路由类型
10.0.0.0/8	企业路由器	静态路由：自定义
172.16.0.0/12	企业路由器	静态路由：自定义
192.168.0.0/16	企业路由器	静态路由：自定义

#### 说明

- 如果您在创建连接时开启“配置连接侧路由”选项，则不用手动在VPC路由表中配置静态路由，系统会在VPC的所有路由表中自动添加指向ER的路由，目的地址固定为10.0.0.0/8，172.16.0.0/12，192.168.0.0/16。
- 如果VPC路由表中的路由与这三个固定网段冲突，则会添加失败。此时建议您不要开启“配置连接侧路由”选项，并在连接创建完成后，手动添加路由。
- 不建议在VPC路由表中将ER的路由配置为默认路由网段0.0.0.0/0，如果VPC内的ECS绑定了EIP，会在ECS内增加默认网段的策略路由，并且优先级高于ER路由，此时会导致流量转发至EIP，无法抵达ER。

表 3-5 ER 路由表 1

目的地址	下一跳	路由类型
VPC4网段： 192.168.0.0/16	VPC4连接：er-attach-share	传播路由

表 3-6 ER 路由表 2

目的地址	下一跳	路由类型
VPC1网段：10.1.0.0/16	VPC1连接：er-attach-isolation-01	传播路由
VPC2网段：10.2.0.0/16	VPC2连接：er-attach-isolation-02	传播路由
VPC3网段：10.3.0.0/16	VPC3连接：er-attach-isolation-03	传播路由

## 规划资源

企业路由器ER、虚拟私有云VPC、弹性云服务器ECS只要位于同一个区域内即可，可用区可以任意选择，不用保持一致。

#### 说明

以下资源规划详情仅为示例，您可以根据需要自行修改。

- 企业路由器ER：1个，资源规划详情如表3-7所示。

表 3-7 ER 资源规划详情

ER名称	AS号	默认路由表关联	默认路由表传播	路由表	连接
er-test-01	64512	关闭	关闭	2个路由表： <ul style="list-style-type: none"> <li>er-rtb-isolation</li> <li>er-rtb-share</li> </ul>	er-attach-isolation-01
					er-attach-isolation-02
					er-attach-isolation-03
					er-attach-share

表 3-8 ER 路由表 1 资源规划详情

路由表名称	关联连接	传播
er-rtb-isolation	er-attach-isolation-01	er-attach-share
	er-attach-isolation-02	
	er-attach-isolation-03	

表 3-9 ER 路由表 2 资源规划详情

路由表名称	关联连接	传播
er-rtb-share	er-attach-share	er-attach-isolation-01
		er-attach-isolation-02
		er-attach-isolation-03

- 虚拟私有云VPC：4个，VPC的网段不能重复，资源规划详情如表3-10所示。

表 3-10 VPC 资源规划详情

VPC名称	VPC网段	子网名称	子网网段	关联路由表
vpc-isolation-01	10.1.0.0/16	subnet-isolation-01	10.1.0.0/24	默认路由表
vpc-isolation-02	10.2.0.0/16	subnet-isolation-02	10.2.0.0/24	默认路由表
vpc-isolation-03	10.3.0.0/16	subnet-isolation-03	10.3.0.0/24	默认路由表

VPC名称	VPC网段	子网名称	子网网段	关联路由表
vpc-share	192.168.0.0/16	subnet-share	192.168.0.0/24	默认路由表

- 弹性云服务器ECS：4个，分别接入4个不同的VPC，资源规划详情如表3-11所示。

表 3-11 ECS 资源规划详情

ECS名称	镜像	VPC名称	子网名称	安全组	私有IP地址
ecs-isolation-01	公共镜像： CentOS 7.5 64bit	vpc-isolation-01	subnet-isolation-01	sg-demo： 通用Web 服务器	10.1.0.134
ecs-isolation-02		vpc-isolation-02	subnet-isolation-02		10.2.0.215
ecs-isolation-03		vpc-isolation-03	subnet-isolation-03		10.3.0.14
ecs-share		vpc-share	subnet-share		192.168.0.130

## 3.3 创建资源

### 3.3.1 创建企业路由器

#### 操作场景

本章节指导用户创建企业路由器。

#### 操作步骤

**步骤1** 在区域A内，创建1个企业路由器。

创建企业路由器，具体方法请参见[创建企业路由器](#)。

企业路由器资源规划详情请参见[表3-7](#)。

----结束

### 3.3.2 创建 VPC 和 ECS

#### 操作场景

本章节指导用户创建虚拟私有云VPC和弹性云服务器ECS。

## 操作步骤

**步骤1** 在区域A内，创建4个VPC和4个ECS。

创建VPC及子网，具体方法请参见[创建虚拟私有云和子网](#)。

创建ECS，具体方法请参见[自定义购买ECS](#)。

- 本示例中的VPC和子网资源规划详情请参见[表3-10](#)。
- 本示例中的ECS资源规划详情请参见[表3-11](#)。

----结束

## 3.4 配置网络

### 3.4.1 在企业路由器中配置 VPC 连接

#### 操作场景

本章节指导用户在企业路由器中配置“虚拟私有云（VPC）”连接，即将VPC接入企业路由器中，并配置企业路由器和VPC的路由。

#### 操作步骤

**步骤1** 将4个VPC分别接入企业路由器中。

添加“虚拟私有云（VPC）”连接，具体方法请参见[在企业路由器中添加VPC连接](#)。

**步骤2** 在企业路由器中创建2个路由表。

创建路由表，具体方法请参见[创建路由表](#)。

**步骤3** 在两个路由表中分别创建“虚拟私有云（VPC）”连接的关联和传播。

创建关联，具体方法请参见[创建关联将连接关联至路由表中](#)。

创建传播，具体方法请参见[创建传播](#)。

- 路由表1资源规划详情，请参见[表3-8](#)。
- 路由表2资源规划详情，请参见[表3-9](#)。

**步骤4** 在VPC路由表中配置ER的路由信息。

配置路由信息，具体方法请参见[在VPC路由表中配置路由](#)。

----结束

## 3.5 验证网络互通情况

**步骤1** 登录弹性云服务器。

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）。

**步骤2** 在弹性云服务器的远程登录窗口，执行以下命令，验证网络情况。

1. 执行以下命令，验证VPC网络隔离情况。

**ping 弹性云服务器IP地址**

以登录ecs-isolation-01，验证vpc-isolation-01与vpc-isolation-02、vpc-isolation-03的网络隔离情况为例：

**ping 10.2.0.215**

**ping 10.3.0.14**

回显如下信息，没有流量信息，表示网络隔离配置成功。

```
PING 10.2.0.215 (10.2.0.215) 56(84) bytes of data.  
^C  
--- 10.2.0.215 ping statistics ---  
6 packets transmitted, 0 received, 100% packet loss, time 4999ms
```

```
PING 10.3.0.14 (10.3.0.14) 56(84) bytes of data.  
^C  
--- 10.3.0.14 ping statistics ---  
3 packets transmitted, 0 received, 100% packet loss, time 1999ms
```

2. 执行以下命令，验证VPC网络互通情况。

**ping 弹性云服务器IP地址**

以登录ecs-isolation-01，验证vpc-isolation-01与vpc-share的网络互通情况为例：

**ping 192.168.0.130**

回显如下信息，表示网络互通。

```
PING 192.168.0.130 (192.168.0.130) 56(84) bytes of data.  
64 bytes from 192.168.0.130: icmp_seq=1 ttl=64 time=0.455 ms  
64 bytes from 192.168.0.130: icmp_seq=2 ttl=64 time=0.340 ms  
64 bytes from 192.168.0.130: icmp_seq=3 ttl=64 time=0.310 ms  
64 bytes from 192.168.0.130: icmp_seq=4 ttl=64 time=0.232 ms  
64 bytes from 192.168.0.130: icmp_seq=5 ttl=64 time=0.275 ms  
^C  
--- 192.168.0.130 ping statistics ---  
5 packets transmitted, 5 received, 0% packet loss, time 4002ms  
rtt min/avg/max/mdev = 0.275/0.578/1.131/0.345 ms
```

**步骤3** 重复执行**步骤1**~**步骤2**，验证其他VPC之间的网络隔离和互通情况。

----结束

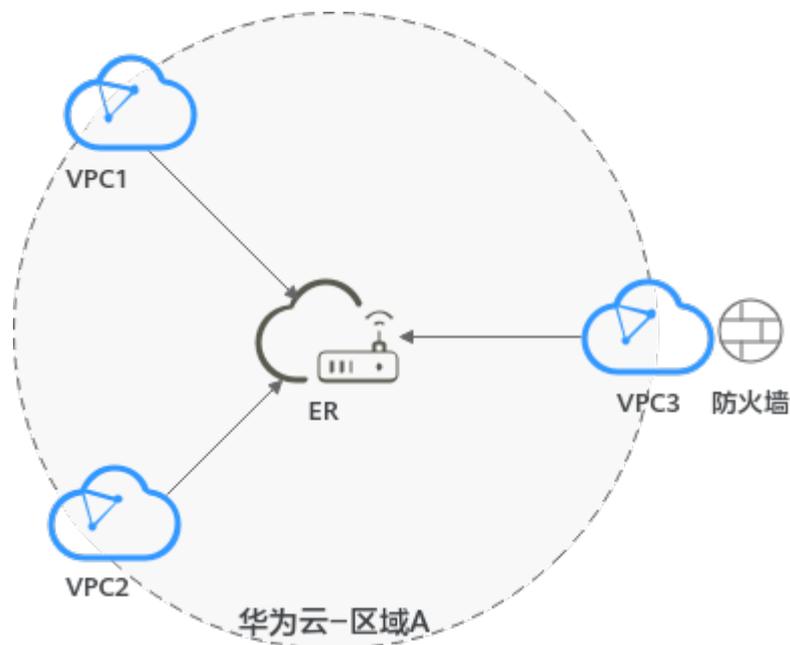
# 4 通过企业路由器和第三方防火墙实现多 VPC 互访流量清洗

## 4.1 方案概述

### 背景信息

XX企业在华为云区域A内部署了3个虚拟私有云VPC，其中业务A、业务B分别部署在VPC1、VPC2，VPC3部署有第三方防火墙软件。出于安全考虑，要求业务A和业务B互相访问的流量必须通过VPC3中防火墙软件的过滤清洗。

图 4-1 同区域 VPC 流量清洗



**说明**

您可以使用**企业路由器的共享功能**，将不同账号下的虚拟私有云添加至同一个企业路由器中构建组网。

**操作流程**

本文档介绍如何通过企业路由器构建同区域VPC流量清洗组网，流程如图4-2所示。

图 4-2 构建同区域 VPC 流量清洗组网流程图

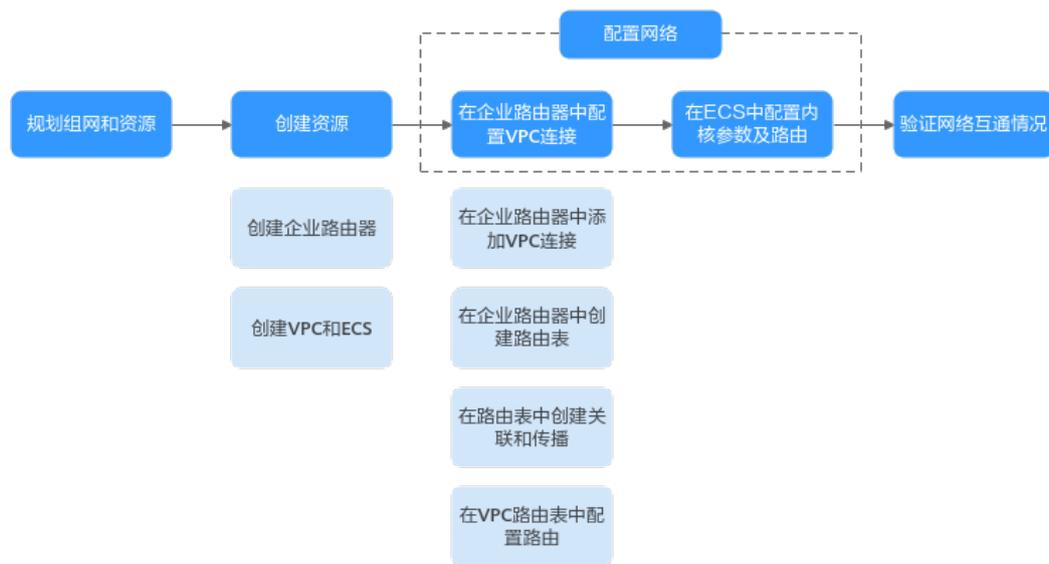


表 4-1 构建同区域 VPC 流量清洗组网流程说明

序号	步骤	说明
1	<b>规划组网和资源</b>	规划组网和资源，包括资源数量及网段信息等。
2	<b>创建资源</b>	1. <b>创建企业路由器</b> ：创建1个企业路由器，构建一个同区域组网只需要1个企业路由器。 2. <b>创建VPC和ECS</b> ：创建3个虚拟私有云VPC和3个弹性云服务器ECS。

序号	步骤	说明
3	配置网络	<ol style="list-style-type: none"> <li>在企业路由器中配置VPC连接：                             <ol style="list-style-type: none"> <li>在企业路由器中添加“虚拟私有云（VPC）”连接：将3个VPC分别接入企业路由器中。</li> <li>在企业路由器中创建路由表；创建2个自定义路由表。</li> <li>在路由表中创建关联和传播：根据网络规划，在两个路由表中分别创建“虚拟私有云（VPC）”连接的关联和传播。</li> <li>在VPC路由表中配置路由：在VPC路由表中配置到企业路由器的路由信息。</li> </ol> </li> <li>在ECS中配置内核参数及路由：安装防火墙的ECS3具有双网卡，需要配置内核参数并添加路由，确保eth0和eth1之间的流量转发路径可达。</li> </ol>
4	验证网络互通情况	登录ECS，执行ping命令，验证网络互通情况。

## 4.2 规划组网和资源

通过企业路由器构建同区域VPC流量清洗组网，您需要规划组网和资源：

- **规划组网**：规划VPC及其子网的网段、VPC路由表和ER路由表信息。
- **规划资源**：规划云上资源的数量、名称以及主要参数等信息，云上资源包括VPC、ECS以及ER。

### 规划组网

同区域VPC流量清洗组网规划如图4-3所示，将3个VPC接入ER中，组网规划说明如表4-3所示。

图 4-3 同区域 VPC 流量清洗组网规划

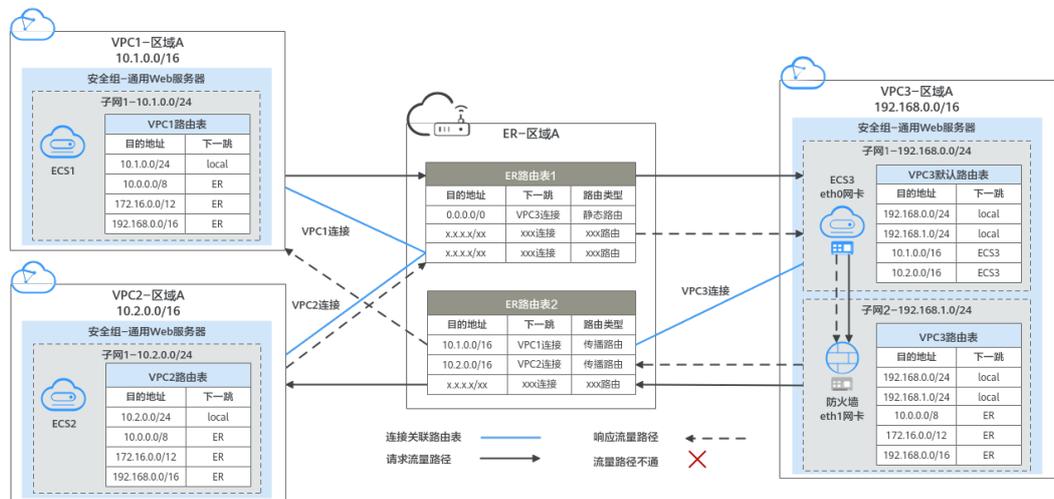


表 4-2 网络流量路径说明

路径	说明
请求路径： VPC1 → VPC2	<ol style="list-style-type: none"> <li>1. 在VPC1路由表中，通过下一跳为ER的路由将流量转送到ER。</li> <li>2. VPC1关联的是ER路由表1，在ER路由表1中，通过下一跳为VPC3连接的静态路由将流量转送到VPC3。</li> <li>3. VPC3有两个子网，分别关联了ECS3的两个网卡：               <ol style="list-style-type: none"> <li>a. 子网1的eth0网卡接收流量。在VPC3默认路由表中，通过下一跳为ECS3的路由，以及ECS内核配置，将流量从eth0网卡转送到eth1网卡。</li> <li>b. 子网2的eth1网卡通过防火墙清洗并送出流量。在VPC3自定义路由表中，通过下一跳为ER的路由，将清洗后的流量转送到ER。</li> </ol> </li> <li>4. VPC3关联的是ER路由表2，在ER路由表2中，通过下一跳为VPC2连接的传播路由将流量送达VPC2。</li> </ol>
响应路径： VPC2 → VPC1	<ol style="list-style-type: none"> <li>1. 在VPC2路由表中，通过下一跳为ER的路由将流量转送到ER。</li> <li>2. VPC2关联的是ER路由表1，在ER路由表1中，通过下一跳为VPC3连接的静态路由将流量转送到VPC3。</li> <li>3. VPC3有两个子网，分别关联了ECS3的两个网卡：               <ol style="list-style-type: none"> <li>a. 子网1的eth0网卡接收流量。在VPC3默认路由表中，通过下一跳为ECS3的路由，以及ECS内核配置，将流量从eth0网卡转送到eth1网卡。</li> <li>b. 子网2的eth1网卡通过防火墙清洗并送出流量。在VPC3自定义路由表中，通过下一跳为ER的路由，将清洗后的流量转送到ER。</li> </ol> </li> <li>4. VPC3关联的是ER路由表2，在ER路由表2中，通过下一跳为VPC1连接的传播路由将流量送达VPC1。</li> </ol>

表 4-3 同区域 VPC 流量清洗组网规划说明

资源	说明
VPC	<ul style="list-style-type: none"> <li>● VPC1和VPC2的互访流量需要通过VPC3部署的防火墙清洗。</li> <li>● VPC网段（CIDR）不能重叠。 本示例中，ER路由表使用的是“虚拟私有云（VPC）”连接的传播路由，由ER自动学习VPC网段作为目的地址，不支持修改，因此重叠的VPC网段会导致路由冲突。 如果您已有的VPC存在网段重叠，则不建议您使用传播路由，请在ER路由表中手动添加静态路由，目的地址可以为VPC子网网段或者范围更小的网段。</li> <li>● VPC1和VPC2各有一个默认路由表。</li> <li>● VPC3有两个子网，子网1关联默认路由表，子网2关联自定义路由表。</li> <li>● VPC默认路由表中的路由说明如下： <ul style="list-style-type: none"> <li>- local：表示VPC本地IPV4的默认路由条目，用于VPC内子网通信，系统自动配置。</li> <li>- ER：表示将VPC子网流量路由至ER，自定义路由，建议网段为0.0.0.0/0，路由信息如表4-4所示。</li> <li>- ECS3：表示将VPC子网流量路由至ECS3，自定义路由，路由表信息如表4-5所示。</li> </ul> </li> </ul>
ER	<p>不开启“默认路由表关联”和“默认路由表传播”功能，手动创建两个路由表，并添加3个“虚拟私有云（VPC）”连接，路由表作如下配置：</p> <ul style="list-style-type: none"> <li>● 路由表1：关联VPC1连接和VPC2连接，并在路由表1中创建VPC3连接的静态路由，路由信息如表4-6所示。</li> <li>● 路由表2：关联VPC3连接，并在路由表2中创建VPC1连接和VPC2连接的传播，路由自动学习VPC网段，路由信息如表4-7所示。</li> </ul>
ECS	<ul style="list-style-type: none"> <li>● 3个ECS分别位于不同的VPC内，VPC中的ECS如果位于不同的安全组，需要在安全组中添加规则放通对端安全组的网络。</li> <li>● ECS3部署了第三方防火墙，共有两个网卡，分别关联VPC3的不同子网。</li> </ul>

表 4-4 VPC1 和 VPC2 路由表、VPC3 自定义路由表

目的地址	下一跳	路由类型
10.0.0.0/8	企业路由器	静态路由：自定义
172.16.0.0/12	企业路由器	静态路由：自定义
192.168.0.0/16	企业路由器	静态路由：自定义

### 说明

- 如果您在创建连接时开启“配置连接侧路由”选项，则不用手动在VPC路由表中配置静态路由，系统会在VPC的所有路由表中自动添加指向ER的路由，目的地址固定为10.0.0.0/8，172.16.0.0/12，192.168.0.0/16。
- 如果VPC路由表中的路由与这三个固定网段冲突，则会添加失败。此时建议您不要开启“配置连接侧路由”选项，并在连接创建完成后，手动添加路由。
- 对于VPC3的连接，不建议开启“配置连接侧路由”选项，VPC3默认路由表中不能添加指向ER的路由。
- 不建议在VPC路由表中将ER的路由配置为默认路由网段0.0.0.0/0，如果VPC内的ECS绑定了EIP，会在ECS内增加默认网段的策略路由，并且优先级高于ER路由，此时会导致流量转发至EIP，无法抵达ER。

表 4-5 VPC3 默认路由表

目的地址	下一跳	路由类型
10.1.0.0/16	服务器实例	静态路由：自定义
10.2.0.0/16	服务器实例	静态路由：自定义

表 4-6 ER 路由表 1

目的地址	下一跳	路由类型
0.0.0.0/0	VPC3连接：er-attach-inspection	静态路由

表 4-7 ER 路由表 2

目的地址	下一跳	路由类型
VPC1网段：10.1.0.0/16	VPC1连接：er-attach-01	传播路由
VPC2网段：10.2.0.0/16	VPC2连接：er-attach-02	传播路由

## 规划资源

企业路由器ER、虚拟私有云VPC、弹性云服务器ECS只要位于同一个区域内即可，可用区可以任意选择，不用保持一致。

### 说明

以下资源规划详情仅为示例，您可以根据需要自行修改。

- 企业路由器ER：1个，资源规划详情如表4-8所示。

表 4-8 ER 资源规划详情

ER名称	AS号	默认路由表关联	默认路由表传播	路由表	连接
er-test-01	64512	关闭	关闭	2个路由表： • <b>er-rtb-01</b> • <b>er-rtb-02</b>	er-attach-01
					er-attach-02
					er-attach-inspection

表 4-9 ER 路由表 1 资源规划详情

路由表名称	关联连接	静态路由
er-rtb-01	er-attach-01	er-attach-inspection
	er-attach-02	

表 4-10 ER 路由表 2 资源规划详情

路由表名称	关联连接	传播
er-rtb-02	er-attach-inspection	er-attach-01
		er-attach-02

- 虚拟私有云VPC：3个，VPC的网段不能重复，资源规划详情如表4-11所示。

表 4-11 VPC 资源规划详情

VPC名称	VPC网段	子网名称	子网网段	关联路由表
vpc-demo-01	10.1.0.0/16	subnet-demo-01	10.1.0.0/24	默认路由表
vpc-demo-02	10.2.0.0/16	subnet-demo-02	10.2.0.0/24	默认路由表
vpc-inspection	192.168.0.0/16	subnet-inspection-01	192.168.0.0/24	默认路由表
		subnet-inspection-02	192.168.1.0/24	自定义路由表

- 弹性云服务器ECS：3个，分别接入3个不同的VPC，资源规划详情如表4-12和表4-13所示。

表 4-12 ECS1 和 ECS2 资源规划详情

ECS名称	镜像	VPC名称	子网名称	安全组	私有IP地址
ecs-demo-01	公共镜像： CentOS 8.0 64bit	vpc-demo-01	subnet-demo-01	sg-demo： 通用Web 服务器	10.1.0.113
ecs-demo-02		vpc-demo-02	subnet-demo-02		10.2.0.175

表 4-13 ECS3 资源规划详情

ECS名称	镜像	网卡	VPC名称	子网名称	安全组	私有IP地址
ecs-inspection	公共镜像： CentOS 8.0 64bit	eth0	vpc-inspection	subnet-inspection-01	sg-demo： 通用Web 服务器	192.168.0.21
		eth1		subnet-inspection-02		192.168.1.22

## 4.3 创建资源

### 4.3.1 创建企业路由器

#### 操作场景

本章节指导用户创建企业路由器。

#### 操作步骤

**步骤1** 在区域A内，创建1个企业路由器。

创建企业路由器，具体方法请参见[创建企业路由器](#)。

企业路由器资源规划详情请参见[表4-8](#)。

----结束

### 4.3.2 创建 VPC 和 ECS

#### 操作场景

本章节指导用户创建虚拟私有云VPC和弹性云服务器ECS，其中一台ECS需要安装第三方防火墙。

## 操作步骤

**步骤1** 在区域A内，创建3个VPC。

创建VPC及子网，具体方法请参见[创建虚拟私有云和子网](#)。

本示例中的VPC和子网资源规划详情请参见[表4-11](#)。

**步骤2** 在区域A内，创建3个ECS。

创建ECS，具体方法请参见[自定义购买ECS](#)。

- 本示例中的ECS1和ECS2资源规划详情请参见[表4-12](#)。
- 本示例中的ECS3需要两个网卡，资源规划详情请参见[表4-13](#)。

ECS3创建完成后，进入ECS3详情页，在“弹性网卡”页签下，关闭第二个网卡（eth1）的“源/目的检查”，以确保从eth1出来的流量不会被拦截。

**步骤3** 在ECS3中安装第三方防火墙。

您可以自行安装或者通过[华为云市场](#)购买第三方防火墙。

----结束

## 4.4 配置网络

### 4.4.1 在企业路由器中配置 VPC 连接

#### 操作场景

本章节指导用户在企业路由器中配置“虚拟私有云（VPC）”连接，即将VPC接入企业路由器中，并配置企业路由器和VPC的路由。

#### 操作步骤

**步骤1** 将3个VPC分别接入企业路由器中。

添加“虚拟私有云（VPC）”连接，具体方法请参见[在企业路由器中添加VPC连接](#)。

**步骤2** 在企业路由器中创建2个路由表。

创建路由表，具体方法请参见[创建路由表](#)。

**步骤3** 在ER路由表1中创建“虚拟私有云（VPC）”连接的关联和静态路由。

路由表1资源规划详情，请参见[表4-9](#)。

1. 将VPC1连接和VPC2连接关联至路由表1。  
创建关联，具体方法请参见[创建关联将连接关联至路由表中](#)。
2. 在路由表1中创建下一跳为VPC3连接的静态路由，网段为0.0.0.0/0。  
创建静态路由，具体方法请参见[创建静态路由](#)。

**步骤4** 在ER路由表2中创建“虚拟私有云（VPC）”连接的关联和传播。

路由表2资源规划详情，请参见[表3-9](#)。

1. 将VPC3连接关联至路由表2。  
创建关联，具体方法请参见[创建关联将连接关联至路由表中](#)。
2. 在路由表2中，创建VPC1连接和VPC2连接的传播。  
创建传播，具体方法请参见[创建传播](#)。

**步骤5** 在VPC路由表中配置路由信息。

配置路由信息，具体方法请参见[在VPC路由表中配置路由](#)。

1. 配置VPC到ER路由。  
路由规划详情，请参见[表4-4](#)。
2. 在VPC3默认路由表中，配置VPC到ECS路由。  
路由规划详情，请参见[表4-5](#)。

----结束

## 4.4.2 在 ECS 中配置内核参数及路由

### 操作场景

ECS3具有双网卡，需要配置内核参数并添加路由，确保eth0和eth1之间的流量转发路径可达。

#### 须知

本示例中的ECS操作系统为CentOS 8.0 64bit，操作系统不同，配置命令可能存在差异。

### 操作步骤

**步骤1** 登录弹性云服务器。

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）。

**步骤2** 执行以下步骤，关闭系统对数据包源地址的校验。

1. 执行以下命令，打开“/etc/sysctl.conf”文件。

```
vim /etc/sysctl.conf
```

2. 按i进入编辑模式。

3. 在文件末尾添加以下配置。

```
net.ipv4.conf.default.rp_filter = 0  
net.ipv4.conf.all.rp_filter = 0
```

4. 按ESC退出，并输入:wq!保存配置。

5. 执行以下命令，刷新使配置立即生效。

```
sysctl -p
```

6. 执行以下命令，查看是否关闭系统对数据包源地址的校验。

```
sysctl -a | grep rp_filter
```

回显类似如下信息，“net.ipv4.conf.all.rp\_filter”和“net.ipv4.conf.default.rp\_filter”取值为0，表示关闭成功。

```
[root@ecs-inspection ~]# sysctl -a | grep rp_filter
net.ipv4.conf.all.rp_filter = 0
net.ipv4.conf.all.rp_filter = 0
net.ipv4.conf.default.rp_filter = 0
net.ipv4.conf.default.rp_filter = 0
net.ipv4.conf.eth0.rp_filter = 0
net.ipv4.conf.eth0.rp_filter = 0
net.ipv4.conf.eth1.rp_filter = 0
net.ipv4.conf.eth1.rp_filter = 0
net.ipv4.conf.lo.rp_filter = 0
net.ipv4.conf.lo.rp_filter = 0
```

**步骤3** 执行以下步骤，打开系统的转发功能。

1. 执行以下命令，打开“/etc/sysctl.conf”文件。

```
vim /etc/sysctl.conf
```

2. 按i进入编辑模式。
3. 在文件末尾添加以下配置。  
net.ipv4.ip\_forward = 1
4. 按ESC退出，并输入:wq!保存配置。
5. 执行以下命令，刷新使配置立即生效。

```
sysctl -p
```

6. 执行以下命令，查看是否打开系统的转发功能。

```
sysctl -a | grep ip_forward
```

回显类似如下信息，“net.ipv4.ip\_forward”取值为1，表示打开成功。

```
[root@ecs-inspection ~]# sysctl -a | grep ip_forward
net.ipv4.ip_forward = 1
net.ipv4.ip_forward_update_priority = 1
net.ipv4.ip_forward_use_pmtu = 0
```

**步骤4** 执行以下步骤，配置路由。

该路由表示去往VPC1和VPC2的流量清洗后，会通过eth1发出去。

本文档为您提供CentOS 8.0和CentOS 7.4路由配置方法供您参考，具体如下：

- CentOS 8.0:

- a. 执行以下命令，打开网卡配置文件。

```
vi /etc/sysconfig/network-scripts/route-eth1
```

- b. 按i进入编辑模式。
- c. 在文件末尾添加以下配置。  
10.1.0.0/16 via 192.168.1.1  
10.2.0.0/16 via 192.168.1.1

其中，10.1.0.0/16为VPC1的网段，10.2.0.0/16为VPC2的网段，192.168.1.1为eth1的网关地址。

- d. 按ESC退出，并输入:wq!保存配置。
- e. 重启ECS3，使路由生效。
- f. 重启完成后，执行以下命令，检查路由是否添加成功。

```
route -n
```

回显类似如下信息，可以在路由表中看到添加的两条路由。

```
[root@ecs-inspection ~]# route -n
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
0.0.0.0 192.168.0.1 0.0.0.0 UG 100 0 0 eth0
10.1.0.0 192.168.1.1 255.255.0.0 UG 0 0 0 eth1
10.2.0.0 192.168.1.1 255.255.0.0 UG 0 0 0 eth1
169.254.169.254 192.168.0.254 255.255.255.255 UGH 100 0 0 eth0
192.168.0.0 0.0.0.0 255.255.255.0 U 100 0 0 eth0
192.168.1.0 0.0.0.0 255.255.255.0 U 101 0 0 eth1
```

- CentOS 7.4:

- a. 执行以下命令，打开网卡配置文件。

```
vi /etc/sysconfig/static-routes
```

- b. 按i进入编辑模式。

- c. 在文件末尾添加以下配置。

```
any net 10.1.0.0/16 gw 192.168.1.1
any net 10.2.0.0/16 gw 192.168.1.1
```

其中，10.1.0.0/16为VPC1的网段，10.2.0.0/16为VPC2的网段，192.168.1.1为eth1的网关地址。

- d. 按ESC退出，并输入:wq!保存配置。
- e. 执行以下命令，重启网络服务使配置生效。

```
service network restart
```

- f. 重启完成后，执行以下命令，检查路由是否添加成功。

```
route -n
```

回显类似如下信息，可以在路由表中看到添加的两条路由。

```
[root@ecs-inspection ~]# route -n
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
0.0.0.0 192.168.0.1 0.0.0.0 UG 100 0 0 eth0
10.1.0.0 192.168.1.1 255.255.0.0 UG 0 0 0 eth1
10.2.0.0 192.168.1.1 255.255.0.0 UG 0 0 0 eth1
169.254.169.254 192.168.0.254 255.255.255.255 UGH 100 0 0 eth0
192.168.0.0 0.0.0.0 255.255.255.0 U 100 0 0 eth0
192.168.1.0 0.0.0.0 255.255.255.0 U 101 0 0 eth1
```

----结束

## 4.5 验证网络互通情况

### 步骤1 登录弹性云服务器。

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）。

### 步骤2 在弹性云服务器的远程登录窗口，执行以下步骤，验证网络情况。

1. 登录ecs-demo-01，验证vpc-demo-01与vpc-demo-02的网络互通情况为例：

```
ping 弹性云服务器IP地址
```

命令示例：

```
ping 10.2.0.175
```

回显类似如下信息，表示网络互通配置成功。

```
[root@ecs-demo-01 ~]# ping 10.2.0.175
PING 10.2.0.175 (10.2.0.175) 56(84) bytes of data.
64 bytes from 10.2.0.175: icmp_seq=1 ttl=63 time=1.78 ms
64 bytes from 10.2.0.175: icmp_seq=2 ttl=63 time=1.03 ms
64 bytes from 10.2.0.175: icmp_seq=3 ttl=63 time=0.951 ms
64 bytes from 10.2.0.175: icmp_seq=4 ttl=63 time=0.963 ms
64 bytes from 10.2.0.175: icmp_seq=5 ttl=63 time=0.965 ms
64 bytes from 10.2.0.175: icmp_seq=6 ttl=63 time=0.943 ms
^C
--- 10.2.0.175 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 12ms
rtt min/avg/max/mdev = 0.943/1.105/1.784/0.307 ms
```

2. 不要中断**步骤2.1**，登录ecs-inspection，验证vpc-demo-01到vpc-demo-02的流量是否通过ecs-inspection。
  - a. 检查eth0网卡的接收流量，至少连续执行两次命令，检查RX packets是否增加。

```
ifconfig eth0
```

- b. 检查eth1网卡的发送流量，至少连续执行两次命令，检查TX packets是否增加。

```
ifconfig eth1
```

回显类似如下信息，表示流量通过ecs-inspection。

```
[root@ecs-inspection ~]# ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.0.21 netmask 255.255.255.0 broadcast 192.168.0.255
    inet6 fe80::34c8:d0f7:a82f:ceb7 prefixlen 64 scopeid 0x20<link>
    ether fa:16:3e:5a:ea:be txqueuelen 1000 (Ethernet)
    RX packets 520241 bytes 50982241 (48.6 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 422285 bytes 41557376 (39.6 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[root@ecs-inspection ~]# ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.0.21 netmask 255.255.255.0 broadcast 192.168.0.255
    inet6 fe80::34c8:d0f7:a82f:ceb7 prefixlen 64 scopeid 0x20<link>
    ether fa:16:3e:5a:ea:be txqueuelen 1000 (Ethernet)
    RX packets 520267 bytes 50984789 (48.6 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 422285 bytes 41557376 (39.6 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[root@ecs-inspection ~]# ifconfig eth1
eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.22 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::dd1f:e122:7899:5611 prefixlen 64 scopeid 0x20<link>
    ether fa:16:3e:db:2d:b2 txqueuelen 1000 (Ethernet)
    RX packets 379 bytes 21854 (21.3 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 98891 bytes 9670654 (9.2 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[root@ecs-inspection ~]# ifconfig eth1
eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.22 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::dd1f:e122:7899:5611 prefixlen 64 scopeid 0x20<link>
    ether fa:16:3e:db:2d:b2 txqueuelen 1000 (Ethernet)
    RX packets 380 bytes 21910 (21.3 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 98924 bytes 9673832 (9.2 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

**步骤3** 重复执行**步骤1~步骤2**，登录ecs-demo-02，验证反向路径。

----结束

# 5 通过企业路由器和中转 VPC 构建组网

## 5.1 方案概述

### 应用场景

您可以通过企业路由器构建中心辐射型组网，简化网络架构。当前为您提供两种典型组网方案，方案一是将业务VPC直接接入企业路由器，方案二是使用中转VPC，结合VPC对等连接和企业路由器共同构建组网。相比方案一，方案二可以降低成本，并且免去一些限制，详细说明如下：

- 相比方案一，使用方案二可以降低流量费用和连接费用，详细说明如下：
  - 业务VPC之间的流量通过VPC对等连接转发，而不再需要经过ER转发，省去部分流量费用。
  - 您只需要将一个中转VPC接入ER，相比接入多个业务VPC，省去部分连接费用。
- 当前将业务VPC直接接入ER，针对业务VPC有部分使用限制。由于方案二中您只需要将中转VPC接入ER，则可以解决以下针对业务VPC的限制：
  - 当业务VPC下存在共享型弹性负载均衡、VPC终端节点、私网NAT网关、分布式缓存服务时，请[提交工单](#)联系华为云客服，确认服务的兼容性，并优先考虑使用中转VPC组网方案。

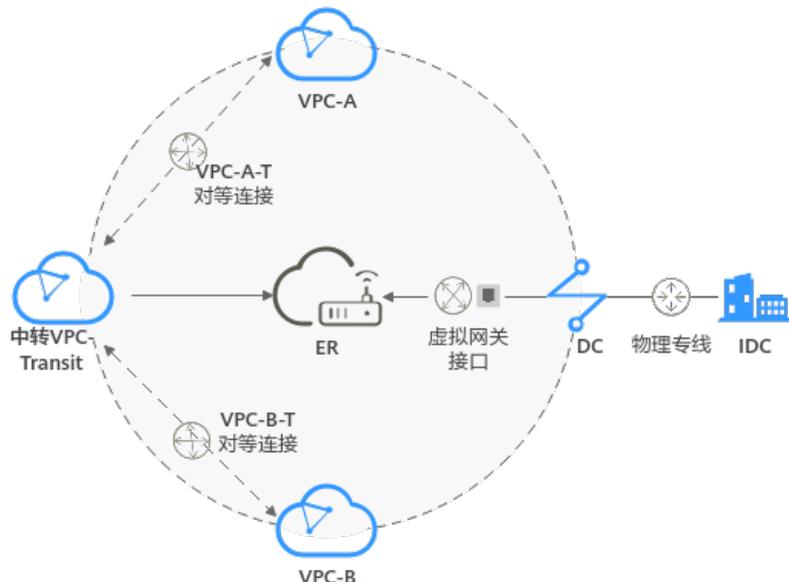
若您在弹性负载均衡、VPC终端节点以及分布式缓存服务场景下，直接将业务VPC接入ER，则当ER处于容灾切换、弹性扩缩容、升级等业务可靠性保障过程中，可能造成长连接会话闪断，请您确保业务客户端具有重连机制，在闪断情况下可以自动重连。
  - 当接入ER的VPC存在以下情况时，则不建议您在VPC路由表中将下一跳为ER的路由配置成默认路由0.0.0.0/0，那样会导致部分业务流量无法转发至ER。
    - VPC内的ECS绑定了EIP。
    - VPC被ELB（独享型或者共享型）、NAT网关、VPCEP、DCS服务占用。
  - 当接入ER的VPC关联NAT网关，并配置SNAT或者DNAT规则的“使用场景”选择“云专线/云连接”，则网络不通。

## 方案架构

在方案二中，业务VPC之间通过对等连接通信，业务VPC和线下IDC通过ER通信，组网架构图如图5-1所示。

1. 在业务VPC-A和中转VPC-Transit、业务VPC-B和中转VPC-Transit之间各创建一个VPC对等连接，通过VPC-Transit和对等连接转发VPC-A和VPC-B之间的流量。
2. 将VPC-Transit接入企业路由器中，VPC-A和VPC-B访问线下IDC的流量通过中转VPC转发至ER，再通过ER和DC抵达线下IDC。

图 5-1 中转 VPC 接入企业路由器组网架构图（方案二）



## 5.2 组网和资源规划

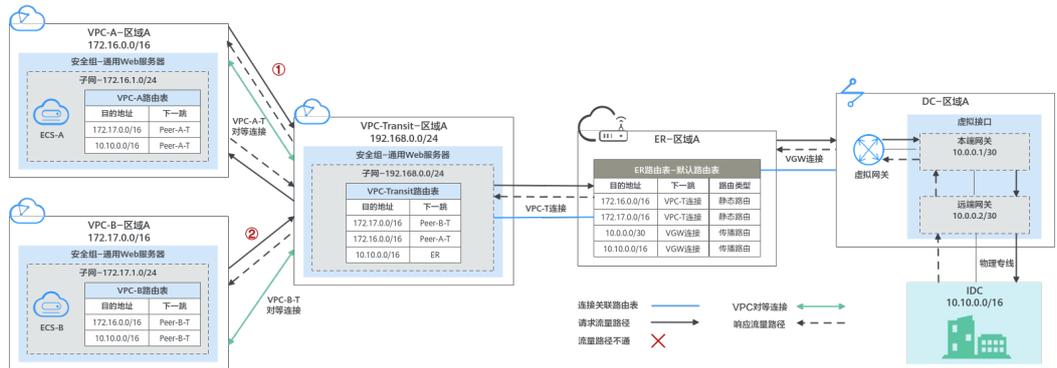
通过企业路由器和中转VPC构建混合云组网，您需要规划资源和组网，本示例中为您详细介绍资源和组网情况。

- **网络规划说明**：规划VPC及其子网、DC和ER的网段、路由等。
- **资源规划说明**：规划云上资源的数量、名称以及主要参数等信息，云上资源包括VPC、VPC对等连接、DC以及ER等。

### 网络规划说明

企业路由器和中转VPC组网规划如图5-2所示，业务VPC之间通过对等连接通信，将中转VPC和DC分别接入ER中，组网规划说明如表5-2所示。

图 5-2 企业路由器和中转 VPC 组网规划



使用企业路由器和中转VPC组网方案，可以实现业务VPC之间的云上网络通过对等连接连通，云上和云下之间的网络通过ER和DC连通。

- 云上VPC和线下IDC通信时，通过ER和DC实现通信，本示例的网络流量路径说明请参见表5-1中的“路径一”
- 云上VPC通信时，通过业务VPC和中转VPC之间的对等连接实现通信，本示例的网络流量路径说明请参见表5-1中的“路径二”。

表 5-1 网络流量路径说明

序号	路径	说明
路径一	请求路径: VPC-A → 线下IDC	<ol style="list-style-type: none"> <li>在VPC-A路由表中，通过下一跳为Peer-A-T的路由将流量转送到VPC-Transit。</li> <li>在VPC-Transit路由中，通过下一跳为ER的路由将流量转送到ER。</li> <li>在ER路由表中，通过下一跳为VGW连接的路由将流量转送到虚拟网关。</li> <li>虚拟网关连接虚拟接口，通过虚拟接口将流量从远端网关转送到物理专线。</li> <li>通过物理专线将流量送达线下IDC。</li> </ol>
	响应路径: 线下IDC → VPC-A	<ol style="list-style-type: none"> <li>通过物理专线将流量转送到虚拟接口。</li> <li>虚拟接口连接虚拟网关，通过虚拟接口将流量从本端网关转送到虚拟网关。</li> <li>通过虚拟网关将流量转送到ER。</li> <li>在ER路由表中，通过下一跳为VPC-T连接的路由将流量转送到VPC-Transit。</li> <li>在VPC-Transit路由中，通过下一跳为Peer-A-T的路由将流量送达VPC-A。</li> </ol>
路径二	请求路径: VPC-B → VPC-A	<ol style="list-style-type: none"> <li>在VPC-B路由表中，通过下一跳为Peer-B-T的路由将流量转送到VPC-Transit。</li> <li>在VPC-Transit路由表中，通过下一跳为Peer-A-T的路由将流量送达VPC-A。</li> </ol>

序号	路径	说明
	响应路径: VPC-A → VPC-B	<ol style="list-style-type: none"> <li>1. 在VPC-A路由表中, 通过下一跳为Peer-A-T的路由将流量转送到VPC-Transit。</li> <li>2. 在VPC-Transit路由表中, 通过下一跳为Peer-B-T的路由将流量送达VPC-B。</li> </ol>

表 5-2 企业路由器和中转 VPC 组网规划说明

资源	说明
VPC	<p>业务VPC, 实际运行客户业务的VPC, 本示例中为VPC-A和VPC-B, 具体说明如下:</p> <ul style="list-style-type: none"> <li>• 业务VPC的网段, 不能与客户IDC侧网段重复。</li> <li>• 通过对等连接连通的VPC子网网段不能重叠, 本示例中业务VPC-A、业务VPC-B以及中转VPC-Transit的网段均不相同。</li> <li>• VPC有一个默认路由表。</li> <li>• VPC默认路由表中的路由说明如下: <ul style="list-style-type: none"> <li>- VPC-A: 表示通过VPC-A和VPC-Transit之间的对等连接Peer-A-T, 将VPC子网流量转发至中转VPC, 此处配置两条路由, 目的地址分别为VPC-B的网段和线下IDC的子网网段, 路由信息如表5-3所示。</li> <li>- VPC-B: 表示通过VPC-B和VPC-Transit之间的对等连接Peer-B-T, 将VPC子网流量转发至中转VPC, 此处配置两条路由, 目的地址分别为VPC-A的网段和线下IDC的子网网段, 路由信息如表5-3所示。</li> </ul> </li> </ul> <p>中转VPC, 接入ER的VPC, 本示例中为VPC-Transit, 具体说明如下:</p> <ul style="list-style-type: none"> <li>• 中转VPC用于中转业务VPC之间、以及业务VPC和线下IDC之间的流量, 该VPC下不建议运行任何业务。</li> <li>• 中转VPC的网段, 不能与客户IDC侧网段重复。</li> <li>• 通过对等连接连通的VPC子网网段不能重叠, 本示例中业务VPC-A、业务VPC-B以及中转VPC-Transit的网段均不相同。</li> <li>• VPC有一个默认路由表。</li> <li>• VPC默认路由表中的路由说明如下, 详细路由信息请参见表5-3。 <ul style="list-style-type: none"> <li>- 下一跳为对等连接: 表示通过Peer-A-T和Peer-B-T, 转发业务VPC-A和VPC-B之间的流量, 此处目的地址分别配置为VPC-A和VPC-B的网段。</li> <li>- 下一跳为企业路由器: 表示通过ER, 将业务VPC-A和VPC-B的流量转发至DC的虚拟网关, 再经过虚拟网关送达线下IDC, 此处目的地址配置为线下IDC网段。</li> </ul> </li> </ul>

资源	说明
DC	<ul style="list-style-type: none"> <li>1个物理连接：需要运营商施工搭建连通华为云和线下IDC的物理专线。</li> <li>1个虚拟网关：将虚拟网关接入ER中，即表示将“虚拟网关（VGW）”连接添加到ER。</li> <li>1个虚拟接口：连接虚拟网关和物理连接。</li> </ul>
ER	<p>在企业路由器中添加以下连接，并配置路由信息：</p> <ul style="list-style-type: none"> <li>VPC： <ul style="list-style-type: none"> <li>将1个“虚拟私有云（VPC）”连接关联至ER默认路由表，不开启“配置连接侧路由”，手动在VPC路由表中添加路由。</li> <li>在默认路由表中添加“虚拟私有云（VPC）”连接的路由，此处不使用传播自动学习路由，需要手动在ER路由表添加静态路由，路由信息如表5-4所示。</li> </ul> </li> <li>DC： <ul style="list-style-type: none"> <li>将1个“虚拟网关（VGW）”连接关联至ER默认路由表。</li> <li>在默认路由表中创建“虚拟网关（VGW）”连接的传播，路由自动学习DC侧的所有路由信息，路由信息如表5-4所示。</li> </ul> </li> </ul>
ECS	<p>每个业务VPC内各有1个ECS，本示例用该ECS来验证云上业务VPC之间、以及业务VPC和线下IDC的网络通信情况。</p> <p>如果您有多台ECS，并且这些ECS位于不同的安全组，需要在安全组中添加规则放通网络。</p>

表 5-3 VPC 路由表

VPC名称	目的地址	下一跳	路由类型
VPC-A	172.17.0.0/16	对等连接：Peer-A-T	静态路由：自定义
	10.10.0.0/16	对等连接：Peer-A-T	静态路由：自定义
VPC-B	172.16.0.0/16	对等连接：Peer-B-T	静态路由：自定义
	10.10.0.0/16	对等连接：Peer-B-T	静态路由：自定义
VPC-Transit	172.17.0.0/16	对等连接：Peer-B-T	静态路由：自定义
	172.16.0.0/16	对等连接：Peer-A-T	静态路由：自定义
	10.10.0.0/16	企业路由器：ER	静态路由：自定义

**须知**

在ER中添加VPC连接时，不开启“配置连接侧路由”选项，需要手动在VPC-Transit路由表中配置路由。

**表 5-4 ER 路由表**

目的地址	下一跳	路由类型
VPC-A网段： 172.16.0.0/16	VPC-T连接：er-attach-VPCtransit	静态路由
VPC-B网段： 172.17.0.0/16	VPC-T连接：er-attach-VPCtransit	静态路由
本端网关和远端网关： 10.0.0.0/30	VGW连接：vgw-demo	传播路由
IDC侧网段：10.10.0.0/16	VGW连接：vgw-demo	传播路由

## 资源规划说明

企业路由器ER、云专线DC、虚拟私有云VPC、弹性云服务器ECS只要位于同一个区域内即可，可用区可以任意选择，不用保持一致。

**说明**

以下资源规划详情仅为示例，您可以根据需要自行修改。

**表 5-5 企业路由器和中转 VPC 组网资源规划总体说明**

资源类型	说明
虚拟私有云VPC	<p>本示例中共创建3个VPC，资源规划示例如表5-6所示。</p> <ul style="list-style-type: none"> <li>业务VPC：2个，实际运行客户业务的VPC。业务VPC只需要和中转VPC建立对等连接，不需要接入ER中。</li> <li>中转VPC：1个，用于转发业务VPC之间、以及业务VPC和线下IDC之间的流量，该VPC下不建议运行任何业务。中转VPC需要接入ER中。</li> </ul> <p><b>须知</b></p> <ul style="list-style-type: none"> <li>业务VPC和中转VPC的网段与客户IDC侧网段不能重复。</li> <li>通过对等连接连通的VPC子网网段不能重叠，因此业务VPC和中转VPC的子网网段不允许重叠。</li> <li>由于中转VPC需要接入企业路由器，关于接入企业路由器的约束，更多详情请参见<a href="#">约束与限制</a>。</li> </ul>
VPC对等连接	<p>本示例中共创建2个对等连接，用于连通VPC-A、VPC-B和VPC-Transit之间的网络，资源规划示例如表5-7所示。</p>
云专线DC	<p>本示例中的DC包含1个物理连接，1个虚拟网关以及1个虚拟接口，资源规划示例如表5-8所示。</p>

资源类型	说明
企业路由器 ER	本示例中创建1个ER，并在ER中添加2个连接，资源规划示例如表5-9所示。
弹性云服务器 ECS	本示例共创建2个ECS，每个业务VPC内各有1个ECS，资源规划示例如表5-10所示。

表 5-6 VPC 资源规划详情

VPC名称	VPC网段	子网名称	子网网段	关联路由表	VPC说明
VPC-A	172.16.0.0/16	subnet-A01	172.16.1.0/24	默认路由表	业务VPC，不接入ER
VPC-B	172.17.0.0/16	subnet-B01	172.17.1.0/24	默认路由表	业务VPC，不接入ER
VPC-Transit	192.168.0.0/24	subnet-Transit	192.168.0.0/24	默认路由表	中转VPC，接入ER

表 5-7 VPC 对等连接资源规划详情

VPC对等连接名称	本端VPC	对端VPC	对等连接说明
Peer-A-T	VPC-A	VPC-Transit	连通VPC-A和VPC-Transit之间的网络
Peer-B-T	VPC-B	VPC-Transit	连通VPC-B和VPC-Transit之间的网络

表 5-8 DC 资源规划详情

资源类型	参数配置示例
物理连接	请根据实际需求创建。
虚拟网关	<ul style="list-style-type: none"> <li>名称：vgw-demo</li> <li>关联模式：企业路由器</li> <li>BGP ASN：此处AS号和企业路由器的AS号一样或者不一样均可，本示例中和ER的AS号一致，保持默认值64512。</li> </ul>

资源类型	参数配置示例
虚拟接口	<ul style="list-style-type: none"> <li>名称: vif-demo</li> <li>虚拟网关: vgw-demo</li> <li>本端网关: 10.0.0.1/30</li> <li>远端网关: 10.0.0.2/30</li> <li>远端子网: 10.10.0.0/16</li> <li>路由模式: BGP</li> <li>BGP邻居AS号: 此处为线下IDC侧的AS号, 不能和云上虚拟网关的AS号一样, 本示例为65525。</li> </ul>

表 5-9 ER 资源规划详情

资源类型	参数配置示例
企业路由器	<ul style="list-style-type: none"> <li>名称: er-demo</li> <li>AS号: 64512</li> <li>默认路由表关联: 开启</li> <li>默认路由表传播: 关闭。 您需要在ER路由表中手动添加“虚拟私有云(VPC)”连接的路由, 因此不能开启自动传播功能。</li> <li>自动接受共享连接: 开启 如果您要将不同账号下的VPC接入ER构建组网, 则建议您开启该功能, 具体请参见<a href="#">企业路由器的共享功能</a>。</li> <li>关联/传播路由表: 默认路由表</li> <li>连接名称: <ul style="list-style-type: none"> <li>er-attach-VPCtransit</li> <li>er-attach-VGW</li> </ul> </li> </ul>
企业路由器连接	<ul style="list-style-type: none"> <li>连接名称: er-attach-VPCtransit <ul style="list-style-type: none"> <li>连接类型: 虚拟私有云(VPC)</li> <li>VPC: VPC-Transit</li> <li>子网: subnet-Transit</li> <li>配置连接侧路由: 不开启。 开启该功能后, 会在VPC路由表中自动添加指向ER的路由, 目的地址固定为10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16。本示例需要添加业务VPC的网段地址作为路由目的地址, 因此需要手动添加。</li> </ul> </li> <li>连接名称: er-attach-VGW <ul style="list-style-type: none"> <li>连接类型: 虚拟网关(VGW)</li> <li>虚拟网关: vgw-demo</li> </ul> </li> </ul>

表 5-10 ECS 资源规划详情

ECS名称	VPC名称	子网名称	私有IP地址	镜像	安全组	ECS说明
ECS-A	VPC-A	subnet-A01	172.16.1.25	公共镜像：	sg-demo	运行业务的云服务器
ECS-B	VPC-B	subnet-B01	172.17.1.113	CentOS 8.2 64bit	通用Web服务器	运行业务的云服务器

## 5.3 通过企业路由器和中转 VPC 构建组网流程

本章节介绍通过企业路由器和中转VPC构建组网总体流程，流程说明如表5-11所示。

表 5-11 通过企业路由器和中转 VPC 构建组网流程说明

步骤	说明
<b>步骤一：创建云服务资源</b>	<ol style="list-style-type: none"><li>1. 创建1个企业路由器，构建一个同区域组网只需要1个企业路由器。</li><li>2. 创建VPC和子网，本示例中创建2个业务VPC和1个中转VPC。</li><li>3. 在VPC内，创建ECS，本示例中创建2个ECS。</li></ol>
<b>步骤二：创建对等连接并配置路由</b>	<ol style="list-style-type: none"><li>1. 创建业务VPC-A和中转VPC-Transit之间的对等连接，并添加路由。</li><li>2. 创建业务VPC-B和中转VPC-Transit之间的对等连接，并添加路由。</li><li>3. 验证业务VPC-A和业务VPC-B之间的通信情况。</li></ol>
<b>步骤三：在企业路由器中添加并配置VPC连接</b>	<ol style="list-style-type: none"><li>1. 在企业路由器中添加“虚拟私有云（VPC）”连接：将1个中转VPC接入企业路由器中。</li><li>2. 在VPC路由表中配置路由：在VPC路由表中添加指向企业路由器的路由信息，目的地址为IDC侧网段。</li><li>3. 在ER路由表中配置路由：在ER路由表中添加指向VPC连接的路由信息，目的地址分别为业务VPC网段。</li></ol>

步骤	说明
<b>步骤四：在企业路由器中添加并配置 VGW 连接</b>	<ol style="list-style-type: none"><li>1. 创建物理连接，物理连接是线下IDC侧和华为云的专属通道，需要运营商进行施工，搭建物理专线链路连接线下和云上。</li><li>2. 创建虚拟网关：创建1个关联企业路由器的虚拟网关，企业路由器中会自动添加“虚拟网关（VGW）”连接。</li><li>3. 在ER路由表中创建传播：在ER路由表中创建“虚拟网关（VGW）”连接的传播，会自动学习IDC侧的路由信息，不用再手动添加路由。</li><li>4. 创建虚拟接口：创建关联虚拟网关的虚拟接口，连接虚拟网关和物理连接。</li><li>5. 配置IDC侧路由：在线下IDC侧路由设备配置网络参数。</li></ol>
<b>步骤五：验证VPC和IDC的通信情况</b>	登录ECS，执行ping命令，验证网络互通情况。

## 5.4 通过企业路由器和中转 VPC 构建组网实施步骤

### 步骤一：创建云服务资源

本步骤指导您创建业务VPC、ECS以及ER服务资源，云服务资源的总体规划说明，请参见[表5-5](#)。

#### 步骤1 创建1个企业路由器。

企业路由器的“默认路由表传播”功能需要关闭，更多资源详情请参见[表5-9](#)。

创建企业路由器，具体方法请参见[创建企业路由器](#)。

#### 步骤2 创建业务VPC和中转VPC。

创建VPC及子网，具体方法请参见[创建虚拟私有云和子网](#)。

#### 步骤3 创建ECS。

本示例中ECS主要用于验证网络通信使用，数量和配置仅供参考，请您根据实际需要创建ECS。

创建ECS，具体方法请参见[自定义购买ECS](#)。

----结束

### 步骤二：创建对等连接并配置路由

#### 步骤1 创建业务VPC和中转VPC之间的对等连接。

1. 创建对等连接Peer-A-T，连通VPC-A和VPC-Transit。
2. 创建对等连接Peer-B-T，连通VPC-B和VPC-Transit。

VPC对等连接的资源详情规划请参见[表5-7](#)。

- 如果业务VPC和中转VPC位于同一个账户下，创建方法请参见：[创建相同账户下的对等连接](#)。

- 如果业务VPC和中转VPC位于不同的账户下，创建方法请参见：[创建不同账户下的对等连接](#)。

**步骤2** 在VPC-A、VPC-B和VPC-Transit的路由表中，依次添加下一跳为对等连接的路由。

配置路由信息，具体方法请参见[在VPC路由表中配置路由](#)。

本示例中添加[表5-3](#)中下一跳为对等连接的路由。

- 在VPC-A的路由表中，添加172.17.0.0/16和10.10.0.0/16两条路由。
- 在VPC-B的路由表中，添加172.16.0.0/16和10.10.0.0/16两条路由。
- 在VPC-Transit的路由表中，添加172.17.0.0/16和172.16.0.0/16两条路由。

**步骤3** 在弹性云服务器的远程登录窗口，执行以下步骤，验证VPC-A和VPC-B的网络通信情况。

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）。

1. 登录ECS-A，验证VPC-A与VPC-B是否可以通过对等连接通信。

**ping ECS-B的私有IP地址**

命令示例：

**ping 172.17.1.113**

回显类似如下信息，表示VPC-A与VPC-B通信正常。

```
[root@ECS-A ~]# ping 172.17.1.113
PING 172.17.1.113 (172.17.1.113) 56(84) bytes of data.
64 bytes from 172.17.1.113: icmp_seq=1 ttl=64 time=0.849 ms
64 bytes from 172.17.1.113: icmp_seq=2 ttl=64 time=0.455 ms
64 bytes from 172.17.1.113: icmp_seq=3 ttl=64 time=0.385 ms
64 bytes from 172.17.1.113: icmp_seq=4 ttl=64 time=0.372 ms
...
--- 172.17.1.113 ping statistics ---
```

2. 登录ECS-B，验证VPC-B与VPC-A是否可以通过对等连接通信。

**ping ECS-A的私有IP地址**

命令示例：

**ping 172.16.1.25**

回显类似如下信息，表示VPC-B与VPC-A通信正常。

```
[root@ECS-B ~]# ping 172.16.1.25
PING 172.16.1.25 (172.16.1.25) 56(84) bytes of data.
64 bytes from 172.16.1.25: icmp_seq=1 ttl=64 time=0.849 ms
64 bytes from 172.16.1.25: icmp_seq=2 ttl=64 time=0.455 ms
64 bytes from 172.16.1.25: icmp_seq=3 ttl=64 time=0.385 ms
64 bytes from 172.16.1.25: icmp_seq=4 ttl=64 time=0.372 ms
...
--- 172.16.1.25 ping statistics ---
```

----结束

## 步骤三：在企业路由器中添加并配置 VPC 连接

**步骤1** 将中转VPC接入企业路由器中。

添加连接时，不开启“配置连接侧路由”功能，更多资源详情请参见[表5-9](#)。

**须知**

开启该功能后，会在VPC路由表中自动添加指向ER的路由，目的地址固定为10.0.0.0/8，172.16.0.0/12，192.168.0.0/16。本示例需要添加业务VPC的网段地址作为路由目的地址，因此需要手动添加。

添加“虚拟私有云（VPC）”连接，具体方法请参见[在企业路由器中添加VPC连接](#)。

**步骤2** 在中转VPC路由表中，添加下一跳为ER的路由。

配置路由信息，具体方法请参见[在VPC路由表中配置路由](#)。

本示例中，在VPC-Transit的路由表中，添加[表5-3](#)中下一跳为ER，目的地址为10.10.0.0/16的路由。

**步骤3** 在ER路由表中，添加下一跳为VPC连接的静态路由。

创建静态路由，具体方法请参见[创建静态路由](#)。

本示例中，在er-demo的路由表中，添加[表5-4](#)中下一跳为VPC-T连接，目的地址分别为172.16.0.0/16和172.17.0.0/16的路由。

----结束

## 步骤四：在企业路由器中添加并配置 VGW 连接

本示例中，云专线DC资源的总体规划说明，请参见[表5-8](#)。

**步骤1** 创建物理连接。

创建方法，具体请参见[物理连接接入](#)。

**步骤2** 创建虚拟网关，即在企业路由器中添加“虚拟网关（VGW）”连接。

1. 在云专线管理控制台，创建虚拟网关。

具体方法请参见[步骤2：创建虚拟网关](#)。

2. 在企业路由器控制台，查看“虚拟网关（VGW）”连接的添加情况。

具体方法请参见[查看连接](#)。

“虚拟网关（VGW）”连接的状态“正常”，表示已成功接入企业路由器中。

由于本示例创建ER时，开启“默认路由表关联”，未开启“默认路由表传播”，因此添加完“虚拟网关（VGW）”连接后：

- 系统自动在ER默认路由表中创建关联，无需手动创建。
- 需要继续执行[步骤3](#)，手动创建传播。

**步骤3** 在ER路由表中，为“虚拟网关（VGW）”连接创建传播，自动学习IDC的路由信息。

创建传播，具体方法请参见[创建传播](#)。

需要执行以下步骤连通DC后，才可以在ER路由表中查看到IDC侧的路由信息。

**步骤4** 创建虚拟接口。

创建虚拟接口用来连接虚拟网关和线下IDC，具体方法请参见[步骤3：创建虚拟接口](#)。

**步骤5** 配置IDC侧路由到华为云的路由。

以华为网络设备为例，配置BGP路由：

```
bgp 65525
peer 10.0.0.1 as-number 64512
peer 10.0.0.1 password simple Qaz12345678
network 10.10.0.0 255.255.0.0
```

表 5-12 BGP 路由

命令	命令说明
<code>bgp 65525</code>	启动BGP，其中： 65525：IDC侧AS号。
<code>peer 10.0.0.1 as-number 64512</code>	创建BGP的对等体(EBGP)，其中： <ul style="list-style-type: none"><li>10.0.0.1：华为云侧网关。</li><li>64512：华为云侧AS号，固定为64512。</li></ul>
<code>peer 10.0.0.1 password simple Qaz12345678</code>	BGP对等体建立TCP连接时对BGP消息进行MD5认证，其中： Qaz12345678：BGP MD5认证密码。
<code>network 10.10.0.0 255.255.0.0</code>	将IP路由表中已存在的路由添加到BGP路由表中，其中： <ul style="list-style-type: none"><li>10.10.0.0：IDC侧子网。</li><li>255.255.0.0：IDC侧子网掩码。</li></ul>

----结束

## 步骤五：验证 VPC 和 IDC 的通信情况

**步骤1** 登录弹性云服务器，执行以下步骤，验证业务VPC与IDC通信情况。

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）。

1. 登录ECS-A，执行以下命令，验证VPC-A与IDC是否可以通过ER通信。

```
ping IDC侧任意一个IP地址
```

命令示例：

```
ping 10.10.0.27
```

回显类似如下信息，表示VPC-A与IDC可以通过ER通信。

```
[root@ECS-A ~]# ping 10.10.0.27
PING 10.10.0.27 (10.10.0.27) 56(84) bytes of data:
64 bytes from 10.10.0.27: icmp_seq=1 ttl=64 time=0.849 ms
64 bytes from 10.10.0.27: icmp_seq=2 ttl=64 time=0.455 ms
64 bytes from 10.10.0.27: icmp_seq=3 ttl=64 time=0.385 ms
64 bytes from 10.10.0.27: icmp_seq=4 ttl=64 time=0.372 ms
...
--- 10.10.0.27 ping statistics ---
```

2. 登录ECS-B，执行以下命令，验证VPC-B与IDC是否可以通过ER通信。

```
ping IDC侧任意一个IP地址
```

命令示例：

### ping 10.10.0.30

回显类似如下信息，表示VPC-B与IDC可以通过ER通信。

```
[root@ECS-B ~]# ping 10.10.0.30
PING 10.10.0.30 (10.10.0.30) 56(84) bytes of data.
64 bytes from 10.10.0.30: icmp_seq=1 ttl=64 time=0.849 ms
64 bytes from 10.10.0.30: icmp_seq=2 ttl=64 time=0.455 ms
64 bytes from 10.10.0.30: icmp_seq=3 ttl=64 time=0.385 ms
64 bytes from 10.10.0.30: icmp_seq=4 ttl=64 time=0.372 ms
...
--- 10.10.0.30 ping statistics ---
```

**步骤2** 登录弹性云服务器，执行以下步骤，验证业务VPC之间的通信情况。

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）。

1. 登录ECS-A，验证VPC-A与VPC-B是否可以通过对等连接通信。

### ping ECS-B的私有IP地址

命令示例：

### ping 172.17.1.113

回显类似如下信息，表示VPC-A与VPC-B通信正常。

```
[root@ECS-A ~]# ping 172.17.1.113
PING 172.17.1.113 (172.17.1.113) 56(84) bytes of data.
64 bytes from 172.17.1.113: icmp_seq=1 ttl=64 time=0.849 ms
64 bytes from 172.17.1.113: icmp_seq=2 ttl=64 time=0.455 ms
64 bytes from 172.17.1.113: icmp_seq=3 ttl=64 time=0.385 ms
64 bytes from 172.17.1.113: icmp_seq=4 ttl=64 time=0.372 ms
...
--- 172.17.1.113 ping statistics ---
```

2. 登录ECS-B，验证VPC-B与VPC-A是否可以通过对等连接通信。

### ping ECS-A的私有IP地址

命令示例：

### ping 172.16.1.25

回显类似如下信息，表示VPC-B与VPC-A通信正常。

```
[root@ECS-B ~]# ping 172.16.1.25
PING 172.16.1.25 (172.16.1.25) 56(84) bytes of data.
64 bytes from 172.16.1.25: icmp_seq=1 ttl=64 time=0.849 ms
64 bytes from 172.16.1.25: icmp_seq=2 ttl=64 time=0.455 ms
64 bytes from 172.16.1.25: icmp_seq=3 ttl=64 time=0.385 ms
64 bytes from 172.16.1.25: icmp_seq=4 ttl=64 time=0.372 ms
...
--- 172.16.1.25 ping statistics ---
```

----结束

# 6 通过企业路由器和云专线构建混合云组网 （全域接入网关 DGW）

## 6.1 方案概述

### 应用场景

云专线（Direct Connect，DC）用于搭建线下IDC和云上虚拟私有云（Virtual Private Cloud，VPC）之间高速、低时延、稳定安全的专属连接通道，您可以通过企业路由器和云专线的全域接入网关，构建满足企业通信的大规模混合云组网。

通过企业路由器，可以实现专线的动态选路和切换，多个专线链路之间形成负载均衡，有效扩展网络带宽，增加吞吐量，提升网络性能的同时保证高可靠性。

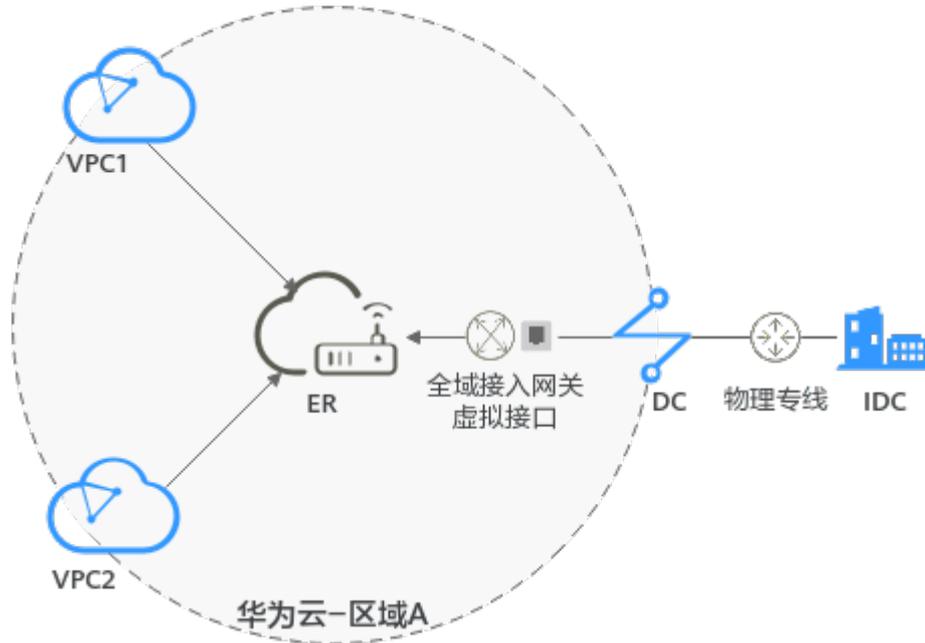
接下来，将主要为您介绍如何通过企业路由器和全域接入网关实现云上VPC和线下IDC网络互通。

### 方案架构

XX企业在华为云区域A内部署了2个虚拟私有云VPC，这2个VPC需要互相访问，并且通过DC全域接入网关和线下IDC网络互通。

在区域A内创建一个企业路由器ER，将VPC和DC的全域接入网关接入ER内，ER可以在接入的VPC和全域接入网关之间转发流量，构建混合云组网。

图 6-1 企业路由器和全域接入网关混合云组网



## 约束与限制

云上VPC子网网段与客户IDC侧子网网段不能重复。

## 6.2 组网和资源规划

通过企业路由器和DC的全域接入网关构建线下IDC和云上VPC互通的混合云组网，您需要规划组网和资源：

- **规划组网**：规划VPC及其子网的网段、专线的全域接入网关和虚拟接口、VPC路由表和ER路由表信息等。
- **规划资源**：规划云上资源的数量、名称以及主要参数等信息，云上资源包括VPC、DC、ECS以及ER。

## 规划组网

企业路由器和全域接入网关混合云组网规划如图6-2所示，将2个VPC和1个DGW网关接入ER中，组网规划说明如表6-2所示。

图 6-2 企业路由器和全域接入网关混合云组网规划

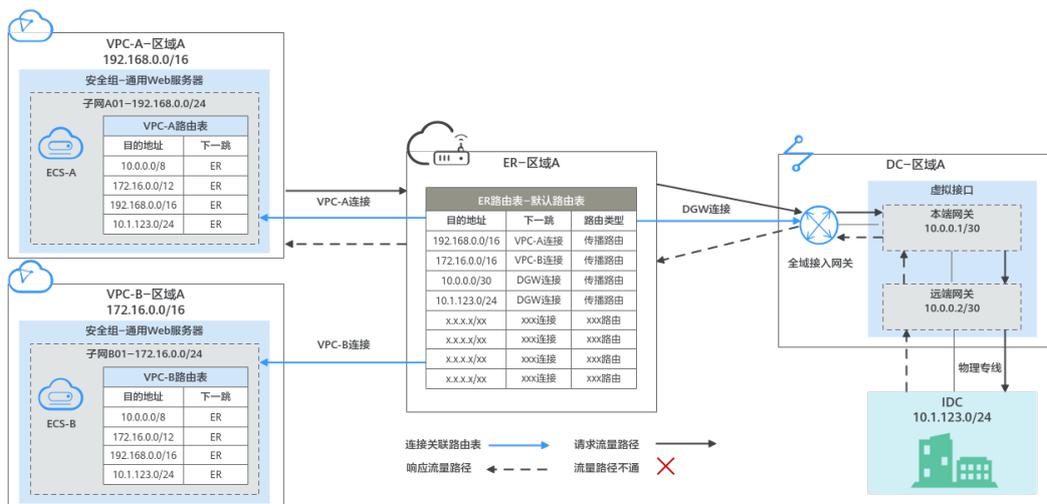


表 6-1 网络流量路径说明

路径	说明
请求路径： VPC-A → 线下IDC	<ol style="list-style-type: none"> <li>1. 在VPC-A路由表中，通过下一跳为ER的路由将流量转送到ER。</li> <li>2. 在ER路由表中，通过下一跳为DGW连接的路由将流量转送到全域接入网关。</li> <li>3. 全域接入网关连接虚拟接口，通过虚拟接口将流量从远端网关转送到物理专线。</li> <li>4. 通过物理专线将流量送达线下IDC。</li> </ol>
响应路径： 线下IDC → VPC-A	<ol style="list-style-type: none"> <li>1. 通过物理专线将流量转送到虚拟接口。</li> <li>2. 虚拟接口连接全域接入网关，通过虚拟接口将流量从本端网关转送到全域接入网关。</li> <li>3. 通过全域接入网关将流量转送到ER。</li> <li>4. 在ER路由表中，通过下一跳为VPC-A连接的路由将流量送达VPC-A。</li> </ol>

表 6-2 企业路由器和全域接入网关混合云组网规划说明

资源	说明
VPC	<p>业务VPC，实际运行客户业务的VPC，具体说明如下：</p> <ul style="list-style-type: none"><li>● VPC网段（CIDR）不能重叠。 本示例中，ER路由表使用的是“虚拟私有云（VPC）”连接的传播路由，由ER自动学习VPC网段作为目的地址，不支持修改，因此重叠的VPC网段会导致路由冲突。<p>如果您已有的VPC存在网段重叠，则不建议您使用传播路由，请在ER路由表中手动添加静态路由，目的地址可以为VPC子网网段或者范围更小的网段。</p><li>● VPC网段与客户IDC侧网段不能重复。</li><li>● VPC有一个默认路由表。</li><li>● VPC默认路由表中的路由信息如表6-3所示。</li></li></ul> <ul style="list-style-type: none"><li>- 固定网段：10.0.0.0/8、172.16.0.0/12、192.168.0.0/16三个固定网段是添加VPC连接时，开启“配置连接侧路由”选项，系统自动在VPC路由表配置的静态路由。如果ER内同时接入多个VPC连接，则这些路由可以将当前VPC访问其他VPC的路由转发至ER，再通过ER将流量转发至下一跳网络实例。</li><li>- 线下IDC侧网段：除了系统自动添加的3个VPC固定网段，您还需要在VPC路由表中添加目的地址为IDC侧网段，下一跳指向ER的路由，本示例为10.1.123.0/24，该路由可以将VPC访问线下IDC侧的流量转发至ER，再通过ER将流量转发至下一跳网络实例。</li></ul> <p><b>须知</b> 如果VPC路由表中的路由与这三个固定网段冲突，则会添加失败。此时建议您不要开启“配置连接侧路由”选项，并在连接创建完成后，手动添加路由。</p>
DC	<ul style="list-style-type: none"><li>● 1个物理连接：需要运营商施工搭建连通华为云和线下IDC的物理专线。</li><li>● 1个全域接入网关：将全域接入网关接入ER中，即表示将“全域接入网关（DGW）”连接添加到ER。</li><li>● 1个虚拟接口：连接全域接入网关和物理连接。</li></ul>
ER	<p>开启“默认路由表关联”和“默认路由表传播”功能，添加完“全域接入网关（DGW）”连接和“虚拟私有云（VPC）”连接，系统会自动执行以下配置：</p> <ul style="list-style-type: none"><li>● DC：<ul style="list-style-type: none"><li>- 将1个“全域接入网关（DGW）”连接关联至ER默认路由表。</li><li>- 在默认路由表中创建“全域接入网关（DGW）”连接的传播，路由自动学习DC侧的所有路由信息，包括本端网关和远端网关、IDC侧网段等信息，路由信息如表6-4所示。</li></ul></li><li>● VPC：<ul style="list-style-type: none"><li>- 将2个“虚拟私有云（VPC）”连接关联至ER默认路由表。</li><li>- 在默认路由表中创建“虚拟私有云（VPC）”连接的传播，路由自动学习VPC网段，路由信息如表6-4所示。</li></ul></li></ul>

资源	说明
ECS	2个ECS分别位于不同的VPC内，VPC中的ECS如果位于不同的安全组，需要在安全组中添加规则放通网络。

表 6-3 VPC 路由表

目的地址	下一跳	路由类型
固定网段：10.0.0.0/8	企业路由器	静态路由：自定义
固定网段：172.16.0.0/12	企业路由器	静态路由：自定义
固定网段： 192.168.0.0/16	企业路由器	静态路由：自定义
线下IDC侧网段： 10.1.123.0/24	企业路由器	静态路由：自定义

#### 📖 说明

- 如果您在创建连接时开启“配置连接侧路由”选项，则不用手动在VPC路由表中配置静态路由，系统会在VPC的所有路由表中自动添加指向ER的路由，目的地址固定为10.0.0.0/8，172.16.0.0/12，192.168.0.0/16。
- 如果VPC路由表中的路由与这三个固定网段冲突，则会添加失败。此时建议您不要开启“配置连接侧路由”选项，并在连接创建完成后，手动添加路由。
- 除了系统自动添加的3个VPC固定网段，您还需要在VPC路由表中添加目的地址为IDC侧网段，下一跳指向ER的路由。

表 6-4 ER 路由表

目的地址	下一跳	路由类型
VPC-A网段： 192.168.0.0/16	VPC-A连接：er-attach- vpc-A	传播路由
VPC-B网段： 172.16.0.0/16	VPC-B连接：er-attach- vpc-B	传播路由
本端网关和远端网关： 10.0.0.0/30	DGW连接：er-attach- dgw	传播路由
IDC侧网段： 10.1.123.0/24	DGW连接：er-attach- dgw	传播路由

## 规划资源

企业路由器ER、云专线DC、虚拟私有云VPC、弹性云服务器ECS只要位于同一个区域内即可，可用区可以任意选择，不用保持一致。

 说明

以下资源规划详情仅为示例，您可以根据需要自行修改。

表 6-5 DC 双链路负载混合云组网资源规划总体说明

资源类型	资源数量	说明
VPC	2	<p>业务VPC，实际运行客户业务的VPC，需要接入ER中。</p> <ul style="list-style-type: none"> <li>• VPC名称：请根据实际情况填写，本示例为vpc-A和vpc-B。</li> <li>• IPv4网段：VPC网段与客户IDC侧网段不能重复，请根据实际情况填写，本示例vpc-A为192.168.0.0/16，vpc-B为172.16.0.0/16。</li> <li>• 子网名称：请根据实际情况填写，本示例为subnet-A01和subnet-B01。</li> <li>• 子网IPv4网段：VPC子网网段与客户IDC侧子网网段不能重复，请根据实际情况填写，本示例subnet-A01为192.168.0.0/24，subnet-B01为172.16.0.0/24。</li> </ul>
ER	1	<ul style="list-style-type: none"> <li>• 名称：请根据实际情况填写，本示例为er-X。</li> <li>• ASN：企业路由器不能和线下IDC的AS号一样，且建议企业路由器和全域接入网关的AS号也不一样，由于64512是全域接入网关的系统预留AS号，因此本示例企业路由器的AS号为64513。</li> <li>• 默认路由表关联：开启</li> <li>• 默认路由表传播：开启</li> <li>• 自动接受共享连接：请根据实际情况选择，本示例选择“开启”。</li> <li>• 连接，本示例需要在企业路由器中添加3个连接： <ul style="list-style-type: none"> <li>- VPC-A连接：er-attach-vpc-A</li> <li>- VPC-B连接：er-attach-vpc-B</li> <li>- DGW连接：er-attach-dgw</li> </ul> </li> </ul>
DC	1	<p>物理连接：请根据实际需求创建。 本示例中，1个物理连接为dc-X。</p> <p>全域接入网关，请根据实际需求创建，本示例说明如下：</p> <ul style="list-style-type: none"> <li>• 名称：请根据实际情况填写，本示例为dgv-X。</li> <li>• BGP ASN：建议全域接入网关和企业路由器的AS号不一样，本示例中全域接入网关的AS号为64512。</li> <li>• 地址类型：请根据实际情况选择，本示例为IPv4。</li> </ul>

资源类型	资源数量	说明
		<p>虚拟接口，请根据实际需求创建，本示例说明如下：</p> <ul style="list-style-type: none"><li>● 名称：本示例虚拟接口为vif-X。</li><li>● 虚拟接口优先级：此处请选择“优先”。</li><li>● 物理连接：本示例中虚拟接口vif-X关联的物理连接为dc-X。</li><li>● 全域接入网关：本示例中虚拟接口vif-X关联的全域接入网关为dgw-X。</li><li>● 本端网关：本示例为10.0.0.1/30。</li><li>● 远端网关：本示例为10.0.0.2/30。</li><li>● 远端子网：此处为IDC侧子网网段，本示例为10.1.123.0/24。</li><li>● 路由模式：请选择“BGP”。</li><li>● BGP邻居AS号：此处为线下IDC侧的AS号，不能和云上全域接入网关、ER等服务的AS号一样，本示例为64515。</li></ul>
		<p>关联实例，即将全域接入网关加入到企业路由器中，请根据实际需求创建，本示例说明如下：</p> <ul style="list-style-type: none"><li>● 实例类型：此处请选择“连接”。</li><li>● 连接名称：请根据实际情况填写，本示例为er-attach-dgw。</li><li>● 连接类型：此处请选择“企业路由器”。</li><li>● 连接资源：选择您的企业路由器，本示例为er-X。</li></ul>
ECS	2	<p>ECS主要用来验证网络通信情况，本示例如下：</p> <ul style="list-style-type: none"><li>● 名称：根据实际情况填写，本示例分别为ecs-A和ecs-B。</li><li>● 镜像：请根据实际情况选择，本示例为公共镜像（CentOS 8.2 64bit）。</li><li>● 网络：<ul style="list-style-type: none"><li>- 虚拟私有云：选择业务VPC，本示例为ecs-A选择vpc-A，ecs-B选择vpc-B。</li><li>- 子网：选择和线下IDC通信的子网，本示例为ecs-A选择subnet-A01，ecs-B选择subnet-B01。</li></ul></li><li>● 安全组：请根据实际情况选择，本示例安全组模板选择“通用Web服务器”，名称为sg-demo。</li><li>● 私有IP地址：本示例中，ecs-A为192.168.1.99，ecs-B为172.16.1.137。</li></ul>

## 6.3 企业路由器和全域接入网关混合云组网构建流程

本文档介绍如何通过企业路由器和DC的全域接入网关构建线下IDC和云上VPC互通的混合云组网，流程如图6-3所示。

图 6-3 企业路由器和全域接入网关混合云组网构建流程图

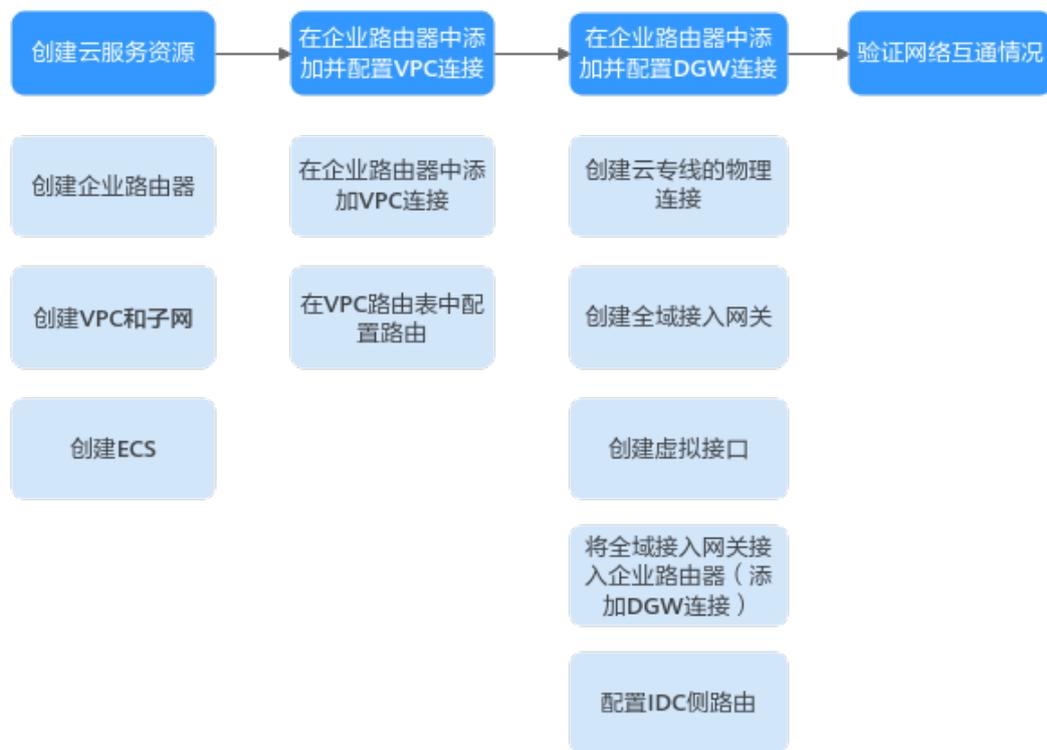


表 6-6 企业路由器和全域接入网关混合云组网构建流程说明

步骤	说明
<b>步骤一：创建云服务资源</b>	1. 创建1个企业路由器，构建一个同区域组网只需要1个企业路由器。 2. 创建业务VPC和子网，本示例中创建2个VPC和子网。 3. 在业务VPC子网内，创建ECS，本示例中创建2个ECS。
<b>步骤二：在企业路由器中添加并配置VPC连接</b>	1. 在企业路由器中添加“虚拟私有云（VPC）”连接：分别将2个业务VPC接入企业路由器中。 2. 在VPC路由表中配置路由：分别在两个VPC的路由表中配置到企业路由器的路由信息，目的地址为IDC侧网段。
<b>步骤三：在企业路由器中添加并配置DGW连接</b>	1. 创建1个物理连接：物理连接是线下IDC侧和华为云的专属通道，需要运营商进行施工，搭建物理专线链路连接线下和云上。 2. 创建1个全域接入网关：创建1个全域接入网关。 3. 创建1个虚拟接口：虚拟接口用来连接全域接入网关和物理连接。 4. 将全域接入网关接入企业路由器：接入后，在企业路由器的连接列表中可以查看“全域接入网关（DGW）”连接。 5. 配置IDC侧路由：在线下IDC侧路由设备配置网络参数。
<b>步骤四：验证网络通信情况</b>	登录ECS，执行ping命令，验证VPC和DC链路通信情况。

## 6.4 企业路由器和全域接入网关混合云组网构建步骤

### 步骤一：创建云服务资源（业务 VPC、ECS、ER）

本步骤指导您创建业务VPC、ECS以及ER服务资源，云服务资源的总体规划说明，请参见[表6-5](#)。

#### 步骤1 创建企业路由器。

创建企业路由器，具体方法请参见[创建企业路由器](#)。

#### 步骤2 创建业务VPC。

创建VPC及子网，具体方法请参见[创建虚拟私有云和子网](#)。

#### 步骤3 创建业务ECS。

本示例中2个业务ECS主要用于验证云上VPC和线下IDC通信使用，数量和配置仅供参考，请您根据实际需要创建业务ECS。

创建ECS，具体方法请参见[自定义购买ECS](#)。

----结束

### 步骤二：在企业路由器中添加并配置 VPC 连接

#### 步骤1 分别将2个业务VPC接入企业路由器中。

添加“虚拟私有云（VPC）”连接，具体方法请参见[在企业路由器中添加VPC连接](#)。

#### 步骤2 检查ER路由表中指向VPC连接的路由。

本示例中，ER开启了“默认路由表关联”和“默认路由表传播”功能，那么在ER中添加“虚拟私有云（VPC）”连接时，系统会自动添加ER指向VPC的路由，无需手动添加，只需要检查即可。

ER路由规划详情，请参见[表6-2](#)和[表6-4](#)，本示例中两条路由的下一跳分别为VPC-A连接和VPC-B连接。

查看ER路由，具体方法请参见[查看路由](#)。

#### 步骤3 在2个业务VPC的路由表中，分别添加指向ER，目的地址为线下IDC网段的路由。

VPC路由规划详情，请参见[表6-3](#)，本示例添加目的地址为10.1.123.0/24的路由。

配置路由信息，具体方法请参见[在VPC路由表中配置路由](#)。

----结束

### 步骤三：在企业路由器中添加并配置 DGW 连接

本示例中，云专线DC资源的总体规划说明，请参见[表6-5](#)。

#### 步骤1 创建物理连接。

创建方法，具体请参见[物理连接接入](#)。

**步骤2** 在企业路由器中添加“全域接入网关（DGW）”连接。

1. 在云专线管理控制台，执行以下操作：
  - a. 创建全域接入网关。
  - b. 创建虚拟接口。
  - c. 将全域接入网关接入企业路由器，即添加“全域接入网关（DGW）”连接。

具体方法请参见[创建全域接入网关](#)。

2. 在企业路由器控制台，查看“全域接入网关（DGW）”连接的添加情况。  
具体方法请参见[查看连接](#)。

“全域接入网关（DGW）”连接的状态“正常”，表示已成功接入企业路由器中。

由于本示例创建ER时，开启“默认路由表关联”和“默认路由表传播”，因此添加完“全域接入网关（DGW）”连接后，以下均为系统自动配置：

- 在ER默认路由表中创建关联。
- 在ER默认路由表中创建传播，并自动学习IDC侧的路由信息。  
需要执行以下步骤连通DC后，才可以在ER路由表中查看到IDC侧的路由信息。

**步骤3** 配置IDC侧路由到华为云的路由。

以华为网络设备为例，配置BGP路由：

```
bgp 64515
peer 10.0.0.1 as-number 64512
peer 10.0.0.1 password simple Qaz12345678
network 10.1.123.0 255.255.255.0
```

**表 6-7** BGP 路由

命令	命令说明
<code>bgp 64515</code>	启动BGP，其中： 64515：IDC侧AS号。
<code>peer 10.0.0.1 as-number 64512</code>	创建BGP的对等体(EBGP)，其中： <ul style="list-style-type: none"><li>● 10.0.0.1：华为云侧网关。</li><li>● 64512：全域接入网关的BGP ASN。</li></ul>
<code>peer 10.0.0.1 password simple Qaz12345678</code>	BGP对等体建立TCP连接时对BGP消息进行MD5认证，其中： Qaz12345678：BGP MD5认证密码。
<code>network 10.1.123.0 255.255.255.0</code>	将IP路由表中已存在的路由添加到BGP路由表中，其中： <ul style="list-style-type: none"><li>● 10.1.123.0：IDC侧子网。</li><li>● 255.255.255.0：IDC侧子网掩码。</li></ul>

----结束

## 步骤四：验证网络通信情况

### 步骤1 登录弹性云服务器。

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）。

### 步骤2 在弹性云服务器的远程登录窗口，执行以下命令，验证网络互通情况。

1. 执行以下命令，验证VPC之间的网络互通情况。

**ping 弹性云服务器IP地址**

以登录ecs-A，验证vpc-A与vpc-B的网络互通情况为例：

**ping 172.16.1.137**

回显类似如下信息，表示vpc-A与vpc-B可以通过ER通信。

```
[root@ecs-A ~]# ping 172.16.1.137
PING 172.16.1.137 (172.16.1.137) 56(84) bytes of data.
64 bytes from 172.16.1.137: icmp_seq=1 ttl=64 time=0.849 ms
64 bytes from 172.16.1.137: icmp_seq=2 ttl=64 time=0.455 ms
64 bytes from 172.16.1.137: icmp_seq=3 ttl=64 time=0.385 ms
64 bytes from 172.16.1.137: icmp_seq=4 ttl=64 time=0.372 ms
...
--- 172.16.1.137 ping statistics ---
```

2. 执行以下命令，验证VPC和DC网络互通情况。

**ping 本端网关（华为云侧）地址**

**ping 远端网关（IDC侧）地址**

**ping IDC侧IP地址**

以登录ecs-A，验证vpc-A与本端网关（华为云侧）的网络互通情况为例：

**ping 10.0.0.1**

回显如下信息，表示VPC与本端网关（华为云侧）的网络已通。

```
[root@ecs-A ~]# ping 10.0.0.1
PING 10.0.0.1 (10.0.0.1) 56(84) bytes of data.
64 bytes from 10.0.0.1: icmp_seq=1 ttl=64 time=0.849 ms
64 bytes from 10.0.0.1: icmp_seq=2 ttl=64 time=0.455 ms
64 bytes from 10.0.0.1: icmp_seq=3 ttl=64 time=0.385 ms
64 bytes from 10.0.0.1: icmp_seq=4 ttl=64 time=0.372 ms
...
--- 10.0.0.1 ping statistics ---
```

### 步骤3 重复执行步骤1~步骤2，验证其他VPC和DC之间的网络互通情况。

----结束

# 7 通过企业路由器构建 DC 双链路负载混合云组网（全域接入网关 DGW）

## 7.1 DC 双链路负载混合云组网方案概述

### 应用场景

云专线（Direct Connect，DC）用于搭建线下IDC和云上虚拟私有云（Virtual Private Cloud，VPC）之间高速、低时延、稳定安全的专属连接通道，您可以通过企业路由器和云专线的全域接入网关，构建满足企业通信的大规模混合云组网。

通过企业路由器，可以实现专线的动态选路和切换，多个专线链路之间形成负载均衡，有效扩展网络带宽，增加吞吐量，提升网络性能的同时保证高可靠性。

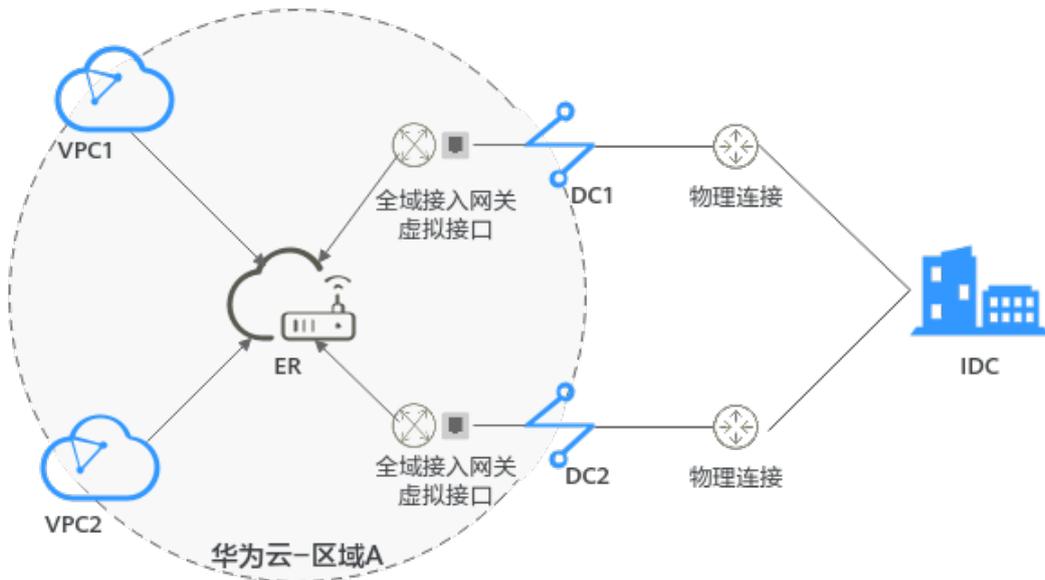
接下来，将主要为您介绍如何通过企业路由器和全域接入网关，构建DC双链路负载混合云组网。

### 方案架构

为了提升混合云组网的网络性能以及可靠性，XX企业同时部署了两条专线DC链路，均可以连通云上VPC和线下IDC的网络。两条DC链路形成负载均衡，当两条DC链路网络均正常，同时工作可提升网络传输能力。当其中一条DC链路故障时，另外一条DC链路可确保整个混合云组网的正常运行，避免了单点故障带来的业务中断。

- 将VPC1、VPC2以及DC接入企业路由器中，VPC1和VPC2网络互通，并且均可以通过两条DC和线下IDC通信。
- 当其中一条DC链路故障时，VPC1和VPC2可以通过另外一条DC链路和线下IDC通信。

图 7-1 DC 双链路负载混合云组网(全域接入网关 DGW)



### 方案优势

通过企业路由器和全域接入网关，可以实现DC双链路负载模式，提升混合云组网的网络性能和高可靠性，避免网络链路单点故障时业务受损。

### 约束与限制

云上VPC子网网段与客户IDC侧子网网段不能重复。

## 7.2 DC 双链路负载混合云组网和资源规划

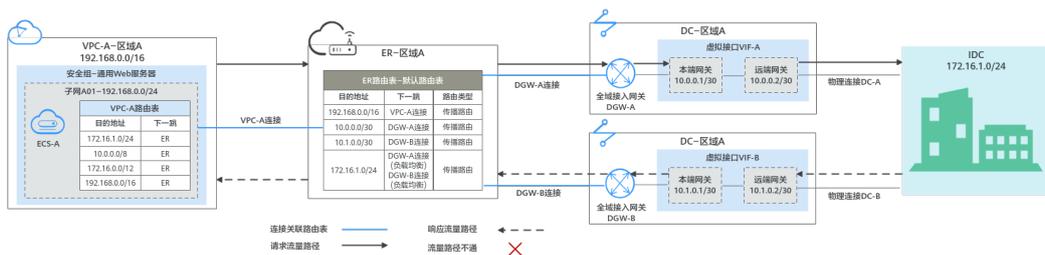
通过企业路由器构建DC双链路负载混合云组网，您需要规划资源和组网，本示例中为您详细介绍资源和组网情况。

- **网络规划说明**：规划VPC及其子网、DC和ER的网段、路由等。
- **资源规划说明**：规划云上资源的数量、名称以及主要参数等信息，云上资源包括VPC、DC以及ER等。

### 网络规划说明

DC双链路负载混合云组网规划如图7-2所示，将VPC、DC分别接入ER中，组网规划说明如表7-2所示。

图 7-2 DC 双链路负载混合云组网规划(全域接入网关 DGW)



两条DC网络链路形成负载均衡，云上VPC和线下IDC通信时，两条链路同时处于工作状态，表7-1为您详细介绍网络流量路径。

表 7-1 网络流量路径说明(全域接入网关 DGW )

路径	说明
请求路径： VPC-A → 线 下IDC	<ol style="list-style-type: none"><li>1. 在VPC-A路由表中，通过下一跳为ER的路由将流量转送到ER。</li><li>2. 在ER路由表中，通过下一跳为DGW-A连接的路由将流量转送到全域接入网关DGW-A。<ul style="list-style-type: none"><li>• 下一跳为DGW-A的路由，其中172.16.1.0/24为线下IDC子网网段地址，10.0.0.0/30为虚拟接口VIF-A的网关地址。</li><li>• 目的地址为172.16.1.0/24的路由，下一跳对应DGW-A和DGW-B，两条路由为等价路由，形成负载均衡。流量根据哈希算法，选择一条网络链路，此处以选择DGW-A，即DC-A为例。</li></ul></li><li>3. 全域接入网关DGW-A连接虚拟接口VIF-A，通过虚拟接口将流量从远端网关转送到物理连接。</li><li>4. 通过物理连接DC-A将流量送达线下IDC。</li></ol>
响应路径： 线下IDC → VPC-A	<ol style="list-style-type: none"><li>1. 根据线下IDC网络的路由配置，通过物理连接DC-B将流量转送到虚拟接口VIF-B。 线下IDC内网络中，指向云上的路由也配置成等价路由，形成负载均衡。返回云上VPC的流量，根据哈希算法选择一条网络链路，此处以选择DC-B为例。</li><li>2. 虚拟接口VIF-B连接全域接入网关DGW-B，通过虚拟接口将流量从本端网关转送到全域接入网关。</li><li>3. 通过全域接入网关DGW-B将流量转送到ER。</li><li>4. 在ER路由表中，通过下一跳为VPC-A连接的路由将流量送达VPC-A。</li></ol>

表 7-2 DC 双链路负载混合云组网规划说明(全域接入网关 DGW)

资源	说明
VPC	<p>业务VPC，实际运行客户业务的VPC，具体说明如下：</p> <ul style="list-style-type: none"> <li>● VPC网段与客户IDC侧网段不能重复。</li> <li>● VPC有一个默认路由表。</li> <li>● VPC默认路由表中的路由信息如表7-3所示。 <ul style="list-style-type: none"> <li>- 固定网段：10.0.0.0/8、172.16.0.0/12、192.168.0.0/16三个固定网段是添加VPC连接时，开启“配置连接侧路由”选项，系统自动在VPC路由表配置的静态路由。如果ER内同时接入多个VPC连接，则这些路由可以将当前VPC访问其他VPC的流量转发至ER，再通过ER将流量转发至下一跳网络实例。</li> <li>- 线下IDC侧网段：除了系统自动添加的3个VPC固定网段，您还需要在VPC路由表中添加目的地址为IDC侧网段，下一跳指向ER的路由，本示例为172.16.1.0/24，该路由可以将VPC访问线下IDC侧的流量转发至ER，再通过ER将流量转发至下一跳网络实例。</li> </ul> </li> </ul> <p><b>须知</b> 如果VPC路由表中的路由与这三个固定网段冲突，则会添加失败。此时建议您不要开启“配置连接侧路由”选项，并在连接创建完成后，手动添加路由。</p>
DC	<p>两个DC需要构建负载均衡网络链路，具体如下：</p> <ul style="list-style-type: none"> <li>● 2个物理连接：需要运营商施工搭建连通华为云和线下IDC的物理专线。</li> <li>● 2个全域接入网关：将两个全域接入网关分别接入ER中，即表示将“全域接入网关（DGW）”连接添加到ER。</li> <li>● 2个虚拟接口：分别连接两个全域接入网关和物理连接，两个虚拟接口之间形成负载分担。</li> </ul>
ER	<p>开启“默认路由表关联”和“默认路由表传播”功能，添加完连接后，系统会自动执行以下配置：</p> <ul style="list-style-type: none"> <li>● VPC： <ul style="list-style-type: none"> <li>- 将1个“虚拟私有云（VPC）”连接关联至ER默认路由表。</li> <li>- 在默认路由表中创建“虚拟私有云（VPC）”连接的传播，路由自动学习VPC网段，路由信息如表7-4所示。</li> </ul> </li> <li>● DC： <ul style="list-style-type: none"> <li>- 将2个“全域接入网关（DGW）”连接关联至ER默认路由表。</li> <li>- 在默认路由表中创建“全域接入网关（DGW）”连接的传播，路由自动学习IDC侧的所有BGP路由信息，路由信息如表7-4所示。</li> </ul> </li> </ul>

资源	说明
路由策略	<ul style="list-style-type: none"> <li>如果ER通过两个DGW连接学习的IDC侧的BGP路由是等价路由，自动形成负载均衡，则您无需创建路由策略。 本示例的表7-4中，目的地址为172.16.1.0/24，下一跳为DGW-A连接和DGW-B连接的两条路由是等价路由。</li> <li>如果ER通过两个DGW连接学习的IDC侧的BGP路由不是等价路由，无法自动形成负载均衡。则您需要在两个DGW连接的传播上，分别绑定路由策略。通过替换路由的AS_Path，将ER通过DGW连接去往IDC侧的路由形成等价路由。 您需要创建一个路由策略，添加两个节点： <ul style="list-style-type: none"> <li>策略节点1：优先级高，匹配BGP路由，对于匹配成功的路由，将路由的AS_Path值替换成全域接入网关的BGP ASN值。</li> <li>策略节点2：优先级低，匹配所有路由，此条节点是确保其他非BGP路由正常通信。</li> </ul> </li> </ul> <p>关于路由策略的详细说明，请您参见<a href="#">路由策略概述</a>。</p> <p><b>须知</b> 配置路由策略，替换路由的AS_Path值，可能会导致网络环路，因此配置前请检查网络规划，根据实际情况谨慎配置。</p>
ECS	<p>1个ECS位于业务VPC内，本示例用该ECS来验证云上和线下IDC的网络通信情况。</p> <p>如果您有多台ECS，并且这些ECS位于不同的安全组，需要在安全组中添加规则放通网络。</p>
IDC侧	<p>需要根据线下IDC侧网络的实际规划，将IDC侧去往云上ER的路由配置成等价路由，形成负载均衡。</p>

表 7-3 VPC 路由表

目的地址	下一跳	路由类型
固定网段：10.0.0.0/8	企业路由器	静态路由：自定义
固定网段： 172.16.0.0/12	企业路由器	静态路由：自定义
固定网段： 192.168.0.0/16	企业路由器	静态路由：自定义
线下IDC侧网段： 172.16.1.0/24	企业路由器	静态路由：自定义

表 7-4 ER 路由表

目的地址	下一跳	路由类型
VPC-A网段： 192.168.0.0/16	VPC-A连接：er-attach-vpc-A	传播路由

目的地址	下一跳	路由类型
VIF-A网关：10.0.0.0/30	DGW-A连接：er-attach-dgw-A	传播路由
VIF-B网关：10.1.0.0/30	DGW-B连接：er-attach-dgw-B	传播路由
IDC侧网段： 172.16.1.0/24	该路由为等价路由，两个连接属于 负载均衡模式。 <ul style="list-style-type: none"> <li>DGW-A连接：er-attach-dgw-A</li> <li>DGW-B连接：er-attach-dgw-B</li> </ul>	传播路由

## 资源规划说明

企业路由器ER、云专线DC、虚拟私有云VPC、弹性云服务器ECS只要位于同一个区域内即可，可用区可以任意选择，不用保持一致。

### 说明

以下资源规划详情仅为示例，您可以根据需要自行修改。

表 7-5 DC 双链路负载混合云组网资源规划总体说明(全域接入网关 DGW )

资源类型	资源数量	说明
VPC	1	<p>业务VPC，实际运行客户业务的VPC，需要接入ER中。</p> <ul style="list-style-type: none"> <li>VPC名称：请根据实际情况填写，本示例为vpc-A。</li> <li>IPv4网段：VPC网段与客户IDC侧网段不能重复，请根据实际情况填写，本示例为192.168.0.0/16。</li> <li>子网名称：请根据实际情况填写，本示例为subnet-A01。</li> <li>子网IPv4网段：VPC子网网段与客户IDC侧子网网段不能重复，请根据实际情况填写，本示例为192.168.0.0/24。</li> </ul>
ER	1	<ul style="list-style-type: none"> <li>名称：请根据实际情况填写，本示例为er-X。</li> <li>ASN：企业路由器不能和线下IDC的AS号一样，且建议企业路由器和全域接入网关的AS号也不一样，由于64512是全域接入网关的系统预留AS号，因此本示例企业路由器的AS号为64513。</li> <li>默认路由表关联：开启</li> <li>默认路由表传播：开启</li> <li>自动接受共享连接：请根据实际情况选择，本示例选择“开启”。</li> <li>连接，本示例需要在企业路由器中添加3个连接： <ul style="list-style-type: none"> <li>VPC-A连接：er-attach-vpc-A</li> <li>DGW-A连接：er-attach-dgw-A</li> <li>DGW-B连接：er-attach-dgw-B</li> </ul> </li> </ul>

资源类型	资源数量	说明
路由策略	1	<p>如果ER通过两个DGW连接学习的IDC侧的BGP路由不是等价路由，无法自动形成负载均衡，则需要配置路由策略，为DGW-A连接和DGW-B连接分别绑定路由策略。</p> <p>路由策略中需要添加两个路由策略节点，本示例如下：</p> <ul style="list-style-type: none"> <li>策略节点1：优先级高，对于BGP路由，替换路由的AS_Path，将ER通过两个DGW连接学习到的路由配置成等价路由。 <ul style="list-style-type: none"> <li>节点号：节点号取值小的策略节点优先执行，因此策略节点1的节点号取值必须小于策略节点2，此处填写10。</li> <li>匹配模式：此处设置成“允许”。</li> <li>匹配条件：此处设置成“路由类型”、“BGP路由”。</li> <li>策略值1：此处设置成“AS_Path”。</li> <li>执行动作：此处设置成“替换”，替换值和全域接入网关的BGP ASN保持一致，请根据实际填写，本示例为“64512”。</li> </ul> </li> <li>策略节点2：优先级低，匹配所有路由，此条节点是确保其他非BGP路由正常通信。 <ul style="list-style-type: none"> <li>节点号：策略节点2的节点号取值必须大于策略节点1，此处填写20。</li> <li>匹配模式：此处设置成“允许”。</li> </ul> </li> </ul> <p>其他参数不填写，为空即可，表示未匹配上策略节点1的其他路由均可以匹配上策略节点2，确保路由策略可放行所有路由。</p>
DC	2	<p>物理连接：请根据实际需求创建。</p> <p>本示例中，两个物理连接分别为dc-A和dc-B。</p> <p>全域接入网关，请根据实际需求创建，本示例说明如下：</p> <ul style="list-style-type: none"> <li>名称：请根据实际情况填写，本示例为dgw-A和dgw-B。</li> <li>BGP ASN：建议全域接入网关和企业路由器的AS号不一样，本示例中全域接入网关的AS号为64512。</li> <li>地址类型：请根据实际情况选择，本示例为IPv4。</li> </ul>

资源类型	资源数量	说明
		<p>虚拟接口，请根据实际需求创建，本示例说明如下：</p> <ul style="list-style-type: none"><li>名称：本示例两个虚拟接口分别为vif-A和vif-B。</li><li>虚拟接口优先级：此处两个虚拟接口均选择“优先”，表示形成负载均衡。</li><li>物理连接：本示例中虚拟接口vif-A关联的物理连接为dc-A，vif-B关联dc-B。</li><li>全域接入网关：本示例中虚拟接口vif-A关联的全域接入网关为dgw-A，vif-B关联dgw-B。</li><li>本端网关：本示例vif-A为10.0.0.1/30，vif-B为10.1.0.1/30。</li><li>远端网关：本示例vif-A为10.0.0.2/30，vif-B为10.1.0.2/30。</li><li>远端子网：此处为IDC侧子网网段，本示例为172.16.1.0/24。</li><li>路由模式：请选择“BGP”。</li><li>BGP邻居AS号：此处为线下IDC侧的AS号，不能和云上全域接入网关、ER等服务的AS号一样，本示例为64555。</li></ul>
ECS	1	<p>ECS主要用来验证网络通信情况，本示例如下：</p> <ul style="list-style-type: none"><li>名称：根据实际情况填写，本示例为ecs-A。</li><li>镜像：请根据实际情况选择，本示例为公共镜像（CentOS 8.2 64bit）。</li><li>网络：<ul style="list-style-type: none"><li>虚拟私有云：选择业务VPC，本示例为vpc-A。</li><li>子网：选择和线下IDC通信的子网，本示例为subnet-A01。</li></ul></li><li>安全组：请根据实际情况选择，本示例安全组模板选择“通用Web服务器”，名称为sg-demo。</li><li>私有IP地址：192.168.0.137</li></ul>

#### 须知

- DC两条链路属于负载均衡模式，因此为了防止网络环路以及形成等价路由，DC两个全域接入网关的AS号必须保持一致，本示例为64512。
- 企业路由器不能和线下IDC的AS号一样，且建议企业路由器和全域接入网关的AS号也不一样，由于64512是全域接入网关的系统预留AS号，因此本示例ER为64513。
- 线下IDC侧的AS号，不能和云上服务的AS号一样，请根据客户的实际情况填写，本示例为64555。

## 7.3 DC 双链路负载混合云组网构建流程

本章节介绍通过企业路由器构建DC双链路负载混合云组网总体流程，流程说明如表7-6所示。

表 7-6 构建 DC 双链路负载混合云组网流程说明(全域接入网关 DGW)

步骤	说明
<b>步骤一：创建云服务资源</b>	<ol style="list-style-type: none"> <li>1. 创建1个企业路由器，构建一个同区域组网只需要1个企业路由器。</li> <li>2. 创建业务VPC和子网，本示例中创建1个VPC和子网。</li> <li>3. 在业务VPC子网内，创建ECS，本示例中创建1个ECS。</li> </ol>
<b>步骤二：在企业路由器中添加并配置VPC连接</b>	<ol style="list-style-type: none"> <li>1. 在企业路由器中添加“虚拟私有云（VPC）”连接：将1个业务VPC接入企业路由器中。</li> <li>2. 在VPC路由表中配置路由：在VPC路由表中配置到企业路由器的路由信息，目的地址为IDC侧网段。</li> </ol>
<b>步骤三：在企业路由器中添加并配置DGW连接</b>	<ol style="list-style-type: none"> <li>1. 搭建第一条专线链路并验证网络通信情况。 <ol style="list-style-type: none"> <li>a. 创建1个物理连接：物理连接是线下IDC侧和华为云的专属通道，需要运营商进行施工，搭建物理专线链路连接线下和云上。</li> <li>b. 创建1个全域接入网关：创建1个全域接入网关。</li> <li>c. 创建1个虚拟接口：虚拟接口用来连接全域接入网关和物理连接。</li> <li>d. 将全域接入网关接入企业路由器：接入后，在企业路由器的连接列表中可以查看“全域接入网关（DGW）”连接。</li> <li>e. 配置IDC侧路由：在线下IDC侧路由设备配置网络参数。</li> <li>f. 登录ECS，执行ping命令，验证DC链路通信情况。</li> </ol> </li> <li>2. 参考1，搭建第二条专线链路并验证网络通信情况。</li> </ol>
<b>步骤四：在ER侧和IDC侧分别配置等价路由</b>	<ol style="list-style-type: none"> <li>1. 在ER路由表中，检查ER通过DGW连接学习的BGP路由是否形成负载均衡。 <ol style="list-style-type: none"> <li>a. 如果形成负载均衡，则无需配置路由策略。</li> <li>b. 如果未形成负载均衡，则需要配置路由策略，执行2，在ER侧配置等价路由。</li> </ol> </li> <li>2. （可选）在ER侧配置等价路由，即创建路由策略并绑定至DGW连接的传播上。配置路由策略，替换路由的AS_Path，可能会导致网络环路，配置前请检查网络规划，谨慎配置。 <ol style="list-style-type: none"> <li>a. 创建1个路由策略：路由策略中包含两个策略节点。</li> <li>b. 为DGW连接的传播绑定路由策略：分别将路由策略绑定至两个DGW连接上，将ER通过DGW连接学习的BGP路由形成等价路由。</li> </ol> </li> <li>3. 登录IDC侧网络设备，配置IDC侧的等价路由。</li> </ol>

## 7.4 DC 双链路负载混合云组网构建步骤

### 步骤一：创建云服务资源（业务 VPC、ECS、ER）

本步骤指导您创建业务VPC、ECS以及ER服务资源，云服务资源的总体规划说明，请参见[表7-5](#)。

#### 步骤1 创建企业路由器。

创建企业路由器，具体方法请参见[创建企业路由器](#)。

#### 步骤2 创建业务VPC。

创建VPC及子网，具体方法请参见[创建虚拟私有云和子网](#)。

#### 步骤3 创建业务ECS。

本示例中1个业务ECS主要用于验证云上VPC和线下IDC通信使用，数量和配置仅供参考，请您根据实际需要创建业务ECS。

创建ECS，具体方法请参见[自定义购买ECS](#)。

----结束

### 步骤二：在企业路由器中添加并配置 VPC 连接

#### 步骤1 将业务VPC接入企业路由器中，即在ER中添加VPC连接。

添加连接时，开启“配置连接侧路由”功能。

#### 须知

开启该功能后，会在VPC路由表中自动添加指向ER的路由，目的地址固定为10.0.0.0/8，172.16.0.0/12，192.168.0.0/16。

添加“虚拟私有云（VPC）”连接，具体方法请参见[在企业路由器中添加VPC连接](#)。

#### 步骤2 检查ER路由表中指向VPC的路由。

本示例中，ER开启了“默认路由表关联”和“默认路由表传播”功能，那么在ER中添加“虚拟私有云（VPC）”连接时，系统会自动添加ER指向VPC的路由，无需手动添加，只需要检查即可。

ER路由规划详情，请参见[表7-2](#)和[表7-4](#)，本示例中，目的地址为192.168.0.0/16，下一跳为VPC-A连接的路由已自动添加。

查看ER路由，具体方法请参见[查看路由](#)。

#### 步骤3 在业务VPC的路由表中，添加指向ER的路由。

VPC路由规划详情，请参见[表7-3](#)，本示例中添加目的地址为线下IDC侧网段172.16.1.0/24的路由。

配置路由信息，具体方法请参见[在VPC路由表中配置路由](#)。

----结束

### 步骤三：在企业路由器中添加并配置 DGW 连接

本示例中，云专线DC资源的总体规划说明，请参见[表7-5](#)。

**步骤1** 执行以下步骤，搭建第一条专线链路并验证网络通信情况。

1. 创建物理连接。  
创建方法，具体请参见[物理连接接入](#)。
2. 在企业路由器中添加“全域接入网关（DGW）”连接。
  - a. 在云专线管理控制台，执行以下操作：
    - i. 创建全域接入网关。
    - ii. 创建虚拟接口。
    - iii. 将全域接入网关接入企业路由器，即添加“全域接入网关（DGW）”连接。

具体方法请参见[创建全域接入网关](#)。

- b. 在企业路由器控制台，查看“全域接入网关（DGW）”连接的添加情况。  
具体方法请参见[查看连接](#)。

“全域接入网关（DGW）”连接的状态“正常”，表示已成功接入企业路由器中。

由于本示例创建ER时，开启“默认路由表关联”和“默认路由表传播”，因此添加完“全域接入网关（DGW）”连接后，以下均为系统自动配置：

- 在ER默认路由表中创建关联。
- 在ER默认路由表中创建传播，并自动学习IDC侧的路由信息。  
需要执行以下步骤连通DC后，才可以在ER路由表中查看到IDC侧的路由信息。

3. 配置IDC侧路由到华为云的路由。

以华为网络设备为例，配置BGP路由：

```
bgp 64555
peer 10.0.0.1 as-number 64512
peer 10.0.0.1 password simple Qaz12345678
network 172.16.1.0 255.255.255.0
```

表 7-7 BGP 路由

命令	命令说明
<code>bgp 64555</code>	启动BGP，其中： 64555：IDC侧AS号。
<code>peer 10.0.0.1 as-number 64512</code>	创建BGP的对等体(EBGP)，其中： - 10.0.0.1：华为云的网关。 - 64512：全域接入网关的BGP ASN。

命令	命令说明
<code>peer 10.0.0.1 password simple Qaz12345678</code>	BGP对等体建立TCP连接时对BGP消息进行MD5认证，其中： Qaz12345678：BGP MD5认证密码。
<code>network 172.16.1.0 255.255.255.0</code>	将IP路由表中已存在的路由添加到BGP路由表中，其中： - 172.16.1.0：IDC侧子网。 - 255.255.255.0：IDC侧子网掩码。

4. 登录弹性云服务器ecs-A。  
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）。
5. 执行以下命令，验证第一条专线链路的通信情况。

**ping IDC侧任意一个IP地址**

命令示例：

**ping 172.16.1.10**

回显类似如下信息，表示vpc-A与IDC可以通过第一条专线链路通信。

```
[root@ecs-A ~]# ping 172.16.1.10
PING 172.16.1.10 (172.16.1.10) 56(84) bytes of data.
64 bytes from 172.16.1.10: icmp_seq=1 ttl=64 time=0.849 ms
64 bytes from 172.16.1.10: icmp_seq=2 ttl=64 time=0.455 ms
64 bytes from 172.16.1.10: icmp_seq=3 ttl=64 time=0.385 ms
64 bytes from 172.16.1.10: icmp_seq=4 ttl=64 time=0.372 ms
...
--- 172.16.1.10 ping statistics ---
```

**步骤2** 执行以下步骤，搭建第二条专线链路并验证网络通信情况。

1. 参考[步骤1.1~步骤1.3](#)，搭建第二条专线链路。
2. 构造第一条专线链路的故障，确保业务VPC已无法通过该链路和IDC通信。

#### 须知

请您务必在没有业务的情况下，构造专线链路故障，以免对业务造成影响。

3. 参考[步骤1.4~步骤1.5](#)，验证第二条专线链路的通信情况。

---结束

## 步骤四：在 ER 侧和 IDC 侧分别配置等价路由

**步骤1** 在ER路由表中，检查ER通过DGW连接学习的BGP路由是否形成负载均衡。

查看ER路由，具体方法请参见[查看路由](#)。

- 如果形成负载均衡，则无需配置路由策略。
- 如果未形成负载均衡，则需要配置路由策略，执行[步骤2](#)，在ER侧配置等价路由。当路由172.16.1.0/24的下一跳显示两个DGW连接时，则表示形成负载均衡模式。

**步骤2**（可选）在ER侧配置等价路由，即创建路由策略并绑定至DGW连接的传播上。

1. 创建路由策略，路由策略中包含两个策略节点。

本示例中，路由策略的总体规划说明，请参见[表7-5](#)。

创建路由策略，具体方法请参见[创建路由策略](#)。

2. 分别将路由策略绑定至两个DGW连接上，将ER通过DGW连接学习的BGP路由形成等价路由。

为DGW连接的传播绑定路由策略，具体方法请参见[将路由策略绑定至ER连接的传播](#)。

3. 再次执行[步骤1](#)，检查路由是否形成负载均衡。

---

#### 须知

配置路由策略，替换路由的AS\_Path值，可能会导致网络环路，因此配置前请检查网络规划，根据实际情况谨慎配置。

---

**步骤3** 登录线下IDC侧网络设备，需要根据网络的实际规划，将IDC侧去往云上ER的路由配置成等价路由，形成负载均衡。

----结束

# 8 通过企业路由器构建 DC 双链路主备混合云组网（全域接入网关 DGW）

## 8.1 DC 双链路主备混合云组网方案概述

### 应用场景

云专线（Direct Connect, DC）用于搭建线下IDC和云上虚拟私有云（Virtual Private Cloud, VPC）之间高速、低时延、稳定安全的专属连接通道，您可以通过企业路由器和云专线的全域接入网关，构建满足企业通信的大规模混合云组网。

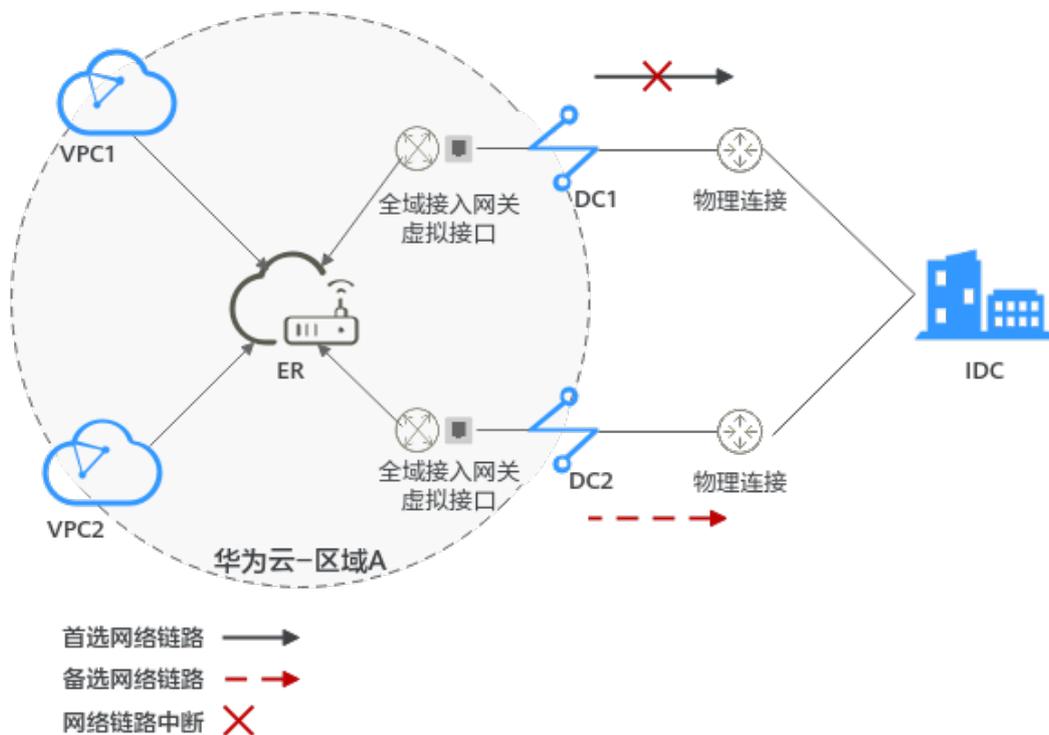
为了助力企业客户实现混合云组网的高可靠性，并且控制成本费用，通过企业路由器，可以实现专线的动态选路和切换，多个专线链路之间形成主备冗余，当主链路故障后，可自动切换至备链路，降低了单链路故障导致的业务中断风险。

接下来，将主要为您介绍如何通过企业路由器和全域接入网关，构建DC双链路主备混合云组网。

### 方案架构

为了提升混合云组网的网络可靠性，并且控制成本费用，XX企业同时部署了两条DC链路，均可以连通云上VPC和线下IDC的网络。两条DC链路形成主备，当主链路故障后，可自动切换至备链路，降低了单链路故障导致的业务中断风险。

图 8-1 DC 双链路主备混合云组网(全域接入网关 DGW)



## 方案优势

通过企业路由器和全域接入网关，可以实现DC双链路主备模式：

- 提升混合云组网的网络性能和高可靠性，避免网络链路单点故障时业务受损。
- 控制成本费用，备用链路选用低成本的线路。
- 简化运维，指定出云链路。

## 约束与限制

云上VPC子网网段与客户IDC侧子网网段不能重复。

## 8.2 DC 双链路主备混合云组网和资源规划

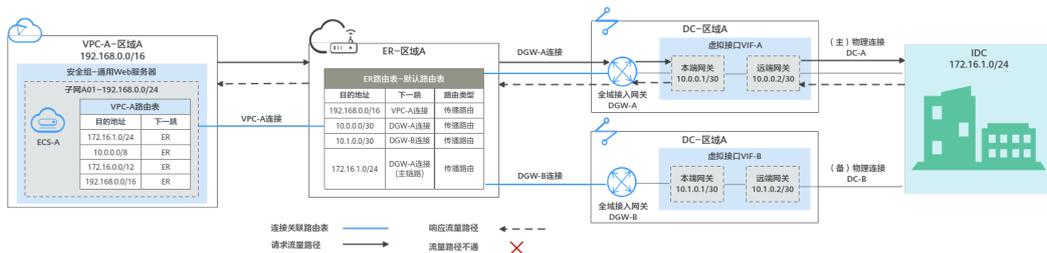
通过全域接入网关构建DC双链路主备混合云组网，您需要规划资源和组网，本示例中为您详细介绍资源和组网情况。

- **网络规划说明：**划VPC及其子网的网段、专线的全域接入网关和虚拟接口、VPC路由表和ER路由表信息等。
- **资源规划说明：**规划云上资源的数量、名称以及主要参数等信息，云上资源包括VPC、DC、ECS以及ER。

## 网络规划说明

DC双链路主备混合云组网规划如图8-2所示，将VPC、DC分别接入ER中，组网规划说明如表8-2所示。

图 8-2 DC 双链路主备混合云组网规划(全域接入网关 DGW)



两条DC网络链路形成主备，DC-A为主链路，DC-B为备链路，云上VPC和线下IDC通信时，正常情况下DC-A处于工作状态，当DC-A链路故障，流量切换到DC-B链路，表8-1为您介绍详细网络流量路径。

在ER路由表中只显示优选路由，由于DGW-A连接(DC-A)处于工作状态，因此ER路由表中显示DGW-A的路由。

表 8-1 网络流量路径说明(全域接入网关 DGW)

路径	说明
请求路径: VPC-A → 线下IDC	<ol style="list-style-type: none"> <li>在VPC-A路由表中，通过下一跳为ER的路由将流量转送到ER。</li> <li>在ER路由表中，通过下一跳为DGW-A连接的路由将流量转送到全域接入网关DGW-A。 <ul style="list-style-type: none"> <li>下一跳为DGW-A的路由，其中172.16.1.0/24为线下IDC子网网段地址，10.0.0.0/30为虚拟接口VIF-A的网关地址。</li> <li>目的地址为172.16.1.0/24的路由，下一跳对应DGW-A，DGW-A的路由优先。</li> </ul> </li> <li>全域接入网关DGW-A连接虚拟接口VIF-A，通过虚拟接口将流量从远端网关转送到物理连接。</li> <li>通过物理连接DC-A将流量送达线下IDC。</li> </ol>
响应路径: 线下IDC → VPC-A	<ol style="list-style-type: none"> <li>根据线下IDC网络的路由配置，通过物理连接DC-A将流量转送到虚拟接口VIF-A。线下IDC内网络中，指向云上的路由也配置成主备，优先转发到DC-A。</li> <li>虚拟接口VIF-A连接全域接入网关DGW-A，通过虚拟接口将流量从本端网关转送到全域接入网关。</li> <li>通过全域接入网关DGW-A将流量转送到ER。</li> <li>在ER路由表中，通过下一跳为VPC-A连接的路由将流量送达VPC-A。</li> </ol>

表 8-2 DC 双链路主备混合云组网规划说明(全域接入网关 DGW)

资源	说明
VPC	<p>业务VPC，实际运行客户业务的VPC，具体说明如下：</p> <ul style="list-style-type: none"> <li>• VPC网段（CIDR）不能重叠。 本示例中，ER路由表使用的是“虚拟私有云（VPC）”连接的传播路由，由ER自动学习VPC网段作为目的地址，不支持修改，因此重叠的VPC网段会导致路由冲突。 如果您已有的VPC存在网段重叠，则不建议您使用传播路由，请在ER路由表中手动添加静态路由，目的地址可以为VPC子网网段或者范围更小的网段。</li> <li>• VPC网段与客户IDC侧网段不能重复。</li> <li>• VPC有一个默认路由表。</li> <li>• VPC默认路由表中的路由信息如表8-3所示。 <ul style="list-style-type: none"> <li>- 固定网段：10.0.0.0/8、172.16.0.0/12、192.168.0.0/16三个固定网段是添加VPC连接时，开启“配置连接侧路由”选项，系统自动在VPC路由表配置的静态路由。如果ER内同时接入多个VPC连接，则这些路由可以将当前VPC访问其他VPC的路由转发至ER，再通过ER将流量转发至下一跳网络实例。</li> <li>- 线下IDC侧网段：除了系统自动添加的3个VPC固定网段，您还需要在VPC路由表中添加目的地址为IDC侧网段，下一跳指向ER的路由，本示例为172.16.1.0/24，该路由可以将VPC访问线下IDC侧的流量转发至ER，再通过ER将流量转发至下一跳网络实例。</li> </ul> </li> </ul> <p><b>说明</b> 如果VPC路由表中的路由与这三个固定网段冲突，则会添加失败。此时建议您不要开启“配置连接侧路由”选项，并在连接创建完成后，手动添加路由。</p>
DC	<p>两个DC需要构建主备冗余网络链路，具体如下：</p> <ul style="list-style-type: none"> <li>• 2个物理连接：需要运营商施工搭建连通华为云和线下IDC的物理专线。</li> <li>• 2个全域接入网关：将两个全球网关分别接入ER中，即表示在“全域接入网关（DGW）”中添加到ER的连接。</li> <li>• 2个虚拟接口：分别连接两个全域接入网关和物理连接。</li> </ul>
ER	<p>开启“默认路由表关联”和“默认路由表传播”功能，添加完“全域接入网关（DGW）”连接和“虚拟私有云（VPC）”连接，系统会自动执行以下配置：</p> <ul style="list-style-type: none"> <li>• DC： <ul style="list-style-type: none"> <li>- 将2个“全域接入网关（DGW）”连接关联至ER默认路由表。</li> <li>- 在默认路由表中创建“全域接入网关（DGW）”连接的传播，路由自动学习DC侧的所有路由信息，包括本端网关和远端网关、IDC侧网段等信息，路由信息如表8-4所示。</li> </ul> </li> <li>• VPC： <ul style="list-style-type: none"> <li>- 将1个“虚拟私有云（VPC）”连接关联至ER默认路由表。</li> <li>- 在默认路由表中创建“虚拟私有云（VPC）”连接的传播，路由自动学习VPC网段，路由信息如表8-4所示。</li> </ul> </li> </ul>

资源	说明
路由策略	<ul style="list-style-type: none"> <li>如果ER通过两个DGW连接学习的IDC侧的BGP路由是等价路由，自动形成负载均衡，需要创建并绑定路由策略，改成主备关系。本示例的表8-4中，目的地址为172.16.1.0/24，下一跳为DGW-A连接和DGW-B连接的两条路由默认情况下是等价路由。</li> <li>需要在备用链路DGW-B连接的传播上，绑定路由策略。通过增加路由的AS_Path，将ER通过DGW-B连接去往IDC侧的路由优先级降低。 您需要创建一个路由策略，添加两个节点： <ul style="list-style-type: none"> <li>策略节点1：优先级高，匹配BGP路由，对于匹配成功的路由，将路由的AS_Path值追加65535。65535是追加的AS_Path示例，不与IDC、ER、DGW的ASN重复即可。</li> <li>策略节点2：优先级低，匹配所有路由，此条节点是确保其他非BGP路由正常通信。</li> </ul> </li> </ul> <p>关于路由策略的详细说明，请您参见<a href="#">路由策略概述</a>。</p> <p>配置路由策略，追加路由的AS_Path值，可能会导致网络环路，因此配置前请检查网络规划，根据实际情况谨慎配置。</p>
ECS	<p>1个ECS位于业务VPC内，本示例用该ECS来验证云上和线下IDC的网络通信情况。</p> <p>如果您有多台ECS，并且这些ECS位于不同的安全组，需要在安全组中添加规则放通网络。</p>
IDC侧	<p>需要根据线下IDC侧网络的实际规划，将IDC侧去往云上专线的路由配置成主备，形成主备冗余。</p>

表 8-3 VPC 路由表

目的地址	下一跳	路由类型
固定网段：10.0.0.0/8	企业路由器	静态路由：自定义
固定网段： 172.16.0.0/12	企业路由器	静态路由：自定义
固定网段： 192.168.0.0/16	企业路由器	静态路由：自定义
线下IDC侧网段： 172.16.1.0/24	企业路由器	静态路由：自定义

### 说明

- 如果您在创建连接时开启“配置连接侧路由”选项，则不用手动在VPC路由表中配置静态路由，系统会在VPC的所有路由表中自动添加指向ER的路由，目的地址固定为10.0.0.0/8，172.16.0.0/12，192.168.0.0/16。
- 如果VPC路由表中的路由与这三个固定网段冲突，则会添加失败。此时建议您不要开启“配置连接侧路由”选项，并在连接创建完成后，手动添加路由。
- 除了系统自动添加的3个VPC固定网段，您还需要在VPC路由表中添加目的地址为IDC侧网段，下一跳指向ER的路由。

表 8-4 ER 路由表

目的地址	下一跳	路由类型
VPC-A网段： 192.168.0.0/16	VPC-A连接：er-attach-vpc-A	传播路由
VIF-A网关：10.0.0.0/30	DGW-A连接：er-attach-dgw-A	传播路由
VIF-B网关：10.1.0.0/30	DGW-B连接：er-attach-dgw-B	传播路由
IDC侧网段： 172.16.1.0/24	该路由只显示优选的下一跳： DGW-A连接：er-attach-dgw-A	传播路由

## 资源规划说明

企业路由器ER、云专线DC、虚拟私有云VPC、弹性云服务器ECS只要位于同一个区域内即可，可用区可以任意选择，不用保持一致。

### 说明

以下资源规划详情仅为示例，您可以根据需要自行修改。

表 8-5 DC 双链路主备混合云组网资源规划总体说明(全域接入网关 DGW)

资源类型	资源数量	说明
VPC	1	业务VPC，实际运行客户业务的VPC，需要接入ER中。 <ul style="list-style-type: none"><li>• VPC名称：请根据实际情况填写，本示例为vpc-A。</li><li>• IPv4网段：VPC网段与客户IDC侧网段不能重复，请根据实际情况填写，本示例为192.168.0.0/16。</li><li>• 子网名称：请根据实际情况填写，本示例为subnet-A01。</li><li>• 子网IPv4网段：VPC子网网段与客户IDC侧子网网段不能重复，请根据实际情况填写，本示例为192.168.0.0/24。</li></ul>

资源类型	资源数量	说明
ER	1	<ul style="list-style-type: none"> <li>● 名称：请根据实际情况填写，本示例为er-X。</li> <li>● ASN：此处AS号不能和线下IDC的AS号一样，本示例为64513。</li> <li>● 默认路由表关联：开启</li> <li>● 默认路由表传播：开启</li> <li>● 自动接受共享连接：请根据实际情况选择，本示例选择“开启”。</li> <li>● 连接，本示例需要在企业路由器中添加3个连接：                             <ul style="list-style-type: none"> <li>- VPC-A连接：er-attach-vpc-A</li> <li>- DGW-A连接：er-attach-dgw-A</li> <li>- DGW-B连接：er-attach-dgw-B</li> </ul> </li> </ul>
路由策略	1	<p>如果ER通过两个DGW连接学习的IDC侧的BGP路由是等价路由，则需要配置路由策略，为DGW-B连接绑定路由策略，追加AS_Path。</p> <p>路由策略中需要添加两个路由策略节点，本示例如下：</p> <ul style="list-style-type: none"> <li>● 策略节点1：优先级高，对于BGP路由，追加路由的AS_Path，将ER通过DGW-B连接学习到的路由优先级降低。                             <ul style="list-style-type: none"> <li>- 节点号：节点号取值小的策略节点优先执行，因此策略节点1的节点号取值必须小于策略节点2，此处填写10。</li> <li>- 匹配模式：此处设置成“允许”。</li> <li>- 匹配条件：此处设置成“路由类型”、“BGP路由”。</li> <li>- 策略值1：此处设置成“AS_Path”。</li> <li>- 执行动作：此处设置成“追加”，追加值和DGW、ER、IDC内部不一致，请根据实际情况填写，本示例为“64535”。</li> </ul> </li> <li>● 策略节点2：优先级低，匹配所有路由，此条节点是确保其他非BGP路由正常通信。                             <ul style="list-style-type: none"> <li>- 节点号：策略节点2的节点号取值必须大于策略节点1，此处填写20。</li> <li>- 匹配模式：此处设置成“允许”。</li> </ul> </li> <li>● 其他参数不填写，为空即可，表示未匹配上策略节点1的其他路由均可以匹配上策略节点2，确保路由策略可放行所有路由。</li> </ul>
DC	2	<p>物理连接：请根据实际需求创建。</p> <p>本示例中，两个物理连接分别为dc-A和dc-B。</p>

资源类型	资源数量	说明
		<p>全域接入网关，请根据实际需求创建，本示例说明如下：</p> <ul style="list-style-type: none"> <li>名称：请根据实际情况填写，本示例为dgw-A和dgw-B。</li> <li>关联模式：请选择“企业路由器”。</li> <li>企业路由器：选择您的企业路由器，本示例为er-X。</li> <li>BGP ASN：两个主备的全域接入网关的AS号可自定义，全域接入网关和企业路由器的AS号一样或者不一样均可，本示例中两个全域接入网关的AS号均为64512。</li> </ul> <p>虚拟接口，请根据实际需求创建，本示例说明如下：</p> <ul style="list-style-type: none"> <li>名称：本示例两个虚拟接口分别为vif-A和vif-B。</li> <li>虚拟接口优先级：此处两个虚拟接口均选择“优先”，表示形成负载均衡，由ER侧路由策略控制出云的主备链路。</li> <li>物理连接：本示例中虚拟接口vif-A关联的物理连接为dc-A，vif-B关联dc-B。</li> <li>全域接入网关：本示例中虚拟接口vif-A关联的全域接入网关为dgw-A，vif-B关联dgw-B。</li> <li>本端网关：本示例vif-A为10.0.0.1/30，vif-B为10.1.0.1/30。</li> <li>远端网关：本示例vif-A为10.0.0.2/30，vif-B为10.1.0.2/30。</li> <li>远端子网：此处为IDC侧子网网段，本示例为172.16.1.0/24。</li> <li>路由模式：请选择“BGP”。</li> <li>BGP邻居AS号：此处为线下IDC侧的AS号，不能和云上全域接入网关、ER等服务的AS号一样，本示例为64555。</li> </ul> <p>关联实例，即将全域接入网关加入到企业路由器中，请根据实际需求创建，本示例说明如下：</p> <ul style="list-style-type: none"> <li>实例类型：此处请选择“连接”。</li> <li>连接名称：请根据实际情况填写，本示例为er-attach-dgw。</li> <li>连接类型：此处请选择“企业路由器”。</li> <li>连接资源：选择您的企业路由器，本示例为er-X。</li> </ul>
ECS	1	<p>ECS主要用来验证网络通信情况，本示例如下：</p> <ul style="list-style-type: none"> <li>名称：根据实际情况填写，本示例为ecs-A。</li> <li>镜像：请根据实际情况选择，本示例为公共镜像（CentOS 8.2 64bit）。</li> <li>网络： <ul style="list-style-type: none"> <li>虚拟私有云：选择业务VPC，本示例为vpc-A。</li> <li>子网：选择和线下IDC通信的子网，本示例为subnet-A01。</li> </ul> </li> <li>安全组：请根据实际情况选择，本示例安全组模板选择“通用Web服务器”，名称为sg-demo。</li> <li>私有IP地址：192.168.0.137</li> </ul>

## 8.3 DC 双链路主备混合云组网构建流程

本章节介绍通过企业路由器构建DC双链路主备混合云组网总体流程，流程说明如表8-6所示。

表 8-6 构建 DC 双链路主备混合云组网流程说明(全域接入网关 DGW )

步骤	说明
<b>步骤一：创建云服务资源</b>	<ol style="list-style-type: none"><li>1. 创建1个企业路由器，构建一个同区域组网只需要1个企业路由器。</li><li>2. 创建业务VPC和子网，本示例中创建1个VPC和子网。</li><li>3. 在业务VPC子网内，创建ECS，本示例中创建1个ECS。</li></ol>
<b>步骤二：在企业路由器中添加并配置VPC连接</b>	<ol style="list-style-type: none"><li>1. 在企业路由器中添加“虚拟私有云（VPC）”连接：将1个业务VPC接入企业路由器中。</li><li>2. 在VPC路由表中配置路由：在VPC路由表中配置到企业路由器的路由信息，目的地址为IDC侧网段。</li></ol>
<b>步骤三：在企业路由器中添加并配置DGW连接</b>	<ol style="list-style-type: none"><li>1. 搭建第一条专线链路并验证网络通信情况。<ol style="list-style-type: none"><li>a. 创建1个物理连接：物理连接是线下IDC侧和华为云的专属通道，需要运营商进行施工，搭建物理专线链路连接线下和云上。</li><li>b. 创建1个全域接入网关：创建1个全域接入网关。</li><li>c. 创建1个虚拟接口：虚拟接口用来连接全域接入网关和物理连接。</li><li>d. 在全域接入网关中关联实例，添加到ER的连接。</li><li>e. 配置IDC侧路由：在线下IDC侧路由设备配置网络参数。</li><li>f. 登录ECS，执行ping命令，验证DC链路通信情况。</li></ol></li><li>2. 参考1，搭建第二条专线链路并验证网络通信情况。</li></ol>
<b>步骤四：在ER侧和IDC侧分别配置主备路由</b>	<ol style="list-style-type: none"><li>1. 在ER路由表中，检查ER通过DGW连接学习的BGP路由是否优选DGW-A连接。<ul style="list-style-type: none"><li>● 当专线链路差异导致AS_Path长度不一样，从而自动形成主备路由的情况，您无需额外配置路由策略。</li><li>● 其他情况，则需要执行2，在ER侧配置主备路由。</li></ul></li><li>2. （可选）在ER侧配置主备路由，即创建路由策略并绑定至DGW-B连接的传播上。<p>配置路由策略，追加路由的AS_Path，可能会导致网络环路，配置前请检查网络规划，谨慎配置。</p><ol style="list-style-type: none"><li>a. 创建路由策略，路由策略中包含两个策略节点。</li><li>b. 分别将路由策略绑定至两个DGW连接上，将ER通过DGW连接学习的BGP路由形成主备路由。</li></ol></li><li>3. 登录IDC侧网络设备，配置IDC侧的主备路由。</li></ol>

## 8.4 DC 双链路主备混合云组网构建步骤

### 步骤一：创建云服务资源（业务 VPC、ECS、ER）

本步骤指导您创建业务VPC、ECS以及ER服务资源，云服务资源的总体规划说明，请参见[表8-5](#)。

#### 步骤1 创建企业路由器。

创建企业路由器，具体方法请参见[创建企业路由器](#)。

#### 步骤2 创建业务VPC。

创建VPC及子网，具体方法请参见[创建虚拟私有云和子网](#)。

#### 步骤3 创建业务ECS。

本示例中1个业务ECS主要用于验证云上VPC和线下IDC通信使用，数量和配置仅供参考，请您根据实际需要创建业务ECS。

创建ECS，具体方法请参见[自定义购买ECS](#)。

----结束

### 步骤二：在企业路由器中添加并配置 VPC 连接

#### 步骤1 将业务VPC接入企业路由器中，即在ER中添加VPC连接。

添加连接时，开启“配置连接侧路由”功能。

#### 须知

开启该功能后，会在VPC路由表中自动添加指向ER的路由，目的地址固定为10.0.0.0/8，172.16.0.0/12，192.168.0.0/16。

添加“虚拟私有云（VPC）”连接，具体方法请参见[在企业路由器中添加VPC连接](#)。

#### 步骤2 检查ER路由表中指向VPC的路由。

本示例中，ER开启了“默认路由表关联”和“默认路由表传播”功能，那么在ER中添加“虚拟私有云（VPC）”连接时，系统会自动添加ER指向VPC的路由，无需手动添加，只需要检查即可。

ER路由规划详情，请参见[表8-2](#)和[表8-4](#)，本示例中两条路由的下一跳分别为VPC-A连接和VPC-B连接。

查看ER路由，具体方法请参见[查看路由](#)。

#### 步骤3 在业务VPC的路由表中，添加指向ER的路由。

VPC路由规划详情，请参见[表8-3](#)，本示例中添加目的地址为线下IDC侧网段172.16.1.0/24的路由。

配置路由信息，具体方法请参见[在VPC路由表中配置路由](#)。

----结束

### 步骤三：在企业路由器中添加并配置 DGW 连接

本示例中，云专线DC资源的总体规划说明，请参见[表8-2](#)。

**步骤1** 执行以下步骤，搭建第一条专线链路并验证网络通信情况。

1. 创建物理连接。  
创建方法，具体请参见[物理连接接入](#)。
2. 在企业路由器中添加“全域接入网关（DGW）”连接。
  - a. 在云专线管理控制台，执行以下操作：
    - i. 创建全域接入网关。
    - ii. 创建虚拟接口。
    - iii. 将全域接入网关接入企业路由器，即添加“全域接入网关（DGW）”连接。

具体方法请参见[创建全域接入网关](#)。

- b. 在企业路由器控制台，查看“全域接入网关（DGW）”连接的添加情况。  
具体方法请参见[查看连接](#)。

“全域接入网关（DGW）”连接的状态“正常”，表示已成功接入企业路由器中。

由于本示例创建ER时，开启“默认路由表关联”和“默认路由表传播”，因此添加完“全域接入网关（DGW）”连接后，以下均为系统自动配置：

- 在ER默认路由表中创建关联。
- 在ER默认路由表中创建传播，并自动学习IDC侧的路由信息。  
需要执行以下步骤连通DC后，才可以在ER路由表中查看到IDC侧的路由信息。

3. 配置IDC侧路由到华为云的路由。

以华为网络设备为例，配置BGP路由：

```
bgp 64555
peer 10.0.0.1 as-number 64512
peer 10.0.0.1 password simple Qaz12345678
network 172.16.1.0 255.255.255.0
```

表 8-7 BGP 路由

命令	命令说明
<code>bgp 64555</code>	启动BGP，其中： 64555：IDC侧AS号。
<code>peer 10.0.0.1 as-number 64512</code>	创建BGP的对等体(EBGP)，其中： - 10.0.0.1：华为云的网关。 - 64512：全域接入网关的BGP ASN。

命令	命令说明
<code>peer 10.0.0.1 password simple Qaz12345678</code>	BGP对等体建立TCP连接时对BGP消息进行MD5认证，其中： Qaz12345678：BGP MD5认证密码。
<code>network 172.16.1.0 255.255.255.0</code>	将IP路由表中已存在的路由添加到BGP路由表中，其中： - 172.16.1.0：IDC侧子网。 - 255.255.255.0：IDC侧子网掩码。

4. 登录弹性云服务器ecs-A。  
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）。

5. 执行以下命令，验证第一条专线链路的通信情况。

`ping IDC侧任意一个IP地址`

命令示例：

`ping 172.16.1.10`

回显类似如下信息，表示vpc-A与IDC可以通过第一条专线链路通信。

```
[root@ecs-A ~]# ping 172.16.1.10
PING 172.16.1.10 (172.16.1.10) 56(84) bytes of data.
64 bytes from 172.16.1.10: icmp_seq=1 ttl=64 time=0.849 ms
64 bytes from 172.16.1.10: icmp_seq=2 ttl=64 time=0.455 ms
64 bytes from 172.16.1.10: icmp_seq=3 ttl=64 time=0.385 ms
64 bytes from 172.16.1.10: icmp_seq=4 ttl=64 time=0.372 ms
...
--- 172.16.1.10 ping statistics ---
```

**步骤2** 执行以下步骤，搭建第二条专线链路并验证网络通信情况。

1. 参考[步骤1.1~步骤1.3](#)，搭建第二条专线链路。
2. 构造第一条专线链路的故障，确保业务VPC已无法通过该链路和IDC通信。

#### 须知

请您务必在没有业务的情况下，构造专线链路故障，以免对业务造成影响。

3. 参考[步骤1.4~步骤1.5](#)，验证第二条专线链路的通信情况。

----结束

## 步骤四：在 ER 侧和 IDC 侧分别配置主备路由

**步骤1** 在ER路由表中，检查ER通过DGW连接学习的BGP路由是否优选DGW-A连接。

查看ER路由，具体方法请参见[查看路由](#)。

- 当专线链路差异导致AS\_Path长度不一样，从而自动形成主备路由的情况，您无需额外配置路由策略。
- 其他情况均需要配置路由策略，请您执行[步骤2](#)，在ER侧配置主备路由。路由172.16.1.0/24的下一跳对应的DGW-A连接，则表示形成主备模式。

**步骤2**（可选）在ER侧配置主备路由，即创建路由策略并绑定至DGW-B连接的传播上。

1. 创建路由策略，路由策略中包含两个策略节点。  
本示例中，路由策略的总体规划说明，请参见表8-5。  
创建路由策略，具体方法请参见[创建路由策略](#)。
2. 分别将路由策略绑定至两个DGW连接上，将ER通过DGW连接学习的BGP路由形成主备路由。  
为DGW连接的传播绑定路由策略，具体方法请参见[将路由策略绑定至ER连接的传播](#)。
3. 再次执行[步骤1](#)，检查路由是否形成主备关系。

### 须知

配置路由策略，追加路由的AS\_Path值，可能会导致网络环路，因此配置前请检查网络规划，根据实际情况谨慎配置。

**步骤3** 登录线下IDC侧网络设备，需要根据网络的实际规划，将IDC侧去往云上专线的路由配置成主备路由，形成主备冗余。

假设希望连接DC-A的线路为入云主线路，可以通过设置Local\_Pref来实现，降低DC-B线路的BGP路由本地优先级。

BGP路由配置示例（以华为设备为例）：

```
route-policy slave_direct_in permit node 10
apply local-preference 90
bgp 64555
peer 10.0.0.1 as-number 64512
peer 10.0.0.1 password simple Qaz12345678
peer 10.1.0.1 as-number 64512
peer 10.1.0.1 password simple Qaz12345678
peer 10.1.0.1 route-policy slave_direct_in import
network 172.16.1.0 255.255.255.0
```

表 8-8 BGP 路由

命令	命令说明
<b>route-policy slave_direct_in permit node 10</b> <b>apply local-preference 90</b>	备链路的路由策略。 slave_direct_in：备链路的路由策略名称
<b>bgp 64555</b>	启动BGP，其中： 64555：IDC侧AS号。
<b>peer 10.0.0.1 as-number 64512</b>	创建BGP的对等体(EBGP)，其中： <ul style="list-style-type: none"> <li>• 10.0.0.1：主链路的华为云网关。</li> <li>• 64512：全域接入网关的BGP ASN。</li> </ul>

命令	命令说明
<b>peer 10.0.0.1 password simple Qaz12345678</b>	BGP对等体建立TCP连接时对BGP消息进行MD5认证，其中： <ul style="list-style-type: none"><li>• 10.0.0.1：主链路的华为云网关。</li><li>• Qaz12345678：BGP MD5认证密码。</li></ul>
<b>peer 10.1.0.1 as-number 64512</b>	创建BGP的对等体(EBGP)，其中： <ul style="list-style-type: none"><li>• 10.1.0.1：备链路的华为云网关。</li><li>• 64512：全域接入网关的BGP ASN。</li></ul>
<b>peer 10.1.0.1 password simple Qaz12345678</b>	BGP对等体建立TCP连接时对BGP消息进行MD5认证，其中： <ul style="list-style-type: none"><li>• 10.1.0.1：备链路的华为云网关。</li><li>• Qaz12345678：BGP MD5认证密码。</li></ul>
<b>peer 10.1.0.1 route-policy slave_direct_in import</b>	备链路的BGP对等体应用入方向的路由策略。 <ul style="list-style-type: none"><li>• 10.1.0.1：备链路的华为云网关。</li><li>• slave_direct_in：备链路的路由策略名称。</li></ul>
<b>network 172.16.1.0 255.255.255.0</b>	将IP路由表中已存在的路由添加到BGP路由表中，其中： <ul style="list-style-type: none"><li>• 172.16.1.0：IDC侧子网。</li><li>• 255.255.255.0：IDC侧子网掩码。</li></ul>

----结束

# 9 通过企业路由器构建 DC/VPN 双链路主备混合云组网 (全域接入网关 DGW)

## 9.1 DC/VPN 双链路互备混合云组网方案概述

### 应用场景

云专线 (Direct Connect, DC) 用于搭建线下IDC和云上虚拟私有云 (Virtual Private Cloud, VPC) 之间高速、低时延、稳定安全的专属连接通道, 您可以通过企业路由器和云专线的全域接入网关, 构建满足企业通信的大规模混合云组网。

虚拟专用网络 (Virtual Private Network, VPN) 用于在线下IDC和云上VPC之间建立一条安全加密的公网通信隧道。相比通过DC构建混合云, 使用VPN更加快速, 成本更低。

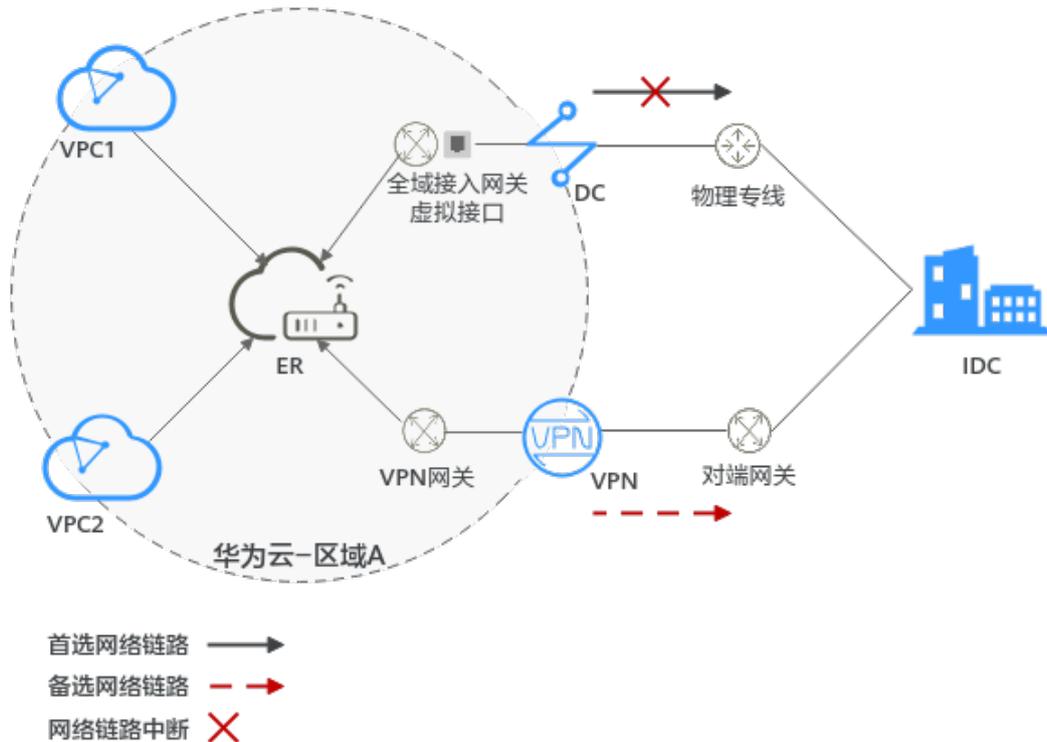
为了助力企业客户实现混合云组网的高可靠性, 并且控制成本费用, 推荐您使用企业路由器、全域接入网关以及虚拟专用网络, 在企业路由器中同时接入DC和VPN两条网络链路, 构建主备双链路的混合云组网。当主链路故障后, 可自动切换至备链路, 降低了单链路故障导致的业务中断风险。

### 方案架构

为了提升混合云组网的可靠性, XX企业同时部署了DC和VPN两条网络链路, 均可以连通云上VPC和线下IDC的网络。DC和VPN两条网络链路互为主备, 主链路为DC, 备链路为VPN, 当DC链路故障时, 可自动切换到VPN链路, 降低网络中断对业务造成的影响。

- 将VPC1、VPC2以及DC接入企业路由器中, VPC1和VPC2网络互通, 并且均可以通过DC和线下IDC通信。
- 将VPN接入企业路由器中, 当主链路DC故障时, VPC1和VPC2可以通过备链路VPN和线下IDC通信。

图 9-1 DC/VPN 双链路主备混合云组网(全域接入网关 DGW)



### 方案优势

通过企业路由器、云专线的全域接入网关以及虚拟专用网络，可以实现DC和VPN主备链路的自动切换，不需要手动切换双链路，不仅避免业务受损，同时降低维护成本。

### 约束与限制

云上VPC子网网段与客户IDC侧子网网段不能重复。

## 9.2 DC/VPN 双链路互备混合云组网和资源规划

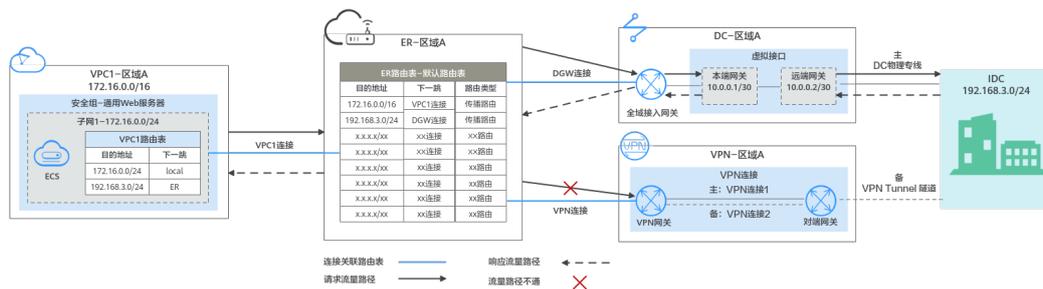
通过企业路由器构建DC/VPN双链路主备混合云组网，您需要规划资源和组网，本示例中为您详细介绍资源和组网情况。

- **网络规划说明**：规划VPC及其子网、DC、VPN和ER的网段、路由等。
- **资源规划说明**：规划云上资源的数量、名称以及主要参数等信息，云上资源包括VPC、DC、VPN以及ER等。

### 网络规划说明

DC/VPN双链路主备混合云组网规划如图9-2所示，将VPC、DC和VPN分别接入ER中，组网规划说明如表9-2所示。

图 9-2 DC/VPN 双链路主备混合云组网规划(全域接入网关 DGW)



DC和VPN互为备用网络链路，在DC网络链路正常的情况下，流量优选云专线DC。

- 在ER路由表中只显示优选路由，由于DGW连接(DC)路由的优先级高于VPN连接，因此ER路由表中不显示VPN连接的路由。
- 云上VPC和线下IDC通信时，默认使用DC这条网络链路，本示例的网络流量路径说明请参见表9-1

表 9-1 网络流量路径说明(全域接入网关 DGW)

路径	说明
请求路径： VPC1 → 线下 IDC	<ol style="list-style-type: none"> <li>1. 在VPC1路由表中，通过下一跳为ER的路由将流量转送到ER。</li> <li>2. 在ER路由表中，通过下一跳为DGW连接的路由将流量转送到全域接入网关。</li> <li>3. 全域接入网关连接虚拟接口，通过虚拟接口将流量从远端网关转送到物理专线。</li> <li>4. 通过物理专线将流量送达线下IDC。</li> </ol>
响应路径： 线下IDC → VPC1	<ol style="list-style-type: none"> <li>1. 通过物理专线将流量转送到虚拟接口。</li> <li>2. 虚拟接口连接全域接入网关，通过虚拟接口将流量从本端网关转送到全域接入网关。</li> <li>3. 通过全域接入网关将流量转送到ER。</li> <li>4. 在ER路由表中，通过下一跳为VPC1连接的路由将流量送达VPC1。</li> </ol>

表 9-2 DC/VPN 双链路互备混合云组网规划说明(全域接入网关 DGW)

资源	说明
VPC	<p>业务VPC，实际运行客户业务的VPC，本示例中为VPC1，具体说明如下：</p> <ul style="list-style-type: none"> <li>● VPC网段与客户IDC侧网段不能重复。</li> <li>● VPC有一个默认路由表。</li> <li>● VPC默认路由表中的路由说明如下：                             <ul style="list-style-type: none"> <li>- local：表示VPC本地IPV4的默认路由条目，用于VPC内子网通信，系统自动配置。</li> <li>- ER：表示将VPC子网流量转发至ER，此处目的地址配置为IDC的子网网段，路由信息如表9-3所示。</li> </ul> </li> </ul> <p>VPN网关使用的子网，建议您创建一个新的VPC，并从中分配子网。您在创建VPN网关时，需要填写该子网网段，VPN网关使用的子网不能与VPC内已有的子网网段重叠。</p>
DC	<ul style="list-style-type: none"> <li>● 1个物理连接：需要运营商施工搭建连通华为云和线下IDC的物理专线。</li> <li>● 1个全域接入网关：将全域接入网关接入ER中，即表示将“全域接入网关（DGW）”连接添加到ER。</li> <li>● 1个虚拟接口：连接全域接入网关和物理连接。</li> </ul>
VPN	<ul style="list-style-type: none"> <li>● 1个VPN网关：将VPN接入ER中，即表示将“VPN网关（VPN）”连接添加到ER。</li> <li>● 1个对端网关：用户IDC侧的对端网关。</li> <li>● 2条VPN连接：连接VPN网关和对端网关，两条VPN连接互为主备链路。</li> </ul>
ER	<p>开启“默认路由表关联”和“默认路由表传播”功能，添加完连接后，系统会自动执行以下配置：</p> <ul style="list-style-type: none"> <li>● VPC：                             <ul style="list-style-type: none"> <li>- 将1个“虚拟私有云（VPC）”连接关联至ER默认路由表。</li> <li>- 在默认路由表中创建“虚拟私有云（VPC）”连接的传播，路由自动学习VPC网段，路由信息如表9-4所示。</li> </ul> </li> <li>● DC：                             <ul style="list-style-type: none"> <li>- 将1个“全域接入网关（DGW）”连接关联至ER默认路由表。</li> <li>- 在默认路由表中创建“全域接入网关（DGW）”连接的传播，路由自动学习DC侧的所有路由信息，路由信息如表9-4所示。</li> </ul> </li> <li>● VPN：                             <ul style="list-style-type: none"> <li>- 将1个“VPN网关（VPN）”连接关联至ER默认路由表。</li> <li>- 在默认路由表中创建“VPN网关（VPN）”连接的传播，路由自动学习VPN侧的所有路由信息，路由信息如表9-4所示。</li> </ul> </li> </ul>

资源	说明
ECS	1个ECS位于业务VPC内，本示例用该ECS来验证云上和线下IDC的网络通信情况。 如果您有多台ECS，并且这些ECS位于不同的安全组，需要在安全组中添加规则放通网络。

表 9-3 VPC 路由表

目的地址	下一跳	路由类型
192.168.3.0/24	企业路由器	静态路由：自定义

#### 说明

- 如果您在创建连接时开启“配置连接侧路由”选项，则不用手动在VPC路由表中配置静态路由，系统会在VPC的所有路由表中自动添加指向ER的路由，目的地址固定为10.0.0.0/8，172.16.0.0/12，192.168.0.0/16。
- 如果VPC路由表中的路由与这三个固定网段冲突，则会添加失败。此时建议您不要开启“配置连接侧路由”选项，并在连接创建完成后，手动添加路由。
- 除了系统自动添加的3个VPC固定网段，您还需要在VPC路由表中添加目的地址为IDC侧网段，下一跳指向ER的路由。

表 9-4 ER 路由表

目的地址	下一跳	路由类型
VPC1网段：172.16.0.0/16	VPC1连接：er-attach-01	传播路由
IDC侧网段： 192.168.3.0/24	DGW连接：dgw-demo	传播路由
IDC侧网段： 192.168.3.0/24	VPN连接：vpngw-demo	传播路由

#### 须知

- 当两条路由功能一样时，ER路由表中只会显示优选路由。当DC和VPN网络链路均正常时，由于DGW连接和VPN连接的传播路由均指向线下IDC，因此只能在ER路由表中看到优先级较高的DGW连接的路由，暂时不支持查看ER路由中VPN连接的所有路由（包括未优选的路由）。
- 当DC出现故障，网络链路切换到VPN时，此时通过管理控制台，可以在ER路由表中看到VPN连接的传播路由。

## 资源规划说明

企业路由器ER、云专线DC、虚拟专用网络VPN、虚拟私有云VPC、弹性云服务器ECS只要位于同一个区域内即可，可用区可以任意选择，不用保持一致。

 说明

以下资源规划详情仅为示例，您可以根据需要自行修改。

表 9-5 DC/VPN 双链路互备混合云组网资源规划总体说明(全域接入网关 DGW )

资源类型	资源数量	说明
VPC	2	<p>业务VPC，实际运行客户业务的VPC，需要接入ER中。</p> <ul style="list-style-type: none"> <li>• VPC名称：请根据实际情况填写，本示例为vpc-for-er。</li> <li>• IPv4网段：VPC网段与客户IDC侧网段不能重复，请根据实际情况填写，本示例为172.16.0.0/16。</li> <li>• 子网名称：请根据实际情况填写，本示例为subnet-for-er。</li> <li>• 子网IPv4网段：VPC子网网段与客户IDC侧子网网段不能重复，请根据实际情况填写，本示例为172.16.0.0/24。</li> </ul> <p>VPN网关使用的VPC，需要从中分配一个子网提供给VPN网关使用。</p> <ul style="list-style-type: none"> <li>• VPC名称：请根据实际情况填写，本示例为vpc-for-vpn。</li> <li>• IPv4网段：请根据实际情况填写，本示例为10.0.0.0/16。</li> <li>• 子网名称：您创建VPC时，必须创建一个默认子网，请根据实际情况填写，本示例为subnet-01。</li> <li>• 子网IPv4网段：默认子网在本示例中不使用，请根据实际情况填写，本示例为10.0.0.0/24。</li> </ul> <p><b>须知</b> 您在创建VPN网关时，“虚拟私有云”需要选择该VPC，“互联子网”填写该VPC下未被占用的网段，该网段不能与VPC内已有的子网网段重叠。本示例中互联子网网段不能与默认子网subnet-01一样。</p>
ER	1	<ul style="list-style-type: none"> <li>• 名称：请根据实际情况填写，本示例为er-test-01。</li> <li>• ASN：企业路由器不能和线下IDC的ASN号一样，且建议企业路由器和全域接入网关的ASN号也不一样，由于64512是全域接入网关的系统预留ASN号，因此本示例企业路由器的ASN号为64513。</li> <li>• 默认路由表关联：开启</li> <li>• 默认路由表传播：开启</li> <li>• 自动接受共享连接：请根据实际情况选择，本示例选择“开启”。</li> <li>• 连接，本示例需要在企业路由器中添加3个连接： <ul style="list-style-type: none"> <li>- VPC连接：er-attach-VPC</li> <li>- DGW连接：er-attach-DGW</li> <li>- VPN连接：er-attach-VPN</li> </ul> </li> </ul>

资源类型	资源数量	说明
DC	1	物理连接：请根据实际需求创建。 本示例中，1个物理连接为dc-demo。
		全域接入网关，请根据实际需求创建，本示例说明如下： <ul style="list-style-type: none"> <li>名称：请根据实际情况填写，本示例为dgw-demo。</li> <li>BGP ASN：建议全域接入网关和企业路由器的AS号不一样，本示例中全域接入网关的AS号为64512。</li> <li>地址类型：请根据实际情况选择，本示例为IPv4。</li> </ul>
		虚拟接口，请根据实际需求创建，本示例说明如下： <ul style="list-style-type: none"> <li>名称：本示例虚拟接口为vif-demo。</li> <li>虚拟接口优先级：此处请选择“优先”。</li> <li>物理连接：本示例中虚拟接口vif-demo关联的物理连接为dc-demo。</li> <li>全域接入网关：本示例中虚拟接口vif-demo关联的全域接入网关为dgw-demo。</li> <li>本端网关：本示例为10.0.0.1/30。</li> <li>远端网关：本示例为10.0.0.2/30。</li> <li>远端子网：此处为IDC侧子网网段，本示例为192.168.3.0/24。</li> <li>路由模式：请选择“BGP”。</li> <li>BGP邻居AS号：此处为线下IDC侧的AS号，不能和云上全域接入网关、ER等服务的AS号一样，本示例为65525。</li> </ul>
VPN	1	VPN网关 <ul style="list-style-type: none"> <li>名称：请根据实际情况填写，本示例为vpngw-demo。</li> <li>关联模式：请选择“企业路由器”。</li> <li>企业路由器：选择您的企业路由器，本示例为er-test-01。</li> <li>BGP ASN：由于DC和VPN为双链路互备，此处AS号和DC全域接入网关的AS号必须一样，本示例为64512。</li> <li>虚拟私有云：选择您的虚拟私有云，本示例为vpc-for-vpn。</li> <li>互联子网：互联子网是VPN网关实际使用的子网，该子网不能与VPC内已有的子网网段重叠，请根据实际情况填写，本示例为10.0.5.0/24。</li> </ul>
		对端网关 <ul style="list-style-type: none"> <li>名称：请根据实际情况填写，本示例为cgw-demo。</li> <li>路由模式：请选择“动态BGP”。</li> <li>BGP ASN：此处为线下IDC侧的AS号，由于DC和VPN为双链路互备，该AS号和DC虚拟接口处设置的AS号必须一样，本示例为65525。</li> </ul>

资源类型	资源数量	说明
		<p>2条VPN连接，互为主动：</p> <ul style="list-style-type: none"><li>名称：请根据实际情况填写，本示例中，主VPN连接为vpn-demo-01，备VPN连接为vpn-demo-02。</li><li>VPN网关：选择您的VPN网关，本示例为vpngw-demo。</li><li>公网IP：请根据实际情况选择，主VPN连接选择主EIP，备VPN连接选择备EIP。</li><li>连接模式：请选择“路由模式”。</li><li>对端网关：选择您的对端网关，本示例为cgw-demo。</li><li>接口分配方式：本示例选择“自动分配”。</li><li>路由模式：请选择“BGP”。</li></ul>
ECS	1	<ul style="list-style-type: none"><li>名称：根据实际情况填写，本示例为ecs-demo。</li><li>镜像：请根据实际情况选择，本示例为公共镜像（CentOS 8.2 64bit）。</li><li>网络：<ul style="list-style-type: none"><li>虚拟私有云：选择您的虚拟私有云，本示例为vpc-for-er。</li><li>子网：选择子网，本示例为subnet-for-er。</li></ul></li><li>安全组：请根据实际情况选择，本示例安全组模板选择“通用Web服务器”，名称为sg-demo。</li><li>私有IP地址：172.16.1.137</li></ul>

#### 须知

- 由于DC和VPN是主备链路，为了防止网络环路，DC全域接入网关和VPN网关的AS号必须保持一致，本示例为64512。
- 企业路由器不能和线下IDC的AS号一样，且建议企业路由器和全域接入网关的AS号也不一样，由于64512是全域接入网关的系统预留AS号，因此本示例ER为64513。
- 线下IDC侧的AS号，不能和云上服务的AS号一样，请根据客户的实际情况填写，本示例为65525。

## 9.3 DC/VPN 双链路互备混合云组网构建流程

本章节介绍通过企业路由器构建DC/VPN双链路主备混合云组网总体流程，流程说明如表9-6所示。

表 9-6 构建 DC/VPN 双链路主备混合云组网流程说明(全域接入网关 DGW)

步骤	说明
<b>步骤一：创建云服务资源</b>	<ol style="list-style-type: none"> <li>1. 创建1个企业路由器，构建一个同区域组网只需要1个企业路由器。</li> <li>2. 创建业务VPC和子网，本示例中创建1个VPC和子网。</li> <li>3. 在业务VPC子网内，创建ECS，本示例中创建1个ECS。</li> </ol>
<b>步骤二：在企业路由器中添加并配置DGW连接</b>	<ol style="list-style-type: none"> <li>1. 创建物理连接，物理连接是线下IDC侧和华为云的专属通道，需要运营商进行施工，搭建物理专线链路连接线下和云上。</li> <li>2. 创建全域接入网关：创建1个全域接入网关。</li> <li>3. 创建虚拟接口：创建1个虚拟接口，虚拟接口用来连接全域接入网关和物理连接。</li> <li>4. 将全域接入网关接入企业路由器：接入后，在企业路由器的连接列表中可以查看“全域接入网关（DGW）”连接。</li> <li>5. 配置IDC侧路由：在线下IDC侧路由设备配置网络参数。</li> </ol>
<b>步骤三：在企业路由器中添加并配置VPC连接</b>	<ol style="list-style-type: none"> <li>1. 在企业路由器中添加“虚拟私有云（VPC）”连接：将1个业务VPC接入企业路由器中。</li> <li>2. 在VPC路由表中配置路由：在VPC路由表中配置到企业路由器的路由信息，目的地址为IDC侧网段。</li> </ol>
<b>步骤四：验证DC链路的通信情况</b>	登录ECS，执行ping命令，验证DC链路的网络互通情况。
<b>步骤五：在企业路由器中添加并配置VPN连接</b>	<ol style="list-style-type: none"> <li>1. 创建VPN网关：创建1个关联企业路由器的VPN网关，企业路由器中会自动添加“VPN网关（VPN）”连接。</li> <li>2. 创建对端网关：创建1个用户IDC侧的对端网关。</li> <li>3. 创建2条VPN连接：VPN连接用来连通VPN网关和对端网关，两条VPN连接互为主备链路。</li> <li>4. 配置IDC侧路由：在线下IDC侧路由设备配置网络参数。</li> </ol>
<b>步骤六：验证VPN链路的通信情况</b>	登录ECS，执行ping命令，验证VPN链路的网络互通情况。 由于VPN链路为备选，如果您需要验证VPN链路通信情况，需要先构造DC主链路故障，然后验证备VPN链路的通信情况。

## 9.4 DC/VPN 双链路互备混合云组网构建步骤

### 步骤一：创建云服务资源（业务 VPC、ECS、ER）

本步骤指导您创建业务VPC、ECS以及ER服务资源，云服务资源的总体规划说明，请参见表9-5。

#### 步骤1 创建企业路由器。

创建企业路由器，具体方法请参见[创建企业路由器](#)。

**步骤2 创建业务VPC。**

创建VPC及子网，具体方法请参见[创建虚拟私有云和子网](#)。

**步骤3 创建业务ECS。**

本示例中1个业务ECS主要用于验证云上VPC和线下IDC通信使用，数量和配置仅供参考，请您根据实际需要创建业务ECS。

创建ECS，具体方法请参见[自定义购买ECS](#)。

----结束

**步骤二：在企业路由器中添加并配置 DGW 连接**

本示例中，云专线DC资源的总体规划说明，请参见[表9-5](#)。

**步骤1 创建物理连接。**

创建方法，具体请参见[物理连接接入](#)。

**步骤2 在企业路由器中添加“全域接入网关（DGW）”连接。**

1. 在云专线管理控制台，执行以下操作：

- a. 创建全域接入网关。
- b. 创建虚拟接口。
- c. 将全域接入网关接入企业路由器，即添加“全域接入网关（DGW）”连接。

具体方法请参见[创建全域接入网关](#)。

2. 在企业路由器控制台，查看“全域接入网关（DGW）”连接的添加情况。

具体方法请参见[查看连接](#)。

“全域接入网关（DGW）”连接的状态“正常”，表示已成功接入企业路由器中。

由于本示例创建ER时，开启“默认路由表关联”和“默认路由表传播”，因此添加完“全域接入网关（DGW）”连接后，以下均为系统自动配置：

- 在ER默认路由表中创建关联。
- 在ER默认路由表中创建传播，并自动学习IDC侧的路由信息。

需要执行以下步骤连通DC后，才可以在ER路由表中查看到IDC侧的路由信息。

**步骤3 在IDC侧的网络设备上，配置网络参数。**

由于组网为DC和VPN的双链路互备，因此配置路由时，需要注意以下方面：

- DC和VPN的路由类型保持一致，构造双链路互备需要配置为BGP路由。
- 配置DC和VPN路由的主备优先级，确保DC的优先级高于VPN。
- DC和VPN网络链路的断连感知时间建议和云上网络保持一致。

----结束

**步骤三：在企业路由器中添加并配置 VPC 连接****步骤1 将业务VPC接入企业路由器中。**

添加连接时，不开启“配置连接侧路由”功能。

**须知**

开启该功能后，会在VPC路由表中自动添加指向ER的路由，目的地址固定为10.0.0.0/8，172.16.0.0/12，192.168.0.0/16。本示例中，需要在VPC路由表中手动配置指向ER的路由，目的地址为IDC侧的网段。

添加“虚拟私有云（VPC）”连接，具体方法请参见[在企业路由器中添加VPC连接](#)。

**步骤2** 检查ER路由表中指向VPC的路由。

本示例中，ER开启了“默认路由表关联”和“默认路由表传播”功能，那么在ER中添加“虚拟私有云（VPC）”连接时，系统会自动添加ER指向VPC的路由，无需手动添加，只需要检查即可。

ER路由规划详情，请参见[表9-2](#)和[表9-4](#)。

查看ER路由，具体方法请参见[查看路由](#)。

**步骤3** 在业务VPC的路由表中，添加指向ER的路由。

VPC路由规划详情，请参见[表9-3](#)。

配置路由信息，具体方法请参见[在VPC路由表中配置路由](#)。

----结束

**步骤四：验证 DC 链路的通信情况****步骤1** 登录弹性云服务器ecs-demo。

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2** 执行以下命令，验证业务VPC与IDC是否可以通过ER通信。

**ping IDC侧任意一个IP地址**

命令示例：

**ping 192.168.3.10**

回显类似如下信息，表示vpc-for-er与IDC可以通过ER通信。

```
[root@ecs-demo ~]# ping 192.168.3.10
PING 192.168.3.10 (192.168.3.10) 56(84) bytes of data:
64 bytes from 192.168.3.10: icmp_seq=1 ttl=64 time=0.849 ms
64 bytes from 192.168.3.10: icmp_seq=2 ttl=64 time=0.455 ms
64 bytes from 192.168.3.10: icmp_seq=3 ttl=64 time=0.385 ms
64 bytes from 192.168.3.10: icmp_seq=4 ttl=64 time=0.372 ms
...
--- 192.168.3.10 ping statistics ---
```

----结束

**步骤五：在企业路由器中添加并配置 VPN 连接**

本示例中，虚拟专用网络VPN、VPN网关使用的VPC资源的总体规划说明，请参见[表9-5](#)。

**步骤1** 创建1个VPN网关使用的VPC。

创建VPC及子网，具体方法请参见[创建虚拟私有云和子网](#)。

#### 须知

您在创建VPN网关时，“虚拟私有云”需要选择该VPC，“互联子网”填写该VPC下未被占用的网段，该网段不能与VPC内已有的子网网段重叠。本示例中互联子网网段不能与默认子网subnet-01一样。

**步骤2** 创建VPN网关，即在企业路由器中添加“VPN网关（VPN）”连接。

1. 在虚拟专用网络管理控制台，创建VPN网关。

具体方法请参见[创建VPN网关](#)。

2. 在企业路由器控制台，查看“VPN网关（VPN）”连接的添加情况。

具体方法请参见[查看连接](#)。

“VPN网关（VPN）”连接的状态“正常”，表示已成功接入企业路由器中。

由于本示例创建ER时，开启“默认路由表关联”和“默认路由表传播”，因此添加完“VPN网关（VPN）”连接后，以下均为系统自动配置：

- 在ER默认路由表中创建关联。
- 在ER默认路由表中创建传播，并自动学习IDC侧的路由信息。

需要执行以下步骤连通VPN后，才可以在ER路由表中查看到IDC侧的路由信息。

**步骤3** 创建对端网关。

具体方法请参见[创建对端网关](#)。

**步骤4** 分别创建两条VPN连接，用作主备。

1. 创建主VPN连接，请参见[创建第一条VPN连接](#)。

2. 创建备VPN连接，请参见[创建第二条VPN连接](#)。

**步骤5** 在IDC侧的网络设备上，配置网络参数。

由于组网为DC和VPN的双链路互备，因此配置路由时，需要注意以下方面：

- DC和VPN的路由类型保持一致，构造双链路互备需要配置为BGP路由。
- 配置DC和VPN路由的主备优先级，确保DC的优先级高于VPN。
- DC和VPN网络链路的断连感知时间建议和云上网络保持一致。

----结束

## 步骤六：验证 VPN 链路的通信情况

由于VPN链路为备选，如果您需要验证VPN链路通信情况，需要先构造DC主链路故障，然后验证备VPN链路的通信情况。

**步骤1** 构造DC主链路的故障，确保业务VPC已无法通过该链路和IDC通信。

#### 须知

请您务必在没有业务的情况下，构造DC链路故障，以免对业务造成影响。

**步骤2** 登录弹性云服务器ecs-demo。

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3** 执行以下命令，验证业务VPC与IDC是否可以通过ER通信。

**ping IDC侧任意一个IP地址**

命令示例：

**ping 192.168.3.10**

回显类似如下信息，表示vpc-for-er与IDC可以通过ER通信。

```
[root@ecs-demo ~]# ping 192.168.3.10
PING 192.168.3.10 (192.168.3.10) 56(84) bytes of data.
64 bytes from 192.168.3.10: icmp_seq=1 ttl=64 time=0.849 ms
64 bytes from 192.168.3.10: icmp_seq=2 ttl=64 time=0.455 ms
64 bytes from 192.168.3.10: icmp_seq=3 ttl=64 time=0.385 ms
64 bytes from 192.168.3.10: icmp_seq=4 ttl=64 time=0.372 ms
...
--- 192.168.3.10 ping statistics ---
```

----**结束**

# 10 通过企业路由器和云专线实现线下 IDC 和云上 VPC 互通（虚拟网关 VGW）

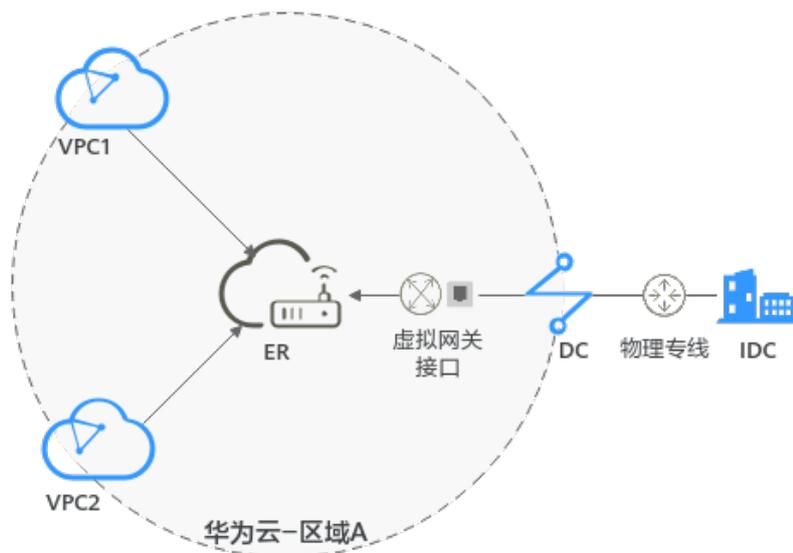
## 10.1 方案概述

### 背景信息

XX企业在华为云区域A内部署了2个虚拟私有云VPC，这2个VPC需要互相访问，并且共享同一条云专线DC访问客户线下的IDC。

在区域A内创建一个企业路由器ER，将VPC和DC的虚拟网关接入ER内，ER可以在接入的VPC和虚拟网关之间转发流量，实现2个VPC共享DC。

图 10-1 线下 IDC 和云上 VPC 互通组网



**说明**

您可以使用**企业路由器的共享功能**，将不同账号下的虚拟私有云添加至同一个企业路由器中构建组网。

如果您需要连通云上VPC和线下IDC构建混合云组网，则推荐您使用企业路由器和云专线的全域接入网关DGW，具体请参见**通过企业路由器和云专线构建混合云组网（全域接入网关DGW）**。

从2024年5月份开始，通过企业路由器和云专线的虚拟网关VGW构建混合云组网的功能不再支持新增组网，只针对存量组网进行维护。

**操作流程**

本文档介绍如何通过企业路由器构建线下IDC和云上VPC互通组网，流程如图10-2所示。

图 10-2 构建线下 IDC 和云上 VPC 互通组网流程图

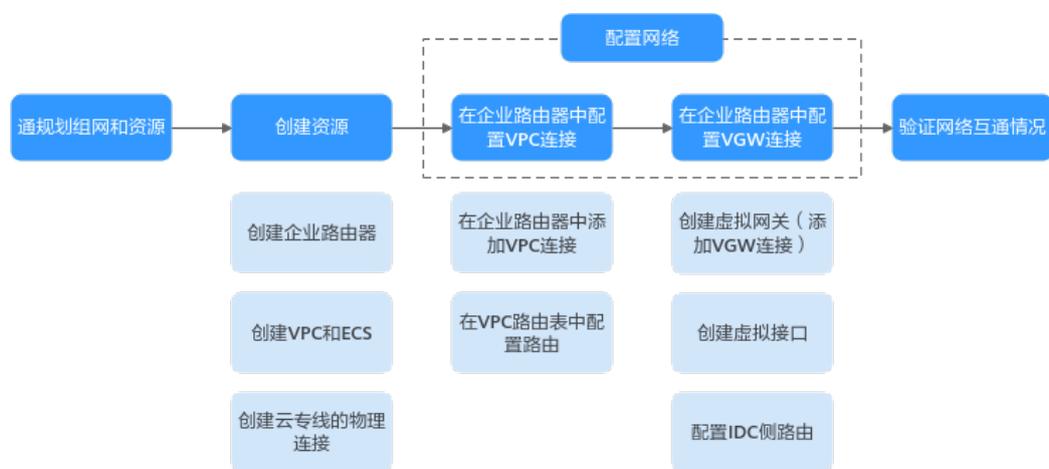


表 10-1 构建线下 IDC 和云上 VPC 互通组网流程说明

序号	步骤	说明
1	<b>规划组网和资源</b>	规划组网和资源，包括资源数量及网段信息等。
2	<b>创建资源</b>	<ol style="list-style-type: none"> <li><b>创建企业路由器</b>：创建1个企业路由器，构建一个同区域组网只需要1个企业路由器。</li> <li><b>创建VPC和ECS</b>：创建VPC和ECS资源，创建2个虚拟私有云VPC和2个弹性云服务器ECS。</li> <li><b>创建云专线的物理连接</b>：物理连接是线下IDC侧和华为云的专属通道，需要运营商进行施工，搭建物理专线链路连接线下和云上。</li> </ol>

序号	步骤	说明
3	配置网络	<p>1. 在企业路由器中配置VPC连接：</p> <p>a. 在企业路由器中添加“虚拟私有云（VPC）”连接：将2个VPC分别接入企业路由器中。</p> <p>b. 在VPC路由表中配置路由：在VPC路由表中配置到企业路由器的路由信息。</p> <p>2. 在企业路由器中配置VGW连接：</p> <p>a. 创建虚拟网关：创建1个关联企业路由器的虚拟网关，企业路由器中会自动添加“虚拟网关（VGW）”连接。</p> <p>b. 创建虚拟接口：创建关联虚拟网关的虚拟接口，连接虚拟网关和物理连接。</p> <p>c. 配置IDC侧路由：在线下IDC侧路由设备配置路由信息。</p>
4	验证网络互通情况	登录ECS，执行ping命令，验证网络互通情况。

## 10.2 规划组网和资源

通过企业路由器构建线下IDC和云上VPC互通组网，您需要规划组网和资源：

- **规划组网：**规划VPC及其子网的网段、专线的虚拟网关和虚拟接口、VPC路由表和ER路由表信息等。
- **规划资源：**规划云上资源的数量、名称以及主要参数等信息，云上资源包括VPC、DC、ECS以及ER。

### 规划组网

线下IDC和云上VPC互通组网规划如图10-3所示，将2个VPC和1个VGW网关接入ER中，组网规划说明如表10-3所示。

图 10-3 线下 IDC 和云上 VPC 互通组网规划

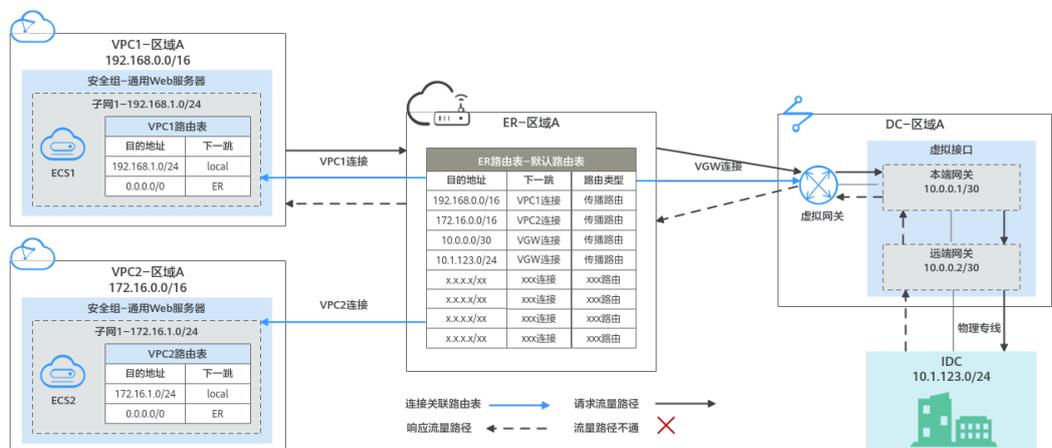


表 10-2 网络流量路径说明

路径	说明
请求路径： VPC1 → 线下 IDC	<ol style="list-style-type: none"><li>1. 在VPC1路由表中，通过下一跳为ER的路由将流量转送到ER。</li><li>2. 在ER路由表中，通过下一跳为VGW连接的路由将流量转送到虚拟网关。</li><li>3. 虚拟网关连接虚拟接口，通过虚拟接口将流量从远端网关转送到物理专线。</li><li>4. 通过物理专线将流量送达线下IDC。</li></ol>
响应路径： 线下IDC → VPC1	<ol style="list-style-type: none"><li>1. 通过物理专线将流量转送到虚拟接口。</li><li>2. 虚拟接口连接虚拟网关，通过虚拟接口将流量从本端网关转送到虚拟网关。</li><li>3. 通过虚拟网关将流量转送到ER。</li><li>4. 在ER路由表中，通过下一跳为VPC1连接的路由将流量送达VPC1。</li></ol>

表 10-3 线下 IDC 和云上 VPC 互通组网规划说明

资源	说明
VPC	<ul style="list-style-type: none"><li>● VPC网段（CIDR）不能重叠。 本示例中，ER路由表使用的是“虚拟私有云（VPC）”连接的传播路由，由ER自动学习VPC网段作为目的地址，不支持修改，因此重叠的VPC网段会导致路由冲突。 如果您已有的VPC存在网段重叠，则不建议您使用传播路由，请在ER路由表中手动添加静态路由，目的地址可以为VPC子网网段或者范围更小的网段。</li><li>● VPC网段与客户IDC侧网段不能重复。</li><li>● VPC有一个默认路由表。</li><li>● VPC默认路由表中的路由说明如下：<ul style="list-style-type: none"><li>- local：表示VPC本地IPV4的默认路由条目，用于VPC内子网通信，系统自动配置。</li><li>- ER：表示将VPC子网流量路由至ER，为了减少路由数量，此处建议使用默认网段0.0.0.0/0，路由信息如表10-4所示。</li></ul></li></ul>
DC	<ul style="list-style-type: none"><li>● 1个物理连接：需要运营商施工搭建连通华为云和线下IDC的物理专线。</li><li>● 1个虚拟网关：将虚拟网关接入ER中，即表示将“虚拟网关（VGW）”连接添加到ER。</li><li>● 1个虚拟接口：连接虚拟网关和物理连接。</li></ul>

资源	说明
ER	<p>开启“默认路由表关联”和“默认路由表传播”功能，添加完“虚拟网关（VGW）”连接和“虚拟私有云（VPC）”连接，系统会自动执行以下配置：</p> <ul style="list-style-type: none"> <li>• DC: <ul style="list-style-type: none"> <li>- 将1个“虚拟网关（VGW）”连接关联至ER默认路由表。</li> <li>- 在默认路由表中创建“虚拟网关（VGW）”连接的传播，路由自动学习DC侧的所有路由信息，包括本端网关和远端网关、IDC侧网段等信息，路由信息如表10-5所示。</li> </ul> </li> <li>• VPC: <ul style="list-style-type: none"> <li>- 将2个“虚拟私有云（VPC）”连接关联至ER默认路由表。</li> <li>- 在默认路由表中创建“虚拟私有云（VPC）”连接的传播，路由自动学习VPC网段，路由信息如表10-5所示。</li> </ul> </li> </ul>
ECS	2个ECS分别位于不同的VPC内，VPC中的ECS如果位于不同的安全组，需要在安全组中添加规则放通网络。

表 10-4 VPC 路由表

目的地址	下一跳	路由类型
0.0.0.0/0	企业路由器	静态路由：自定义

### 📖 说明

- 如果您在创建连接时开启“配置连接侧路由”选项，则不用手动在VPC路由表中配置静态路由，系统会在VPC的所有路由表中自动添加指向ER的路由，目的地址固定为10.0.0.0/8，172.16.0.0/12，192.168.0.0/16。
- 如果VPC路由表中的路由与这三个固定网段冲突，则会添加失败。此时建议您不要开启“配置连接侧路由”选项，并在连接创建完成后，手动添加路由。
- 除了系统自动添加的3个VPC固定网段，您还需要在VPC路由表中添加目的地址为IDC侧网段，下一跳指向ER的路由。
- 为了减少路由数量，建议在VPC路由表中将ER的路由配置为默认路由网段0.0.0.0/0，但是VPC内的ECS将不能绑定EIP。如果VPC内的ECS绑定了EIP，会在ECS内增加默认网段的策略路由，并且优先级高于ER路由，此时会导致流量转发至EIP，无法抵达ER。

表 10-5 ER 路由表

目的地址	下一跳	路由类型
VPC1网段： 192.168.0.0/16	VPC1连接：er-attach-01	传播路由
VPC2网段：172.16.0.0/16	VPC2连接：er-attach-02	传播路由
本端网关和远端网关： 10.0.0.0/30	VGW连接：vgw-demo	传播路由

目的地址	下一跳	路由类型
IDC侧网段： 10.1.123.0/24	VGW连接：vgw-demo	传播路由

## 规划资源

企业路由器ER、云专线DC、虚拟私有云VPC、弹性云服务器ECS只要位于同一个区域内即可，可用区可以任意选择，不用保持一致。

### 说明

以下资源规划详情仅为示例，您可以根据需要自行修改。

- 企业路由器ER：1个，资源规划详情如表10-6所示。

表 10-6 ER 资源规划详情

ER名称	AS号	默认路由表关联	默认路由表传播	关联路由表	传播路由表	连接
er-test-01	64512	开启	开启	默认路由表	默认路由表	er-attach-01
						er-attach-02

- 云专线DC：资源规划详情如表10-7所示。

表 10-7 DC 资源规划详情

虚拟网关	虚拟接口	本端网关（华为云侧）	远端网关（用户侧）	远端子网	路由模式及BGP邻居AS号
vgw-demo	vif-demo	10.0.0.1/30	10.0.0.2/30	10.1.123.0/24	路由模式：BGP BGP邻居AS号：64510

- 虚拟私有云VPC：2个，VPC的网段不能重复，资源规划详情如表10-8所示。

表 10-8 VPC 资源规划详情

VPC名称	VPC网段	子网名称	子网网段	关联路由表
vpc-demo-01	192.168.0.0/16	subnet-demo-01	192.168.1.0/24	默认路由表
vpc-demo-02	172.16.0.0/16	subnet-demo-02	172.16.1.0/24	默认路由表

- 弹性云服务器ECS：2个，分别接入2个不同的VPC，资源规划详情如表10-9所示。

表 10-9 ECS 资源规划详情

ECS名称	镜像	VPC名称	子网名称	安全组	私有IP地址
ecs-demo-01	公共镜像： EulerOS 2.5 64bit	vpc-demo-01	subnet-demo-01	sg-demo： 通用We b 服务器	192.168. 1.99
ecs-demo-02		vpc-demo-02	subnet-demo-02		172.16.1. 137

## 10.3 创建资源

### 10.3.1 创建企业路由器

#### 操作场景

本章节指导用户创建企业路由器。

#### 操作步骤

**步骤1** 在区域A内，创建1个企业路由器。

创建企业路由器，具体方法请参见[创建企业路由器](#)。

企业路由器资源规划详情请参见[表10-6](#)。

----结束

### 10.3.2 创建 VPC 和 ECS

#### 操作场景

本章节指导用户创建虚拟私有云VPC和弹性云服务器ECS。

#### 操作步骤

**步骤1** 在区域A内，创建2个VPC和2个ECS。

创建VPC及子网，具体方法请参见[创建虚拟私有云和子网](#)。

创建ECS，具体方法请参见[自定义购买ECS](#)。

- 本示例中的VPC和子网资源规划详情请参见[表10-8](#)。
- 本示例中的ECS资源规划详情请参见[表10-9](#)。

----结束

### 10.3.3 创建云专线的物理连接

#### 操作场景

本章节指导用户在云专线中创建物理连接，物理连接指华为云和线下IDC通信的专属物理链路。

#### 操作步骤

**步骤1** 创建物理连接。

创建方法，具体请参见[物理连接接入](#)。

----结束

## 10.4 配置网络

### 10.4.1 在企业路由器中配置 VPC 连接

#### 操作场景

本章节指导用户在企业路由器中配置“虚拟私有云（VPC）”连接，即将VPC接入企业路由器中，并配置路由。

#### 操作步骤

**步骤1** 将2个VPC分别接入企业路由器中。

添加“虚拟私有云（VPC）”连接，具体方法请参见[在企业路由器中添加VPC连接](#)。

由于本示例创建ER时，开启“默认路由表关联”和“默认路由表传播”，因此添加完“虚拟私有云（VPC）”连接后，以下均为系统自动配置：

- 在默认路由表中创建关联
- 在默认路由表中创建传播，并自动学习VPC网段路由信息。

**步骤2** 在VPC路由表中配置ER的路由信息。

配置路由信息，具体方法请参见[在VPC路由表中配置路由](#)。

----结束

### 10.4.2 在企业路由器中配置 VGW 连接

#### 操作场景

本章节指导用户在企业路由器中配置“虚拟网关（VGW）”连接，即将DC专线接入企业路由器中，并配置路由。

#### 操作步骤

**步骤1** 创建虚拟网关，即在企业路由器中添加“虚拟网关（VGW）”连接。

1. 在云专线管理控制台，创建虚拟网关。  
具体方法请参见[步骤2：创建虚拟网关](#)。
2. 在企业路由器控制台，查看“虚拟网关（VGW）”连接的添加情况。  
具体方法请参见[查看连接](#)。  
“虚拟网关（VGW）”连接的状态“正常”，表示已成功接入企业路由器中。  
由于本示例创建ER时，开启“默认路由表关联”和“默认路由表传播”，因此添加完“虚拟网关（VGW）”连接后，以下均为系统自动配置：
  - 在ER默认路由表中创建关联
  - 在ER默认路由表中创建传播，并自动学习IDC侧的路由信息。  
需要执行[步骤2](#)创建虚拟接口后，才可以在ER路由表中查看到IDC侧的路由信息。

### 步骤2 创建虚拟接口。

创建虚拟接口用来连接虚拟网关和线下IDC，具体方法请参见[步骤3：创建虚拟接口](#)。

本示例中的虚拟接口的资源规划详情请参见[表10-7](#)。

### 步骤3 配置IDC侧路由到华为云的路由。

以华为网络设备为例，配置BGP路由：

```

bgp 64510
peer 10.0.0.1 as-number 64512
peer 10.0.0.1 password simple Qaz12345678
network 10.1.123.0 255.255.255.0

```

表 10-10 BGP 路由

命令	命令说明
<b>bgp 64510</b>	启动BGP，其中： 64510：IDC侧AS号。
<b>peer 10.0.0.1 as-number 64512</b>	创建BGP的对等体(EBGP)，其中： <ul style="list-style-type: none"> <li>• 10.0.0.1：华为云的网关。</li> <li>• 64512：华为云侧AS号，固定为64512。</li> </ul>
<b>peer 10.0.0.1 password simple Qaz12345678</b>	BGP对等体建立TCP连接时对BGP消息进行MD5认证，其中： Qaz12345678：BGP MD5认证密码。
<b>network 10.1.123.0 255.255.255.0</b>	将IP路由表中已存在的路由添加到BGP路由表中，其中： <ul style="list-style-type: none"> <li>• 10.1.123.0：IDC侧子网。</li> <li>• 255.255.255.0：IDC侧子网掩码。</li> </ul>

----结束

## 10.5 验证网络互通情况

**步骤1** 登录弹性云服务器。

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）。

**步骤2** 在弹性云服务器的远程登录窗口，执行以下命令，验证网络互通情况。

1. 执行以下命令，验证VPC网络互通情况。

**ping 弹性云服务器IP地址**

以登录ecs-demo-01，验证vpc-demo-01与vpc-demo-02的网络互通情况为例：

**ping 172.16.1.137**

回显如下信息，表示网络已通。

```
[root@ecs-demo-01 ~]# ping 172.16.1.137
PING 172.16.1.137 (172.16.1.137) 56(84) bytes of data.
64 bytes from 172.16.1.137: icmp_seq=1 ttl=64 time=0.455 ms
64 bytes from 172.16.1.137: icmp_seq=2 ttl=64 time=0.299 ms
64 bytes from 172.16.1.137: icmp_seq=3 ttl=64 time=0.232 ms
64 bytes from 172.16.1.137: icmp_seq=4 ttl=64 time=0.236 ms
^C
--- 172.16.1.137 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 92ms
rtt min/avg/max/mdev = 0.232/0.305/0.455/0.091 ms
```

2. 执行以下命令，验证VPC和DC网络互通情况。

**ping 本端网关（华为云侧）地址**

**ping 远端网关（IDC侧）地址**

**ping IDC侧IP地址**

以登录ecs-demo-01，验证vpc-demo-01与本端网关（华为云侧）的网络互通情况为例：

**ping 10.0.0.1**

回显如下信息，表示VPC与本端网关（华为云侧）的网络已通。

```
[root@ecs-demo-01 ~]# ping 10.0.0.1
PING 10.0.0.1 (10.0.0.1) 56(84) bytes of data.
64 bytes from 10.0.0.1: icmp_seq=1 ttl=255 time=7.90 ms
64 bytes from 10.0.0.1: icmp_seq=2 ttl=255 time=3.72 ms
64 bytes from 10.0.0.1: icmp_seq=3 ttl=255 time=3.22 ms
^C
--- 10.0.0.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 3.228/4.952/7.907/2.099 ms
[root@ecs-demo-01 ~]#
```

**步骤3** 重复执行**步骤1~步骤2**，验证其他VPC和DC之间的网络互通情况。

---结束

# 11 通过企业路由器构建 DC 双链路负载混合云组网 (虚拟网关 VGW)

## 11.1 方案概述

### 应用场景

云专线 (Direct Connect, DC) 用于搭建线下IDC和云上虚拟私有云 (Virtual Private Cloud, VPC) 之间高速、低时延、稳定安全的专属连接通道, 您可以通过企业路由器和云专线构建满足企业通信的大规模混合云组网。

通过企业路由器, 可以实现专线的动态选路和切换, 多个专线链路之间形成负载均衡, 有效扩展网络带宽, 增加吞吐量, 提升网络性能的同时保证高可靠性。

接下来, 将主要为您介绍如何通过企业路由器构建DC双链路负载混合云组网。

#### 📖 说明

您可以使用[企业路由器的共享功能](#), 将不同账号下的虚拟私有云添加至同一个企业路由器中构建组网。

如果您需要连通云上VPC和线下IDC构建混合云组网, 则推荐您使用企业路由器和云专线的全域接入网关DGW, 具体请参见[通过企业路由器构建DC双链路负载混合云组网 \(全域接入网关 DGW\)](#)。

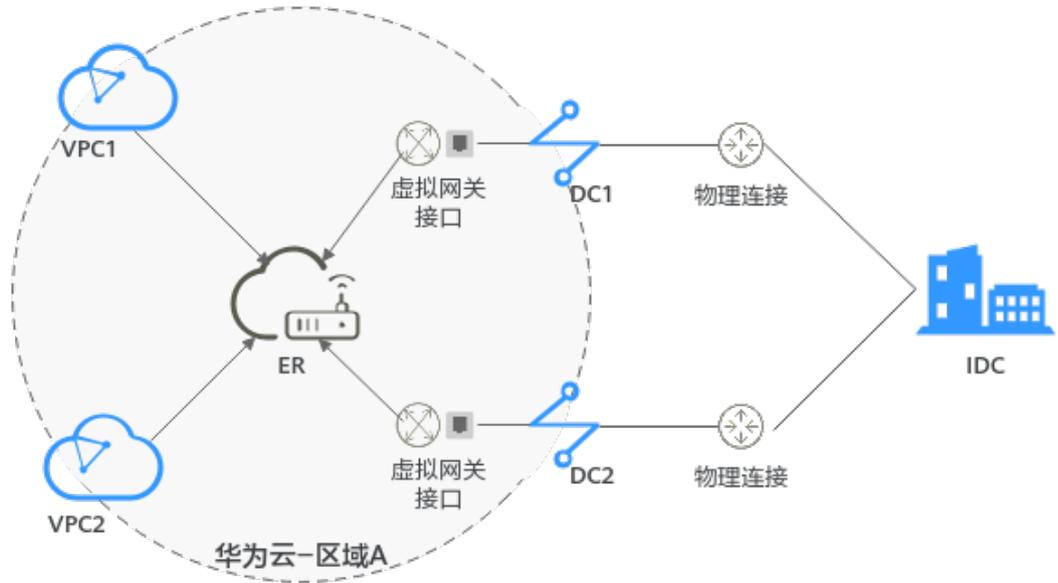
从2024年5月份开始, 通过企业路由器和云专线的虚拟网关VGW构建混合云组网的功能不再支持新增组网, 只针对存量组网进行维护。

### 方案架构

为了提升混合云组网的网络性能以及可靠性, XX企业同时部署了两条专线DC链路, 均可以连通云上VPC和线下IDC的网络。两条DC链路形成负载均衡, 当两条DC链路网络均正常, 同时工作可提升网络传输能力。当其中一条DC链路故障时, 另外一条DC链路可确保整个混合云组网的正常运行, 避免了单点故障带来的业务中断。

- 将VPC1、VPC2以及DC接入企业路由器中, VPC1和VPC2网络互通, 并且均可以通过两条DC和线下IDC通信。
- 当其中一条DC链路故障时, VPC1和VPC2可以通过另外一条DC链路和线下IDC通信。

图 11-1 DC 双链路负载混合云组网



### 方案优势

通过企业路由器，可以实现DC双链路负载模式，提升混合云组网的网络性能和高可靠性，避免网络链路单点故障时业务受损。

### 约束与限制

云上VPC子网网段与客户IDC侧子网网段不能重复。

## 11.2 组网和资源规划

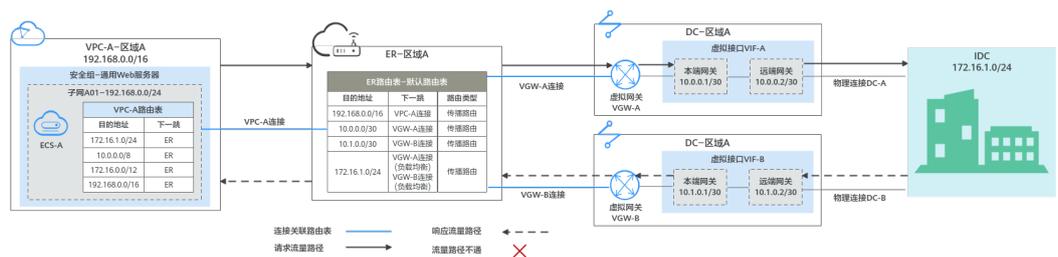
通过企业路由器构建DC双链路负载混合云组网，您需要规划资源和组网，本示例中为您详细介绍资源和组网情况。

- **网络规划说明：**规划VPC及其子网、DC和ER的网段、路由等。
- **资源规划说明：**规划云上资源的数量、名称以及主要参数等信息，云上资源包括VPC、DC以及ER等。

### 网络规划说明

DC双链路负载混合云组网规划如图11-2所示，将VPC、DC分别接入ER中，组网规划说明如表11-2所示。

图 11-2 DC 双链路负载混合云组网规划



两条DC网络链路形成负载均衡，云上VPC和线下IDC通信时，两条链路同时处于工作状态，表11-1为您介绍详细网络流量路径。

表 11-1 网络流量路径说明

路径	说明
请求路径： VPC-A → 线 下IDC	<ol style="list-style-type: none"><li>1. 在VPC-A路由表中，通过下一跳为ER的路由将流量转送到ER。</li><li>2. 在ER路由表中，通过下一跳为VGW-A连接的路由将流量转送到虚拟网关VGW-A。<ul style="list-style-type: none"><li>• 下一跳为VGW-A的路由，其中172.16.1.0/24为线下IDC子网网段地址，10.0.0.0/30为虚拟接口VIF-A的网关地址。</li><li>• 目的地址为172.16.1.0/24的路由，下一跳对应VGW-A和VGW-B，两条路由为等价路由，形成负载均衡。流量根据哈希算法，选择一条网络链路，此处以选择VGW-A，即DC-A为例。</li></ul></li><li>3. 虚拟网关VGW-A连接虚拟接口VIF-A，通过虚拟接口将流量从远端网关转送到物理连接。</li><li>4. 通过物理连接DC-A将流量送达线下IDC。</li></ol>
响应路径： 线下IDC → VPC-A	<ol style="list-style-type: none"><li>1. 根据线下IDC网络的路由配置，通过物理连接DC-B将流量转送到虚拟接口VIF-B。 线下IDC内网络中，指向云上的路由也配置成等价路由，形成负载均衡。返回云上VPC的流量，根据哈希算法选择一条网络链路，此处以选择DC-B为例。</li><li>2. 虚拟接口VIF-B连接虚拟网关VGW-B，通过虚拟接口将流量从本端网关转送到虚拟网关。</li><li>3. 通过虚拟网关VGW-B将流量转送到ER。</li><li>4. 在ER路由表中，通过下一跳为VPC-A连接的路由将流量送达VPC-A。</li></ol>

表 11-2 DC 双链路负载混合云组网规划说明

资源	说明
VPC	<p>业务VPC，实际运行客户业务的VPC，具体说明如下：</p> <ul style="list-style-type: none"><li>● VPC网段与客户IDC侧网段不能重复。</li><li>● VPC有一个默认路由表。</li><li>● VPC默认路由表中的路由信息如表11-3所示。<ul style="list-style-type: none"><li>- 固定网段：10.0.0.0/8、172.16.0.0/12、192.168.0.0/16三个固定网段是添加VPC连接时，开启“配置连接侧路由”选项，系统自动在VPC路由表配置的静态路由。如果ER内同时接入多个VPC连接，则这些路由可以将当前VPC访问其他VPC的路由转发至ER，再通过ER将流量转发至下一跳网络实例。</li><li>- 线下IDC侧网段：除了系统自动添加的3个VPC固定网段，您还需要在VPC路由表中添加目的地址为IDC侧网段，下一跳指向ER的路由，本示例为172.16.1.0/24，该路由可以将VPC访问线下IDC侧的流量转发至ER，再通过ER将流量转发至下一跳网络实例。</li></ul></li></ul> <p><b>须知</b> 如果VPC路由表中的路由与这三个固定网段冲突，则会添加失败。此时建议您不要开启“配置连接侧路由”选项，并在连接创建完成后，手动添加路由。</p>
DC	<p>两个DC需要构建负载均衡网络链路，具体如下：</p> <ul style="list-style-type: none"><li>● 2个物理连接：需要运营商施工搭建连通华为云和线下IDC的物理专线。</li><li>● 2个虚拟网关：将两个虚拟网关分别接入ER中，即表示将“虚拟网关（VGW）”连接添加到ER。</li><li>● 2个虚拟接口：分别连接两个虚拟网关和物理连接，两个虚拟接口之间形成负载分担。</li></ul>
ER	<p>开启“默认路由表关联”和“默认路由表传播”功能，添加完连接后，系统会自动执行以下配置：</p> <ul style="list-style-type: none"><li>● VPC：<ul style="list-style-type: none"><li>- 将1个“虚拟私有云（VPC）”连接关联至ER默认路由表。</li><li>- 在默认路由表中创建“虚拟私有云（VPC）”连接的传播，路由自动学习VPC网段，路由信息如表11-4所示。</li></ul></li><li>● DC：<ul style="list-style-type: none"><li>- 将2个“虚拟网关（VGW）”连接关联至ER默认路由表。</li><li>- 在默认路由表中创建“虚拟网关（VGW）”连接的传播，路由自动学习IDC侧的所有BGP路由信息，路由信息如表11-4所示。</li></ul></li></ul>

资源	说明
路由策略	<ul style="list-style-type: none"> <li>如果ER通过两个VGW连接学习的IDC侧的BGP路由是等价路由，自动形成负载均衡，则您无需创建路由策略。 本示例的表11-4中，目的地址为172.16.1.0/24，下一跳为VGW-A连接和VGW-B连接的两条路由是等价路由。</li> <li>如果ER通过两个VGW连接学习的IDC侧的BGP路由不是等价路由，无法自动形成负载均衡。则您需要在两个VGW连接的传播上，分别绑定路由策略。通过替换路由的AS_Path，将ER通过VGW连接去往IDC侧的路由形成等价路由。 您需要创建一个路由策略，添加两个节点： <ul style="list-style-type: none"> <li>策略节点1：优先级高，匹配BGP路由，对于匹配成功的路由，将路由的AS_Path值替换成虚拟网关的BGP ASN值。</li> <li>策略节点2：优先级低，匹配所有路由，此条节点是确保其他非BGP路由正常通信。</li> </ul> </li> </ul> <p>关于路由策略的详细说明，请您参见<a href="#">路由策略概述</a>。</p> <p><b>须知</b> 配置路由策略，替换路由的AS_Path值，可能会导致网络环路，因此配置前请检查网络规划，根据实际情况谨慎配置。</p>
ECS	<p>1个ECS位于业务VPC内，本示例用该ECS来验证云上和线下IDC的网络通信情况。</p> <p>如果您有多台ECS，并且这些ECS位于不同的安全组，需要在安全组中添加规则放通网络。</p>
IDC侧	<p>需要根据线下IDC侧网络的实际规划，将IDC侧去往云上ER的路由配置成等价路由，形成负载均衡。</p>

表 11-3 VPC 路由表

目的地址	下一跳	路由类型
固定网段：10.0.0.0/8	企业路由器	静态路由：自定义
固定网段：172.16.0.0/12	企业路由器	静态路由：自定义
固定网段：192.168.0.0/16	企业路由器	静态路由：自定义
线下IDC侧网段：172.16.1.0/24	企业路由器	静态路由：自定义

表 11-4 ER 路由表

目的地址	下一跳	路由类型
VPC-A网段：192.168.0.0/16	VPC-A连接：er-attach-vpc-A	传播路由

目的地址	下一跳	路由类型
VIF-A网关: 10.0.0.0/30	VGW-A连接: er-attach-vgw-A	传播路由
VIF-B网关: 10.1.0.0/30	VGW-B连接: er-attach-vgw-B	传播路由
IDC侧网段: 172.16.1.0/24	该路由为等价路由, 两个连接属于 负载均衡模式。 <ul style="list-style-type: none"> <li>VGW-A连接: er-attach-vgw-A</li> <li>VGW-B连接: er-attach-vgw-B</li> </ul>	传播路由

## 资源规划说明

企业路由器ER、云专线DC、虚拟私有云VPC、弹性云服务器ECS只要位于同一个区域内即可, 可用区可以任意选择, 不用保持一致。

### 说明

以下资源规划详情仅为示例, 您可以根据需要自行修改。

表 11-5 DC 双链路负载混合云组网资源规划总体说明

资源类型	资源数量	说明
VPC	1	业务VPC, 实际运行客户业务的VPC, 需要接入ER中。 <ul style="list-style-type: none"> <li>VPC名称: 请根据实际情况填写, 本示例为vpc-A。</li> <li>IPv4网段: VPC网段与客户IDC侧网段不能重复, 请根据实际情况填写, 本示例为192.168.0.0/16。</li> <li>子网名称: 请根据实际情况填写, 本示例为subnet-A01。</li> <li>子网IPv4网段: VPC子网网段与客户IDC侧子网网段不能重复, 请根据实际情况填写, 本示例为192.168.0.0/24。</li> </ul>
ER	1	<ul style="list-style-type: none"> <li>名称: 请根据实际情况填写, 本示例为er-X。</li> <li>ASN: 此处AS号不能和线下IDC的AS号一样, 本示例为64512。</li> <li>默认路由表关联: 开启</li> <li>默认路由表传播: 开启</li> <li>自动接受共享连接: 请根据实际情况选择, 本示例选择“开启”。</li> <li>连接, 本示例需要在企业路由器中添加3个连接:                             <ul style="list-style-type: none"> <li>VPC-A连接: er-attach-vpc-A</li> <li>VGW-A连接: er-attach-vgw-A</li> <li>VGW-B连接: er-attach-vgw-B</li> </ul> </li> </ul>

资源类型	资源数量	说明
路由策略	1	<p>如果ER通过两个VGW连接学习的IDC侧的BGP路由不是等价路由，无法自动形成负载均衡，则需要配置路由策略，为VGW-A连接和VGW-B连接分别绑定路由策略。</p> <p>路由策略中需要添加两个路由策略节点，本示例如下：</p> <ul style="list-style-type: none"> <li>策略节点1：优先级高，对于BGP路由，替换路由的AS_Path，将ER通过两个VGW连接学习到的路由配置成等价路由。 <ul style="list-style-type: none"> <li>节点号：节点号取值小的策略节点优先执行，因此策略节点1的节点号取值必须小于策略节点2，此处填写10。</li> <li>匹配模式：此处设置成“允许”。</li> <li>匹配条件：此处设置成“路由类型”、“BGP路由”。</li> <li>策略值1：此处设置成“AS_Path”。</li> <li>执行动作：此处设置成“替换”，替换值和虚拟网关的BGP ASN保持一致，请根据实际填写，本示例为“64513”。</li> </ul> </li> <li>策略节点2：优先级低，匹配所有路由，此条节点是确保其他非BGP路由正常通信。 <ul style="list-style-type: none"> <li>节点号：策略节点2的节点号取值必须大于策略节点1，此处填写20。</li> <li>匹配模式：此处设置成“允许”。</li> </ul> </li> </ul> <p>其他参数不填写，为空即可，表示未匹配上策略节点1的其他路由均可以匹配上策略节点2，确保路由策略可放行所有路由。</p>
DC	2	<p>物理连接：请根据实际需求创建。 本示例中，两个物理连接分别为dc-A和dc-B。</p> <p>虚拟网关，请根据实际需求创建，本示例说明如下：</p> <ul style="list-style-type: none"> <li>名称：请根据实际情况填写，本示例为vgw-A和vgw-B。</li> <li>关联模式：请选择“企业路由器”。</li> <li>企业路由器：选择您的企业路由器，本示例为er-X。</li> <li>BGP ASN：两个虚拟网关的AS号需要保持一致，虚拟网关和企业路由器的AS号一样或者不一样均可，本示例中两个虚拟网关的AS号均为64513。</li> </ul>

资源类型	资源数量	说明
		<p>虚拟接口，请根据实际需求创建，本示例说明如下：</p> <ul style="list-style-type: none"><li>● 名称：本示例两个虚拟接口分别为vif-A和vif-B。</li><li>● 虚拟接口优先级：此处两个虚拟接口均选择“优先”，表示形成负载均衡。</li><li>● 物理连接：本示例中虚拟接口vif-A关联的物理连接为dc-A，vif-B关联dc-B。</li><li>● 虚拟网关：本示例中虚拟接口vif-A关联的虚拟网关为vgw-A，vif-B关联vgw-B。</li><li>● 本端网关：本示例vif-A为10.0.0.1/30，vif-B为10.1.0.1/30。</li><li>● 远端网关：本示例vif-A为10.0.0.2/30，vif-B为10.1.0.2/30。</li><li>● 远端子网：此处为IDC侧子网网段，本示例为172.16.1.0/24。</li><li>● 路由模式：请选择“BGP”。</li><li>● BGP邻居AS号：此处为线下IDC侧的AS号，不能和云上虚拟网关、ER等服务的AS号一样，本示例为64555。</li></ul>
ECS	1	<p>ECS主要用来验证网络通信情况，本示例如下：</p> <ul style="list-style-type: none"><li>● 名称：根据实际情况填写，本示例为ecs-A。</li><li>● 镜像：请根据实际情况选择，本示例为公共镜像（CentOS 8.2 64bit）。</li><li>● 网络：<ul style="list-style-type: none"><li>- 虚拟私有云：选择业务VPC，本示例为vpc-A。</li><li>- 子网：选择和线下IDC通信的子网，本示例为subnet-A01。</li></ul></li><li>● 安全组：请根据实际情况选择，本示例安全组模板选择“通用Web服务器”，名称为sg-demo。</li><li>● 私有IP地址：192.168.0.137</li></ul>

#### 须知

- DC两条链路属于负载均衡模式，因此为了防止网络环路以及形成等价路由，DC两个虚拟网关的AS号必须保持一致，本示例为64513。
- ER的AS号和DC的一样或者不一样均可，本示例为64512。
- 线下IDC侧的AS号，不能和云上服务的AS号一样，请根据客户的实际情况填写，本示例为64555。

## 11.3 DC 双链路负载混合云组网构建流程

本章节介绍通过企业路由器构建DC双链路负载混合云组网总体流程，流程说明如表11-6所示。

表 11-6 构建 DC 双链路负载混合云组网流程说明

步骤	说明
<b>步骤一：创建云服务资源</b>	<ol style="list-style-type: none"> <li>1. 创建1个企业路由器，构建一个同区域组网只需要1个企业路由器。</li> <li>2. 创建业务VPC和子网，本示例中创建1个VPC和子网。</li> <li>3. 在业务VPC子网内，创建ECS，本示例中创建1个ECS。</li> </ol>
<b>步骤二：在企业路由器中添加并配置VPC连接</b>	<ol style="list-style-type: none"> <li>1. 在企业路由器中添加“虚拟私有云（VPC）”连接：将1个业务VPC接入企业路由器中。</li> <li>2. 在VPC路由表中配置路由：在VPC路由表中配置到企业路由器的路由信息，目的地址为IDC侧网段。</li> </ol>
<b>步骤三：在企业路由器中添加并配置VGW连接</b>	<ol style="list-style-type: none"> <li>1. 搭建第一条专线链路并验证网络通信情况。 <ol style="list-style-type: none"> <li>a. 创建1个物理连接：物理连接是线下IDC侧和华为云的专属通道，需要运营商进行施工，搭建物理专线链路连接线下和云上。</li> <li>b. 创建1个虚拟网关：创建关联企业路由器的虚拟网关，企业路由器中会自动添加“虚拟网关（VGW）”连接。</li> <li>c. 创建1个虚拟接口：虚拟接口用来连接虚拟网关和物理连接。</li> <li>d. 配置IDC侧路由：在线下IDC侧路由设备配置网络参数。</li> <li>e. 登录ECS，执行ping命令，验证DC链路通信情况。</li> </ol> </li> <li>2. 参考1，搭建第二条专线链路并验证网络通信情况。</li> </ol>
<b>步骤四：在ER侧和IDC侧分别配置等价路由</b>	<ol style="list-style-type: none"> <li>1. 在ER路由表中，检查ER通过VGW连接学习的BGP路由是否形成负载均衡。 <ol style="list-style-type: none"> <li>a. 如果形成负载均衡，则无需配置路由策略。</li> <li>b. 如果未形成负载均衡，则需要配置路由策略，执行2，在ER侧配置等价路由。</li> </ol> </li> <li>2. （可选）在ER侧配置等价路由，即创建路由策略并绑定至VGW连接的传播上。 配置路由策略，替换路由的AS_Path，可能会导致网络环路，配置前请检查网络规划，谨慎配置。 <ol style="list-style-type: none"> <li>a. 创建1个路由策略：路由策略中包含两个策略节点。</li> <li>b. 为VGW连接的传播绑定路由策略：分别将路由策略绑定至两个VGW连接上，将ER通过VGW连接学习的BGP路由形成等价路由。</li> </ol> </li> <li>3. 登录IDC侧网络设备，配置IDC侧的等价路由。</li> </ol>

## 11.4 DC 双链路负载混合云组网构建步骤

### 步骤一：创建云服务资源（业务 VPC、ECS、ER）

本步骤指导您创建业务VPC、ECS以及ER服务资源，云服务资源的总体规划说明，请参见表11-5。

**步骤1** 创建企业路由器。

创建企业路由器，具体方法请参见[创建企业路由器](#)。

**步骤2** 创建业务VPC。

创建VPC及子网，具体方法请参见[创建虚拟私有云和子网](#)。

**步骤3** 创建业务ECS。

本示例中1个业务ECS主要用于验证云上VPC和线下IDC通信使用，数量和配置仅供参考，请您根据实际需要创建业务ECS。

创建ECS，具体方法请参见[自定义购买ECS](#)。

----结束

**步骤二：在企业路由器中添加并配置 VPC 连接****步骤1** 将业务VPC接入企业路由器中，即在ER中添加VPC连接。

添加连接时，开启“配置连接侧路由”功能。

**须知**

开启该功能后，会在VPC路由表中自动添加指向ER的路由，目的地址固定为10.0.0.0/8，172.16.0.0/12，192.168.0.0/16。

添加“虚拟私有云（VPC）”连接，具体方法请参见[在企业路由器中添加VPC连接](#)。

**步骤2** 检查ER路由表中指向VPC的路由。

本示例中，ER开启了“默认路由表关联”和“默认路由表传播”功能，那么在ER中添加“虚拟私有云（VPC）”连接时，系统会自动添加ER指向VPC的路由，无需手动添加，只需要检查即可。

ER路由规划详情，请参见[表11-2](#)和[表11-4](#)。

本示例中，目的地址为192.168.0.0/16，下一跳为VPC-A连接的路由已自动添加。

查看ER路由，具体方法请参见[查看路由](#)。

**步骤3** 在业务VPC的路由表中，添加指向ER的路由。

VPC路由规划详情，请参见[表11-3](#)。

本示例中添加目的地址为线下IDC侧网段172.16.1.0/24的路由。

配置路由信息，具体方法请参见[在VPC路由表中配置路由](#)。

----结束

**步骤三：在企业路由器中添加并配置 VGW 连接**

本示例中，云专线DC资源的总体规划说明，请参见[表11-5](#)。

**步骤1** 执行以下步骤，搭建第一条专线链路并验证网络通信情况。

1. 创建物理连接。  
创建方法，具体请参见[物理连接接入](#)。
2. 创建虚拟网关，即在企业路由器中添加“虚拟网关（VGW）”连接。
  - a. 在云专线管理控制台，创建虚拟网关。  
具体方法请参见[步骤2：创建虚拟网关](#)。
  - b. 在企业路由器控制台，查看“虚拟网关（VGW）”连接的添加情况。  
具体方法请参见[查看连接](#)。  
“虚拟网关（VGW）”连接的状态“正常”，表示已成功接入企业路由器中。  
由于本示例创建ER时，开启“默认路由表关联”和“默认路由表传播”，因此添加完“虚拟网关（VGW）”连接后，以下均为系统自动配置：
    - 在ER默认路由表中创建关联。
    - 在ER默认路由表中创建传播，并自动学习IDC侧的路由信息。  
需要执行以下步骤连通DC后，才可以在ER路由表中查看到IDC侧的路由信息。
3. 创建虚拟接口。  
创建虚拟接口用来连接虚拟网关和线下IDC，具体方法请参见[步骤3：创建虚拟接口](#)。
4. 配置IDC侧路由到华为云的路由。  
以华为网络设备为例，配置BGP路由：
 

```

bgp 64555
peer 10.0.0.1 as-number 64512
peer 10.0.0.1 password simple Qaz12345678
network 172.16.1.0 255.255.255.0
      
```

表 11-7 BGP 路由

命令	命令说明
<b>bgp</b> 64555	启动BGP，其中： 64555：IDC侧AS号。
<b>peer</b> 10.0.0.1 as-number 64512	创建BGP的对等体(EBGP)，其中： - 10.0.0.1：华为云的网关。 - 64512：华为云侧AS号，固定为64512。
<b>peer</b> 10.0.0.1 password simple Qaz12345678	BGP对等体建立TCP连接时对BGP消息进行MD5认证，其中： Qaz12345678：BGP MD5认证密码。
<b>network</b> 172.16.1.0 255.255.255.0	将IP路由表中已存在的路由添加到BGP路由表中，其中： - 172.16.1.0：IDC侧子网。 - 255.255.255.0：IDC侧子网掩码。

5. 登录弹性云服务器ecs-A。  
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，验证第一条专线链路的通信情况。

**ping IDC侧任意一个IP地址**

命令示例：

**ping 172.16.1.10**

回显类似如下信息，表示vpc-A与IDC可以通过第一条专线链路通信。

```
[root@ecs-A ~]# ping 172.16.1.10
PING 172.16.1.10 (172.16.1.10) 56(84) bytes of data.
64 bytes from 172.16.1.10: icmp_seq=1 ttl=64 time=0.849 ms
64 bytes from 172.16.1.10: icmp_seq=2 ttl=64 time=0.455 ms
64 bytes from 172.16.1.10: icmp_seq=3 ttl=64 time=0.385 ms
64 bytes from 172.16.1.10: icmp_seq=4 ttl=64 time=0.372 ms
...
--- 172.16.1.10 ping statistics ---
```

**步骤2** 执行以下步骤，搭建第二条专线链路并验证网络通信情况。

1. 参考[步骤1.1~步骤1.4](#)，搭建第二条专线链路。
2. 构造第一条专线链路的故障，确保业务VPC已无法通过该链路和IDC通信。

#### 须知

请您务必在没有业务的情况下，构造专线链路故障，以免对业务造成影响。

3. 参考[步骤1.5~步骤1.6](#)，验证第二条专线链路的通信情况。

----结束

## 步骤四：在 ER 侧和 IDC 侧分别配置等价路由

**步骤1** 在ER路由表中，检查ER通过VGW连接学习的BGP路由是否形成负载均衡。

查看ER路由，具体方法请参见[查看路由](#)。

- 如果形成负载均衡，则无需配置路由策略。
- 如果未形成负载均衡，则需要配置路由策略，执行[步骤2](#)，在ER侧配置等价路由。  
当路由172.16.1.0/24的下一跳显示两个VGW连接时，则表示形成负载均衡模式。

**步骤2**（可选）在ER侧配置等价路由，即创建路由策略并绑定至VGW连接的传播上。

1. 创建路由策略，路由策略中包含两个策略节点。  
本示例中，路由策略的总体规划说明，请参见[表11-5](#)。  
创建路由策略，具体方法请参见[创建路由策略](#)。
2. 分别将路由策略绑定至两个VGW连接上，将ER通过VGW连接学习的BGP路由形成等价路由。  
为VGW连接的传播绑定路由策略，具体方法请参见[将路由策略绑定至ER连接的传播](#)。
3. 再次执行[步骤1](#)，检查路由是否形成负载均衡。

---

**须知**

配置路由策略，替换路由的AS\_Path值，可能会导致网络环路，因此配置前请检查网络规划，根据实际情况谨慎配置。

---

**步骤3** 登录线下IDC侧网络设备，需要根据网络的实际规划，将IDC侧去往云上ER的路由配置成等价路由，形成负载均衡。

----结束

# 12 通过企业路由器构建 DC/VPN 双链路主备混合云组网（虚拟网关 VGW）

## 12.1 方案概述

### 应用场景

云专线（Direct Connect，DC）用于搭建线下IDC和云上虚拟私有云（Virtual Private Cloud，VPC）之间高速、低时延、稳定安全的专属连接通道，您可以通过企业路由器和云专线构建满足企业通信的大规模混合云组网。

虚拟专用网络（Virtual Private Network，VPN）用于在线下IDC和云上VPC之间建立一条安全加密的公网通信隧道。相比通过DC构建混合云，使用VPN更加快速，成本更低。

为了助力企业客户实现混合云组网的高可靠性，并且控制成本费用，推荐您在企业路由器中同时接入DC和VPN两条网络链路，构建主备双链路的混合云组网。当主链路故障后，可自动切换至备链路，降低了单链路故障导致的业务中断风险。

#### 📖 说明

您可以使用[企业路由器的共享功能](#)，将不同账号下的虚拟私有云添加至同一个企业路由器中构建组网。

如果您需要连通云上VPC和线下IDC构建混合云组网，则推荐您使用企业路由器和云专线的全域接入网关DGW，具体请参见[通过企业路由器构建DC/VPN双链路主备混合云组网（全域接入网关DGW）](#)。

从2024年5月份开始，通过企业路由器和云专线的虚拟网关VGW构建混合云组网的功能不再支持新增组网，只针对存量组网进行维护。

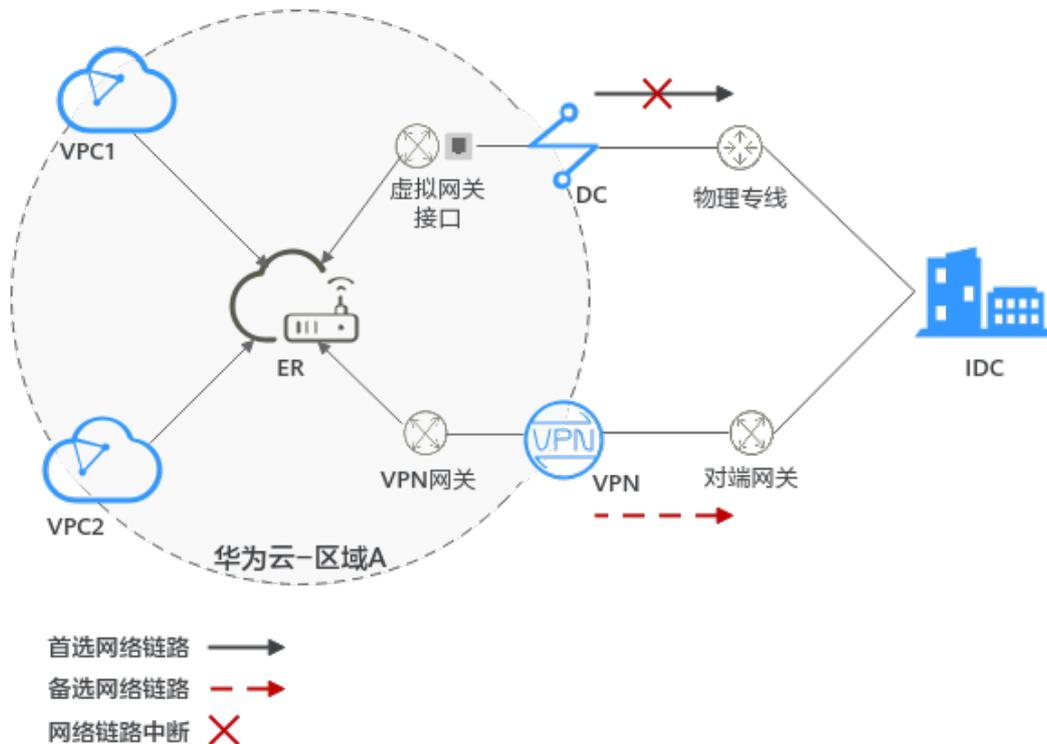
### 方案架构

为了提升混合云组网的可靠性，XX企业同时部署了DC和VPN两条网络链路，均可以连通云上VPC和线下IDC的网络。DC和VPN两条网络链路互为主备，主链路为DC，备链路为VPN，当DC链路故障时，可自动切换到VPN链路，降低网络中断对业务造成的影响。

- 将VPC1、VPC2以及DC接入企业路由器中，VPC1和VPC2网络互通，并且均可以通过DC和线下IDC通信。

- 将VPN接入企业路由器中，当主链路DC故障时，VPC1和VPC2可以通过备链路VPN和线下IDC通信。

图 12-1 DC/VPN 双链路主备混合云组网



## 方案优势

通过企业路由器，可以实现DC和VPN主备链路的自动切换，不需要手动切换双链路，不仅避免业务受损，同时降低维护成本。

## 约束与限制

云上VPC子网网段与客户IDC侧子网网段不能重复。

## 12.2 组网和资源规划

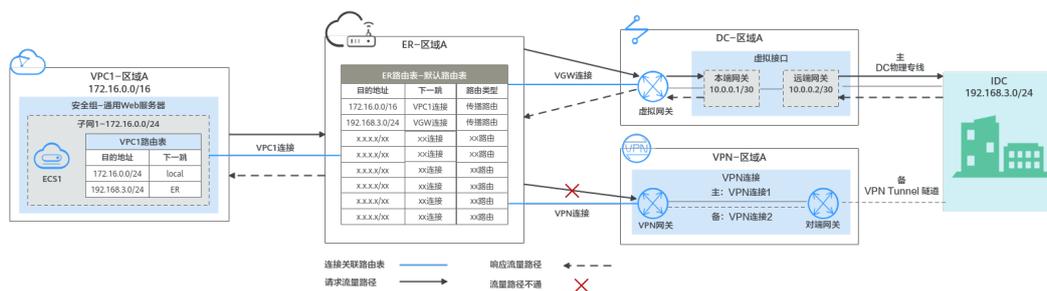
通过企业路由器构建DC/VPN双链路主备混合云组网，您需要规划资源和组网，本示例中为您详细介绍资源和组网情况。

- **网络规划说明**：规划VPC及其子网、DC、VPN和ER的网段、路由等。
- **资源规划说明**：规划云上资源的数量、名称以及主要参数等信息，云上资源包括VPC、DC、VPN以及ER等。

## 网络规划说明

DC/VPN双链路主备混合云组网规划如图12-2所示，将VPC、DC和VPN分别接入ER中，组网规划说明如表12-2所示。

图 12-2 DC/VPN 双链路主备混合云组网规划



DC和VPN互为备用网络链路，在DC网络链路正常的情况下，流量优选云专线DC。

- 在ER路由表中只显示优选路由，由于VGW连接(DC)路由的优先级高于VPN连接，因此ER路由表中不显示VPN连接的路由。
- 云上VPC和线下IDC通信时，默认使用DC这条网络链路，本示例的网络流量路径说明请参见表12-1

表 12-1 网络流量路径说明

路径	说明
请求路径： VPC1 → 线下 IDC	<ol style="list-style-type: none"> <li>1. 在VPC1路由表中，通过下一跳为ER的路由将流量转送到ER。</li> <li>2. 在ER路由表中，通过下一跳为VGW连接的路由将流量转送到虚拟网关。</li> <li>3. 虚拟网关连接虚拟接口，通过虚拟接口将流量从远端网关转送到物理专线。</li> <li>4. 通过物理专线将流量送达线下IDC。</li> </ol>
响应路径： 线下IDC → VPC1	<ol style="list-style-type: none"> <li>1. 通过物理专线将流量转送到虚拟接口。</li> <li>2. 虚拟接口连接虚拟网关，通过虚拟接口将流量从本端网关转送到虚拟网关。</li> <li>3. 通过虚拟网关将流量转送到ER。</li> <li>4. 在ER路由表中，通过下一跳为VPC1连接的路由将流量送达VPC1。</li> </ol>

表 12-2 DC/VPN 双链路互备混合云组网规划说明

资源	说明
VPC	<p>业务VPC，实际运行客户业务的VPC，本示例中为VPC1，具体说明如下：</p> <ul style="list-style-type: none"><li>● VPC网段与客户IDC侧网段不能重复。</li><li>● VPC有一个默认路由表。</li><li>● VPC默认路由表中的路由说明如下：<ul style="list-style-type: none"><li>- local：表示VPC本地IPV4的默认路由条目，用于VPC内子网通信，系统自动配置。</li><li>- ER：表示将VPC子网流量转发至ER，此处目的地址配置为IDC的子网网段，路由信息如表12-3所示。</li></ul></li></ul>
	<p>VPN网关使用的子网，建议您创建一个新的VPC，并从中分配子网。您在创建VPN网关时，需要填写该子网网段，VPN网关使用的子网不能与VPC内已有的子网网段重叠。</p>
DC	<ul style="list-style-type: none"><li>● 1个物理连接：需要运营商施工搭建连通华为云和线下IDC的物理专线。</li><li>● 1个虚拟网关：将虚拟网关接入ER中，即表示将“虚拟网关（VGW）”连接添加到ER。</li><li>● 1个虚拟接口：连接虚拟网关和物理连接。</li></ul>
VPN	<ul style="list-style-type: none"><li>● 1个VPN网关：将VPN接入ER中，即表示将“VPN网关（VPN）”连接添加到ER。</li><li>● 1个对端网关：用户IDC侧的对端网关。</li><li>● 2条VPN连接：连接VPN网关和对端网关，两条VPN连接互为主备链路。</li></ul>
ER	<p>开启“默认路由表关联”和“默认路由表传播”功能，添加完连接后，系统会自动执行以下配置：</p> <ul style="list-style-type: none"><li>● VPC：<ul style="list-style-type: none"><li>- 将1个“虚拟私有云（VPC）”连接关联至ER默认路由表。</li><li>- 在默认路由表中创建“虚拟私有云（VPC）”连接的传播，路由自动学习VPC网段，路由信息如表12-4所示。</li></ul></li><li>● DC：<ul style="list-style-type: none"><li>- 将1个“虚拟网关（VGW）”连接关联至ER默认路由表。</li><li>- 在默认路由表中创建“虚拟网关（VGW）”连接的传播，路由自动学习DC侧的所有路由信息，路由信息如表12-4所示。</li></ul></li><li>● VPN：<ul style="list-style-type: none"><li>- 将1个“VPN网关（VPN）”连接关联至ER默认路由表。</li><li>- 在默认路由表中创建“VPN网关（VPN）”连接的传播，路由自动学习VPN侧的所有路由信息，路由信息如表12-4所示。</li></ul></li></ul>

资源	说明
ECS	1个ECS位于业务VPC内，本示例用该ECS来验证云上和线下IDC的网络通信情况。 如果您有多台ECS，并且这些ECS位于不同的安全组，需要在安全组中添加规则放通网络。

表 12-3 VPC 路由表

目的地址	下一跳	路由类型
192.168.3.0/24	企业路由器	静态路由：自定义

### 说明

- 如果您在创建连接时开启“配置连接侧路由”选项，则不用手动在VPC路由表中配置静态路由，系统会在VPC的所有路由表中自动添加指向ER的路由，目的地址固定为10.0.0.0/8，172.16.0.0/12，192.168.0.0/16。
- 如果VPC路由表中的路由与这三个固定网段冲突，则会添加失败。此时建议您不要开启“配置连接侧路由”选项，并在连接创建完成后，手动添加路由。
- 除了系统自动添加的3个VPC固定网段，您还需要在VPC路由表中添加目的地址为IDC侧网段，下一跳指向ER的路由。

表 12-4 ER 路由表

目的地址	下一跳	路由类型
VPC1网段：172.16.0.0/16	VPC1连接：er-attach-01	传播路由
IDC侧网段： 192.168.3.0/24	VGW连接：vgw-demo	传播路由
IDC侧网段： 192.168.3.0/24	VPN连接：vpngw-demo	传播路由

### 须知

- 当两条路由功能一样时，ER路由表中只会显示优选路由。当DC和VPN网络链路均正常时，由于VGW连接和VPN连接的传播路由均指向线下IDC，因此只能在ER路由表中看到优先级较高的VGW连接的路由，暂时不支持查看ER路由中VPN连接的所有路由（包括未优选的路由）。
- 当DC出现故障，网络链路切换到VPN时，此时通过管理控制台，可以在ER路由表中看到VPN连接的传播路由。

## 资源规划说明

企业路由器ER、云专线DC、虚拟专用网络VPN、虚拟私有云VPC、弹性云服务器ECS只要位于同一个区域内即可，可用区可以任意选择，不用保持一致。

### 📖 说明

以下资源规划详情仅为示例，您可以根据需要自行修改。

表 12-5 DC/VPN 双链路互备混合云组网资源规划总体说明

资源类型	资源数量	说明
VPC	2	<p>业务VPC，实际运行客户业务的VPC，需要接入ER中。</p> <ul style="list-style-type: none"> <li>• VPC名称：请根据实际情况填写，本示例为vpc-for-er。</li> <li>• IPv4网段：VPC网段与客户IDC侧网段不能重复，请根据实际情况填写，本示例为172.16.0.0/16。</li> <li>• 子网名称：请根据实际情况填写，本示例为subnet-for-er。</li> <li>• 子网IPv4网段：VPC子网网段与客户IDC侧子网网段不能重复，请根据实际情况填写，本示例为172.16.0.0/24。</li> </ul> <p>VPN网关使用的VPC，需要从中分配一个子网提供给VPN网关使用。</p> <ul style="list-style-type: none"> <li>• VPC名称：请根据实际情况填写，本示例为vpc-for-vpn。</li> <li>• IPv4网段：请根据实际情况填写，本示例为10.0.0.0/16。</li> <li>• 子网名称：您创建VPC时，必须创建一个默认子网，请根据实际情况填写，本示例为subnet-01。</li> <li>• 子网IPv4网段：默认子网在本示例中不使用，请根据实际情况填写，本示例为10.0.0.0/24。</li> </ul> <p><b>须知</b> 您在创建VPN网关时，“虚拟私有云”需要选择该VPC，“互联子网”填写该VPC下未被占用的网段，该网段不能与VPC内已有的子网网段重叠。本示例中互联子网网段不能与默认子网subnet-01一样。</p>
ER	1	<ul style="list-style-type: none"> <li>• 名称：请根据实际情况填写，本示例为er-test-01。</li> <li>• ASN：此处AS号不能和线下IDC的AS号一样，本示例中保持默认值64512。</li> <li>• 默认路由表关联：开启</li> <li>• 默认路由表传播：开启</li> <li>• 自动接受共享连接：请根据实际情况选择，本示例选择“开启”。</li> <li>• 连接，本示例需要在企业路由器中添加3个连接： <ul style="list-style-type: none"> <li>- VPC连接：er-attach-VPC</li> <li>- VGW连接：er-attach-VGW</li> <li>- VPN连接：er-attach-VPN</li> </ul> </li> </ul>
DC	1	物理连接：请根据实际需求创建。

资源类型	资源数量	说明
		<p>虚拟网关</p> <ul style="list-style-type: none"> <li>名称：请根据实际情况填写，本示例为vgw-demo。</li> <li>关联模式：请选择“企业路由器”。</li> <li>企业路由器：选择您的企业路由器，本示例为er-test-01。</li> <li>BGP ASN：此处AS号和企业路由器的AS号一样或者不一样均可，本示例中和ER的AS号一致，保持默认值64512。</li> </ul> <p>虚拟接口</p> <ul style="list-style-type: none"> <li>名称：请根据实际情况填写，本示例vif-demo。</li> <li>虚拟网关：选择您的虚拟网关，本示例为vgw-demo。</li> <li>本端网关：请根据实际情况填写，本示例为10.0.0.1/30。</li> <li>远端网关：请根据实际情况填写，本示例为10.0.0.2/30。</li> <li>远端子网：请根据实际情况填写，本示例为192.168.3.0/24。</li> <li>路由模式：请选择“BGP”。</li> <li>BGP邻居AS号：此处为线下IDC侧的AS号，不能和云上虚拟网关的AS号一样，本示例为65525。</li> </ul>
VPN	1	<p>VPN网关</p> <ul style="list-style-type: none"> <li>名称：请根据实际情况填写，本示例为vpngw-demo。</li> <li>关联模式：请选择“企业路由器”。</li> <li>企业路由器：选择您的企业路由器，本示例为er-test-01。</li> <li>BGP ASN：由于DC和VPN为双链路互备，此处AS号和DC虚拟网关的AS号必须一样，本示例为64512。</li> <li>虚拟私有云：选择您的虚拟私有云，本示例为vpc-for-vpn。</li> <li>互联子网：互联子网是VPN网关实际使用的子网，该子网不能与VPC内已有的子网网段重叠，请根据实际情况填写，本示例为10.0.5.0/24。</li> </ul> <p>对端网关</p> <ul style="list-style-type: none"> <li>名称：请根据实际情况填写，本示例为cgw-demo。</li> <li>路由模式：请选择“动态BGP”。</li> <li>BGP ASN：此处为线下IDC侧的AS号，由于DC和VPN为双链路互备，该AS号和DC虚拟接口处设置的AS号必须一样，本示例为65525。</li> </ul>

资源类型	资源数量	说明
		<p>2条VPN连接，互为主动：</p> <ul style="list-style-type: none"><li>● 名称：请根据实际情况填写，本示例中，主VPN连接为vpn-demo-01，备VPN连接为vpn-demo-02。</li><li>● VPN网关：选择您的VPN网关，本示例为vpngw-demo。</li><li>● 公网IP：请根据实际情况选择，主VPN连接选择主EIP，备VPN连接选择备EIP。</li><li>● 连接模式：请选择“路由模式”。</li><li>● 对端网关：选择您的对端网关，本示例为cgw-demo。</li><li>● 接口分配方式：本示例选择“自动分配”。</li><li>● 路由模式：请选择“BGP”。</li></ul>
ECS	1	<ul style="list-style-type: none"><li>● 名称：根据实际情况填写，本示例为ecs-demo。</li><li>● 镜像：请根据实际情况选择，本示例为公共镜像（CentOS 8.2 64bit）。</li><li>● 网络：<ul style="list-style-type: none"><li>- 虚拟私有云：选择您的虚拟私有云，本示例为vpc-for-er。</li><li>- 子网：选择子网，本示例为subnet-for-er。</li></ul></li><li>● 安全组：请根据实际情况选择，本示例安全组模板选择“通用Web服务器”，名称为sg-demo。</li><li>● 私有IP地址：172.16.1.137</li></ul>

#### 须知

- 由于DC和VPN是主备链路，为了防止网络环路，DC虚拟网关和VPN网关的AS号必须保持一致，本示例为64512。
- ER的AS号和DC、VPN的一样或者不一样均可，本示例为64512。
- 线下IDC侧的AS号，不能和云上服务的AS号一样，请根据客户的实际情况填写，本示例为65525。

## 12.3 DC/VPN 双链路互备混合云组网构建流程

本章节介绍通过企业路由器构建DC/VPN双链路主备混合云组网总体流程，流程说明如表12-6所示。

表 12-6 构建 DC/VPN 双链路主备混合云组网流程说明

步骤	说明
<b>步骤一：创建云服务资源</b>	<ol style="list-style-type: none"> <li>1. 创建1个企业路由器，构建一个同区域组网只需要1个企业路由器。</li> <li>2. 创建业务VPC和子网，本示例中创建1个VPC和子网。</li> <li>3. 在业务VPC子网内，创建ECS，本示例中创建1个ECS。</li> </ol>
<b>步骤二：在企业路由器中添加并配置VGW连接</b>	<ol style="list-style-type: none"> <li>1. 创建物理连接，物理连接是线下IDC侧和华为云的专属通道，需要运营商进行施工，搭建物理专线链路连接线下和云上。</li> <li>2. 创建虚拟网关：创建1个关联企业路由器的虚拟网关，企业路由器中会自动添加“虚拟网关（VGW）”连接。</li> <li>3. 创建虚拟接口：创建关联虚拟网关的虚拟接口，连接虚拟网关和物理连接。</li> <li>4. 配置IDC侧路由：在线下IDC侧路由设备配置网络参数。</li> </ol>
<b>步骤三：在企业路由器中添加并配置VPC连接</b>	<ol style="list-style-type: none"> <li>1. 在企业路由器中添加“虚拟私有云（VPC）”连接：将1个业务VPC接入企业路由器中。</li> <li>2. 在VPC路由表中配置路由：在VPC路由表中配置到企业路由器的路由信息，目的地址为IDC侧网段。</li> </ol>
<b>步骤四：验证DC链路的通信情况</b>	登录ECS，执行ping命令，验证DC链路的网络互通情况。
<b>步骤五：在企业路由器中添加并配置VPN连接</b>	<ol style="list-style-type: none"> <li>1. 创建VPN网关：创建1个关联企业路由器的VPN网关，企业路由器中会自动添加“VPN网关（VPN）”连接。</li> <li>2. 创建对端网关：创建1个用户IDC侧的对端网关。</li> <li>3. 创建2条VPN连接：VPN连接用来连通VPN网关和对端网关，两条VPN连接互为主备链路。</li> <li>4. 配置IDC侧路由：在线下IDC侧路由设备配置网络参数。</li> </ol>
<b>步骤六：验证VPN链路的通信情况</b>	登录ECS，执行ping命令，验证VPN链路的网络互通情况。 由于VPN链路为备选，如果您需要验证VPN链路通信情况，需要先构造DC主链路故障，然后验证备VPN链路的通信情况。

## 12.4 DC/VPN 双链路互备混合云组网构建步骤

### 步骤一：创建云服务资源（业务 VPC、ECS、ER）

本步骤指导您创建业务VPC、ECS以及ER服务资源，云服务资源的总体规划说明，请参见表12-5。

#### 步骤1 创建企业路由器。

创建企业路由器，具体方法请参见[创建企业路由器](#)。

#### 步骤2 创建业务VPC。

创建VPC及子网，具体方法请参见[创建虚拟私有云和子网](#)。

**步骤3 创建业务ECS。**

本示例中1个业务ECS主要用于验证云上VPC和线下IDC通信使用，数量和配置仅供参考，请您根据实际需要创建业务ECS。

创建ECS，具体方法请参见[自定义购买ECS](#)。

----结束

**步骤二：在企业路由器中添加并配置 VGW 连接**

本示例中，云专线DC资源的总体规划说明，请参见[表12-5](#)。

**步骤1 创建物理连接。**

创建方法，具体请参见[物理连接接入](#)。

**步骤2 创建虚拟网关，即在企业路由器中添加“虚拟网关（VGW）”连接。**

1. 在云专线管理控制台，创建虚拟网关。  
具体方法请参见[步骤2：创建虚拟网关](#)。
2. 在企业路由器控制台，查看“虚拟网关（VGW）”连接的添加情况。  
具体方法请参见[查看连接](#)。

“虚拟网关（VGW）”连接的状态“正常”，表示已成功接入企业路由器中。

由于本示例创建ER时，开启“默认路由表关联”和“默认路由表传播”，因此添加完“虚拟网关（VGW）”连接后，以下均为系统自动配置：

- 在ER默认路由表中创建关联。
- 在ER默认路由表中创建传播，并自动学习IDC侧的路由信息。

需要执行以下步骤连通DC后，才可以在ER路由表中查看到IDC侧的路由信息。

**步骤3 创建虚拟接口。**

创建虚拟接口用来连接虚拟网关和线下IDC，具体方法请参见[步骤3：创建虚拟接口](#)。

**步骤4 在IDC侧的网络设备上，配置网络参数。**

由于组网为DC和VPN的双链路互备，因此配置路由时，需要注意以下方面：

- DC和VPN的路由类型保持一致，构造双链路互备需要配置为BGP路由。
- 配置DC和VPN路由的主备优先级，确保DC的优先级高于VPN。
- DC和VPN网络链路的断连感知时间建议和云上网络保持一致。

----结束

**步骤三：在企业路由器中添加并配置 VPC 连接****步骤1 将业务VPC接入企业路由器中。**

添加连接时，不开启“配置连接侧路由”功能。

**须知**

开启该功能后，会在VPC路由表中自动添加指向ER的路由，目的地址固定为10.0.0.0/8，172.16.0.0/12，192.168.0.0/16。本示例中，需要在VPC路由表中手动配置指向ER的路由，目的地址为IDC侧的网段。

添加“虚拟私有云（VPC）”连接，具体方法请参见[在企业路由器中添加VPC连接](#)。

**步骤2** 检查ER路由表中指向VPC的路由。

本示例中，ER开启了“默认路由表关联”和“默认路由表传播”功能，那么在ER中添加“虚拟私有云（VPC）”连接时，系统会自动添加ER指向VPC的路由，无需手动添加，只需要检查即可。

ER路由规划详情，请参见[表12-2](#)和[表12-4](#)。

查看ER路由，具体方法请参见[查看路由](#)。

**步骤3** 在业务VPC的路由表中，添加指向ER的路由。

VPC路由规划详情，请参见[表12-3](#)。

配置路由信息，具体方法请参见[在VPC路由表中配置路由](#)。

----结束

**步骤四：验证 DC 链路的通信情况****步骤1** 登录弹性云服务器ecs-demo。

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2** 执行以下命令，验证业务VPC与IDC是否可以通过ER通信。

**ping IDC侧任意一个IP地址**

命令示例：

**ping 192.168.3.10**

回显类似如下信息，表示vpc-for-er与IDC可以通过ER通信。

```
[root@ecs-demo ~]# ping 192.168.3.10
PING 192.168.3.10 (192.168.3.10) 56(84) bytes of data:
64 bytes from 192.168.3.10: icmp_seq=1 ttl=64 time=0.849 ms
64 bytes from 192.168.3.10: icmp_seq=2 ttl=64 time=0.455 ms
64 bytes from 192.168.3.10: icmp_seq=3 ttl=64 time=0.385 ms
64 bytes from 192.168.3.10: icmp_seq=4 ttl=64 time=0.372 ms
...
--- 192.168.3.10 ping statistics ---
```

----结束

**步骤五：在企业路由器中添加并配置 VPN 连接**

本示例中，虚拟专用网络VPN、VPN网关使用的VPC资源的总体规划说明，请参见[表12-5](#)。

**步骤1** 创建1个VPN网关使用的VPC。

创建VPC及子网，具体方法请参见[创建虚拟私有云和子网](#)。

### 须知

您在创建VPN网关时，“虚拟私有云”需要选择该VPC，“互联子网”填写该VPC下未被占用的网段，该网段不能与VPC内已有的子网网段重叠。本示例中互联子网网段不能与默认子网subnet-01一样。

**步骤2** 创建VPN网关，即在企业路由器中添加“VPN网关（VPN）”连接。

1. 在虚拟专用网络管理控制台，创建VPN网关。

具体方法请参见[创建VPN网关](#)。

2. 在企业路由器控制台，查看“VPN网关（VPN）”连接的添加情况。

具体方法请参见[查看连接](#)。

“VPN网关（VPN）”连接的状态“正常”，表示已成功接入企业路由器中。

由于本示例创建ER时，开启“默认路由表关联”和“默认路由表传播”，因此添加完“VPN网关（VPN）”连接后，以下均为系统自动配置：

- 在ER默认路由表中创建关联。
- 在ER默认路由表中创建传播，并自动学习IDC侧的路由信息。

需要执行以下步骤连通VPN后，才可以在ER路由表中查看到IDC侧的路由信息。

**步骤3** 创建对端网关。

具体方法请参见[创建对端网关](#)。

**步骤4** 分别创建两条VPN连接，用作主备。

1. 创建主VPN连接，请参见[创建第一条VPN连接](#)。

2. 创建备VPN连接，请参见[创建第二条VPN连接](#)。

**步骤5** 在IDC侧的网络设备上，配置网络参数。

由于组网为DC和VPN的双链路互备，因此配置路由时，需要注意以下方面：

- DC和VPN的路由类型保持一致，构造双链路互备需要配置为BGP路由。
- 配置DC和VPN路由的主备优先级，确保DC的优先级高于VPN。
- DC和VPN网络链路的断连感知时间建议和云上网络保持一致。

----结束

## 步骤六：验证 VPN 链路的通信情况

由于VPN链路为备选，如果您需要验证VPN链路通信情况，需要先构造DC主链路故障，然后验证备VPN链路的通信情况。

**步骤1** 构造DC主链路的故障，确保业务VPC已无法通过该链路和IDC通信。

### 须知

请您务必在没有业务的情况下，构造DC链路故障，以免对业务造成影响。

**步骤2** 登录弹性云服务器ecs-demo。

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3** 执行以下命令，验证业务VPC与IDC是否可以通过ER通信。

**ping IDC侧任意一个IP地址**

命令示例：

**ping 192.168.3.10**

回显类似如下信息，表示vpc-for-er与IDC可以通过ER通信。

```
[root@ecs-demo ~]# ping 192.168.3.10
PING 192.168.3.10 (192.168.3.10) 56(84) bytes of data.
64 bytes from 192.168.3.10: icmp_seq=1 ttl=64 time=0.849 ms
64 bytes from 192.168.3.10: icmp_seq=2 ttl=64 time=0.455 ms
64 bytes from 192.168.3.10: icmp_seq=3 ttl=64 time=0.385 ms
64 bytes from 192.168.3.10: icmp_seq=4 ttl=64 time=0.372 ms
...
--- 192.168.3.10 ping statistics ---
```

----**结束**

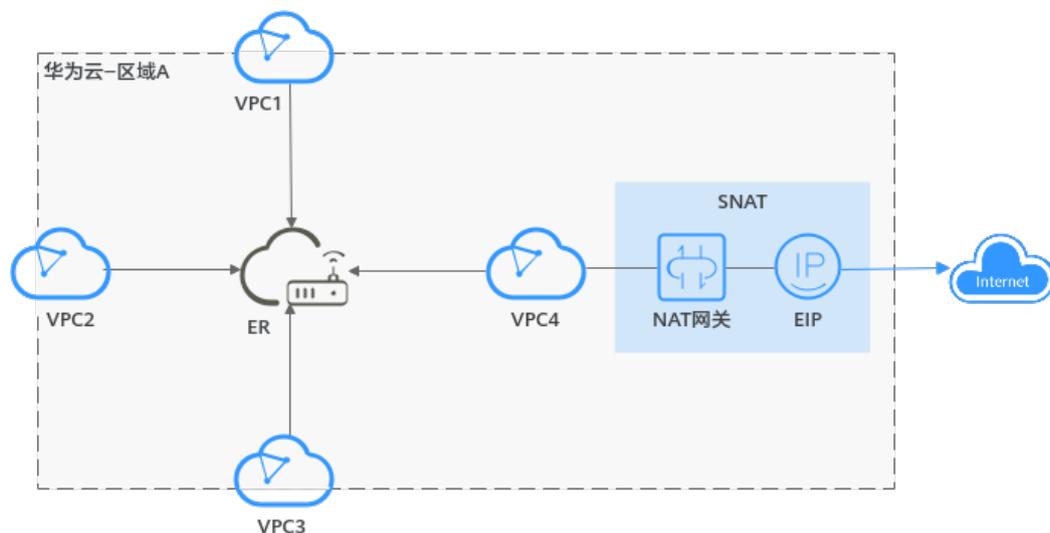
# 13 通过企业路由器和 NAT 网关实现多个 VPC 共享 SNAT 访问公网

## 13.1 方案概述

### 背景信息

XX企业在华为云区域A内部署了4个虚拟私有云VPC，VPC1、VPC2、VPC3需要互相访问，并且可以共享VPC4的SNAT访问公网。

图 13-1 VPC 共享 SNAT



### 说明

您可以使用[企业路由器的共享功能](#)，将不同账号下的虚拟私有云添加至同一个企业路由器中构建组网。

### 操作流程

本文档介绍如何通过企业路由器构建同区域VPC共享SNAT组网，流程如[图13-2](#)所示。

图 13-2 构建同区域 VPC 共享 SNAT 组网流程图

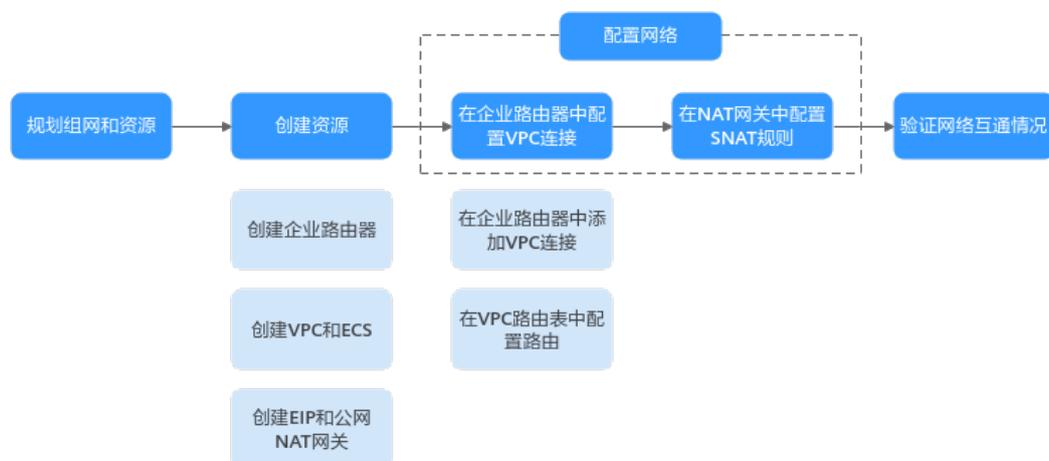


表 13-1 构建同区域 VPC 共享 SNAT 组网流程说明

序号	步骤	说明
1	规划组网和资源	规划组网和资源，包括资源数量及网段信息等。
2	创建资源	<ol style="list-style-type: none"> <li><b>创建企业路由器</b>：创建1个企业路由器，构建一个同区域组网只需要1个企业路由器。</li> <li><b>创建VPC和ECS</b>：创建4个虚拟私有云VPC和3个弹性云服务器ECS，其中一个VPC用来创建NAT网关实例。</li> <li><b>创建EIP和公网NAT网关</b>：创建弹性公网IP，基于一个独立的VPC创建公网NAT网关。</li> </ol>
3	配置网络	<ol style="list-style-type: none"> <li><b>在企业路由器中配置VPC连接</b>： <ol style="list-style-type: none"> <li>在企业路由器中添加“虚拟私有云（VPC）”连接：将4个VPC分别接入企业路由器中。</li> <li>在VPC路由表中配置路由：在VPC路由表中配置到企业路由器的路由信息。</li> </ol> </li> <li><b>在NAT网关中配置SNAT规则</b>：在NAT网关中添加VPC的SNAT规则。</li> </ol>
4	验证网络互通情况	登录ECS，执行ping命令，验证网络互通情况。

## 13.2 规划组网和资源

通过企业路由器构建同区域VPC共享SNAT组网，您需要规划组网和资源：

- **规划组网**：规划VPC及其子网的网段、弹性公网IP、公网NAT网关、VPC路由表和ER路由表信息。
- **规划资源**：规划云上资源的数量、名称以及主要参数等信息，云上资源包括VPC、EIP、NAT网关、ECS以及ER。

## 规划组网

同区域VPC共享SNAT组网规划如图13-3所示，将4个VPC接入ER中，组网规划说明如表13-3所示。

图 13-3 同区域 VPC 共享 SNAT 组网规划

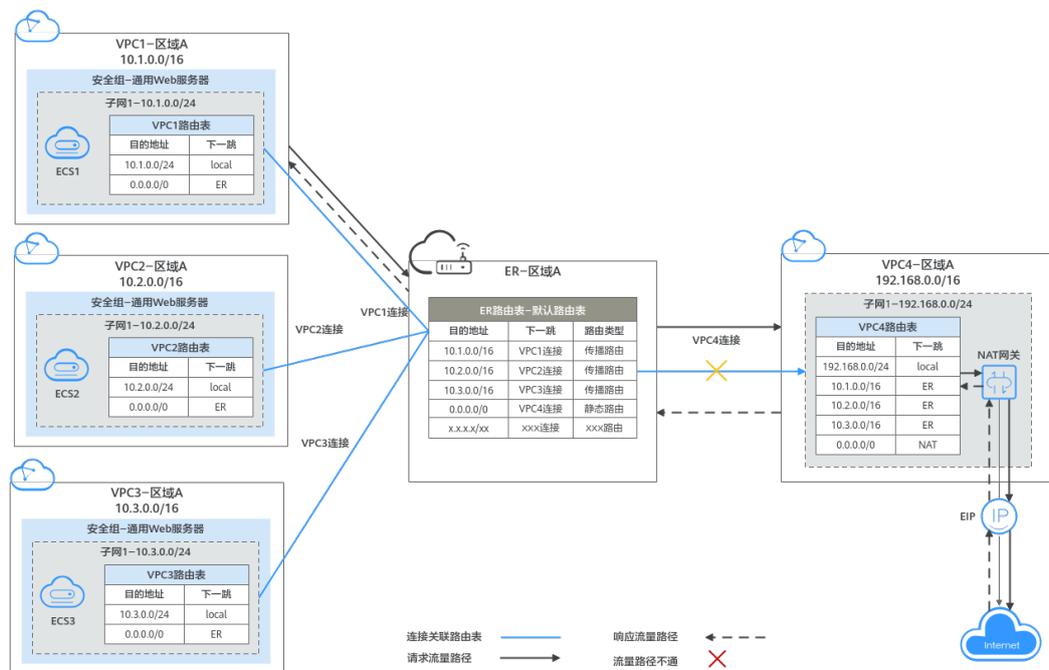


表 13-2 网络流量路径说明

路径	说明
请求路径： VPC1 → Internet	<ol style="list-style-type: none"> <li>1. 在VPC1路由表中，通过下一跳为ER的路由将流量转送到ER。</li> <li>2. 在ER路由表中，通过下一跳为VPC4连接的静态路由将流量转送到VPC4。</li> <li>3. 在VPC4路由表中，通过下一跳为NAT的路由将流量转送到NAT网关。</li> <li>4. 在NAT网关中，通过SNAT规则绑定的弹性IP将流量送达公网目的地址。</li> </ol>
响应路径： Internet → VPC1	<ol style="list-style-type: none"> <li>1. 公网目的地址通过SNAT规则绑定的弹性IP将流量转送到NAT网关。</li> <li>2. 在NAT网关中，通过SNAT规则将流量转送到VPC4。</li> <li>3. 在VPC4路由表中，通过下一跳为ER的路由将流量转送到ER。</li> <li>4. 在ER路由表中，通过下一跳为VPC1连接的传播路由将流量转送到VPC1。</li> </ol>

表 13-3 同区域 VPC 共享 SNAT 组网规划说明

资源	说明
VPC	<ul style="list-style-type: none"> <li>● VPC网段（CIDR）不能重叠。 本示例中，ER路由表使用的是“虚拟私有云（VPC）”连接的传播路由，由ER自动学习VPC网段作为目的地址，不支持修改，因此重叠的VPC网段会导致路由冲突。 如果您已有的VPC存在网段重叠，则不建议您使用传播路由，请在ER路由表中手动添加静态路由，目的地址可以为VPC子网网段或者范围更小的网段。</li> <li>● VPC有一个默认路由表。</li> <li>● VPC默认路由表中的路由说明如下： <ul style="list-style-type: none"> <li>- local：表示VPC本地IPV4的默认路由条目，用于VPC内子网通信，系统自动配置。</li> <li>- ER：表示将VPC子网流量路由至ER，自定义路由。 为了减少路由数量，此处建议VPC1、VPC2和VPC3使用默认网段0.0.0.0/0，路由信息如表13-4所示。 在VPC4中，会自动添加下一跳为NAT网关，网段为0.0.0.0/0的路由，为了不和NAT网关的路由冲突，此处到ER路由的目的地址需要配置成VPC的实际网段，路由信息如表13-5所示。</li> <li>- NAT：表示将VPC子网流量路由至NAT网关，创建NAT网关时系统自动配置。</li> </ul> </li> </ul>
NAT	基于VPC4创建公网NAT网关，并关联EIP配置SNAT规则。
ER	<ul style="list-style-type: none"> <li>● 开启“默认路由表关联”和“默认路由表传播”功能，添加完“虚拟私有云（VPC）”连接，系统会自动执行以下配置： <ul style="list-style-type: none"> <li>- 将4个“虚拟私有云（VPC）”连接关联至ER默认路由表。</li> <li>- 在默认路由表中创建“虚拟私有云（VPC）”连接的传播，路由自动学习VPC网段，路由信息如表13-6所示。</li> </ul> </li> <li>● 在ER路由表中，添加静态路由，网段为0.0.0.0/0，表示将访问公网的流量路由至VPC4。</li> </ul>
ECS	3个ECS分别位于3个不同的VPC内，VPC中的ECS如果位于不同的安全组，需要在安全组中添加规则放通对端安全组的网络。

表 13-4 VPC1/VPC2/VPC3 路由表

目的地址	下一跳	路由类型
0.0.0.0/0	企业路由器	静态路由：自定义

**说明**

- 如果您在创建连接时开启“配置连接侧路由”选项，则不用手动在VPC路由表中配置静态路由，系统会在VPC的所有路由表中自动添加指向ER的路由，目的地址固定为10.0.0.0/8，172.16.0.0/12，192.168.0.0/16。
- 如果VPC路由表中的路由与这三个固定网段冲突，则会添加失败。此时建议您不要开启“配置连接侧路由”选项，并在连接创建完成后，手动添加路由。
- 除了系统自动添加的3个VPC固定网段，您还需要在VPC路由表中添加目的地址为公网侧网段，下一跳指向ER的路由。
- 为了减少路由数量，建议在VPC路由表中将ER的路由配置为默认路由网段0.0.0.0/0，但是VPC内的ECS将不能绑定EIP。如果VPC内的ECS绑定了EIP，会在ECS内增加默认网段的策略路由，并且优先级高于ER路由，此时会导致流量转发至EIP，无法抵达ER。

**表 13-5 VPC4 路由表**

目的地址	下一跳	路由类型
VPC1网段：10.1.0.0/16	企业路由器	静态路由：自定义
VPC2网段：10.2.0.0/16	企业路由器	静态路由：自定义
VPC3网段：10.3.0.0/16	企业路由器	静态路由：自定义
0.0.0.0/0	NAT网关	静态路由：自定义

**说明**

- 建议您添加连接时，不要开启“配置连接侧路由”选项，并在企业路由器创建完成后，在VPC路由表中手动添加路由。
- VPC内的ECS不能绑定EIP，如果ECS绑定了EIP，会在ECS内增加默认网段0.0.0.0/0的策略路由，并且优先级高于NAT网关路由，因此会导致流量转发至EIP，无法抵达NAT网关，流量中断。

**表 13-6 ER 路由表**

目的地址	下一跳	路由类型
VPC1网段：10.1.0.0/16	VPC1连接：er-attach-business-01	传播路由
VPC2网段：10.2.0.0/16	VPC2连接：er-attach-business-02	传播路由
VPC3网段：10.3.0.0/16	VPC3连接：er-attach-business-03	传播路由
0.0.0.0/0	VPC4连接：er-attach-nat	静态路由

**规划资源**

企业路由器ER、NAT网关、弹性公网IP、虚拟私有云VPC、弹性云服务器ECS只要位于同一个区域内即可，可用区可以任意选择，不用保持一致。

 说明

以下资源规划详情仅为示例，您可以根据需要自行修改。

- 企业路由器ER：1个，资源规划详情如表13-7所示。

表 13-7 ER 资源规划详情

ER名称	AS号	默认路由表关联	默认路由表传播	关联路由表	传播路由表	连接
er-test-01	64512	开启	开启	默认路由表	默认路由表	er-attach-business-01
						er-attach-business-02
						er-attach-business-03
						er-attach-nat

- 弹性公网IP：1个，线路和带宽参数请根据实际需求创建，本示例IP地址为123.60.73.78。
- 公网NAT网关：1个，资源规划详情如表13-8所示。

表 13-8 公网 NAT 网关资源规划详情

公网NAT网关名称	VPC名称	子网名称	SNAT使用场景	SNAT子网
nat-demo	vpc-nat	subnet-nat	虚拟私有云	自定义：0.0.0.0/0

- 虚拟私有云VPC：4个，VPC的网段不能重复，资源规划详情如表13-9所示。

表 13-9 VPC 资源规划详情

VPC名称	VPC网段	子网名称	子网网段	关联路由表
vpc-business-01	10.1.0.0/16	subnet-business-01	10.1.0.0/24	默认路由表
vpc-business-02	10.2.0.0/16	subnet-business-02	10.2.0.0/24	默认路由表

VPC名称	VPC网段	子网名称	子网网段	关联路由表
vpc-business-03	10.3.0.0/16	subnet-business-03	10.3.0.0/24	默认路由表
vpc-nat	192.168.0.0/16	subnet-nat	192.168.0.0/24	默认路由表

- 弹性云服务器ECS：3个，分别接入3个不同的VPC，资源规划详情如表13-10所示。

表 13-10 ECS 资源规划详情

ECS名称	镜像	VPC名称	子网名称	安全组	私有IP地址
ecs-business-01	公共镜像： CentOS 7.5 64bit	vpc-business-01	subnet-business-01	sg-demo： 通用Web 服务器	10.1.0.13 4
ecs-business-02		vpc-business-02	subnet-business-02		10.2.0.21 5
ecs-business-03		vpc-business-03	subnet-business-03		10.3.0.14

## 13.3 创建资源

### 13.3.1 创建企业路由器

#### 操作场景

本章节指导用户创建企业路由器。

#### 操作步骤

**步骤1** 在区域A内，创建1个企业路由器。

创建企业路由器，具体方法请参见[创建企业路由器](#)。

企业路由器资源规划详情请参见[表13-7](#)。

----结束

### 13.3.2 创建 VPC 和 ECS

#### 操作场景

本章节指导用户创建虚拟私有云VPC和弹性云服务器ECS。

## 操作步骤

**步骤1** 在区域A内，创建4个VPC和3个ECS。

创建VPC及子网，具体方法请参见[创建虚拟私有云和子网](#)。

创建ECS，具体方法请参见[自定义购买ECS](#)。

- 本示例中的VPC和子网资源规划详情请参见[表13-9](#)。
- 本示例中的ECS资源规划详情请参见[表13-10](#)。

----结束

### 13.3.3 创建 EIP 和公网 NAT 网关

#### 操作场景

本章节指导用户创建弹性公网IP和公网NAT网关。

#### 操作步骤

**步骤1** 在区域A内，创建EIP。

创建EIP，具体方法请参见[申请弹性公网IP](#)。

**步骤2** 在区域A内，创建公网NAT网关。

创建公网NAT网关，具体方法请参见[购买公网NAT网关](#)。

本示例中公网NAT网关资源规划详情请参见[表13-8](#)。

----结束

## 13.4 配置网络

### 13.4.1 在企业路由器中配置 VPC 连接

#### 操作场景

本章节指导用户在企业路由器中配置“虚拟私有云（VPC）”连接，即将VPC接入企业路由器中，并配置企业路由器和VPC的路由。

#### 操作步骤

**步骤1** 将4个VPC分别接入企业路由器中。

添加“虚拟私有云（VPC）”连接，具体方法请参见[在企业路由器中添加VPC连接](#)。

由于本示例创建ER时，开启“默认路由表关联”和“默认路由表传播”，因此添加完“虚拟私有云（VPC）”连接后，以下均为系统自动配置：

- 在默认路由表中创建关联
- 在默认路由表中创建传播，并自动学习VPC网段路由信息。

**步骤2** 在ER路由表中创建下一跳为VPC4连接的静态路由，网段为0.0.0.0/0，表示将访问公网的流量路由至VPC4。

创建静态路由，具体方法请参见[创建静态路由](#)。

创建VPC4的静态路由后，可以删除VPC4的传播路由，具体方法请参见[删除传播](#)。

**步骤3** 在VPC路由表中配置ER的路由信息。

配置路由信息，具体方法请参见[在VPC路由表中配置路由](#)。

- VPC1/VPC2/VPC3的路由配置相同，具体请参见[表13-4](#)。
- VPC4的路由配置，具体请参见[表13-5](#)。

----结束

## 13.4.2 在 NAT 网关中配置 SNAT 规则

### 操作场景

本章节指导用户在公网NAT网关中添加SNAT规则，实现访问公网。

### 操作步骤

**步骤1** 在公网NAT网关中，配置SNAT规则。

配置SNAT规则，具体方法请参见[添加SNAT规则](#)。

本示例中SNAT规划详情请参见[表13-8](#)。

----结束

## 13.5 验证网络互通情况

**步骤1** 登录弹性云服务器。

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）。

**步骤2** 在弹性云服务器的远程登录窗口，执行以下步骤，验证网络情况。

1. 执行以下命令，验证VPC网络互通情况。

**ping 弹性云服务器IP地址**

以登录ecs-business-01，验证vpc-business-01与vpc-business-02、vpc-business-03的网络互通情况为例：

**ping 10.2.0.215**

**ping 10.3.0.14**

回显如下信息，表示网络互通配置成功。

```
PING 10.2.0.215 (10.2.0.215) 56(84) bytes of data.  
64 bytes from 10.2.0.215: icmp_seq=1 ttl=64 time=0.460 ms  
64 bytes from 10.2.0.215: icmp_seq=2 ttl=64 time=0.358 ms  
64 bytes from 10.2.0.215: icmp_seq=3 ttl=64 time=0.345 ms  
64 bytes from 10.2.0.215: icmp_seq=4 ttl=64 time=0.303 ms  
64 bytes from 10.2.0.215: icmp_seq=5 ttl=64 time=0.289 ms  
64 bytes from 10.2.0.215: icmp_seq=6 ttl=64 time=0.262 ms  
64 bytes from 10.2.0.215: icmp_seq=7 ttl=64 time=0.297 ms  
^C  
--- 10.2.0.215 ping statistics ---  
7 packets transmitted, 7 received, 0% packet loss, time 6008ms  
rtt min/avg/max/mdev = 0.262/0.330/0.460/0.064 ms
```

```
PING 10.3.0.14 (10.3.0.14) 56(84) bytes of data.  
64 bytes from 10.3.0.14: icmp_seq=1 ttl=64 time=0.900 ms  
64 bytes from 10.3.0.14: icmp_seq=2 ttl=64 time=1.87 ms  
64 bytes from 10.3.0.14: icmp_seq=3 ttl=64 time=0.323 ms  
64 bytes from 10.3.0.14: icmp_seq=4 ttl=64 time=0.315 ms  
64 bytes from 10.3.0.14: icmp_seq=5 ttl=64 time=0.296 ms  
64 bytes from 10.3.0.14: icmp_seq=6 ttl=64 time=0.286 ms  
64 bytes from 10.3.0.14: icmp_seq=7 ttl=64 time=0.281 ms  
^C  
--- 10.3.0.14 ping statistics ---  
7 packets transmitted, 7 received, 0% packet loss, time 6008ms  
rtt min/avg/max/mdev = 0.281/0.610/1.874/0.556 ms
```

2. 执行以下命令，验证VPC访问公网情况。

**ping 公网IP地址或者域名**

以登录ecs-isolation-01，验证vpc-business-01与公网网络互通情况为例：

**ping support.huaweicloud.com**

回显如下信息，表示网络互通。

```
[root@ecs-1-1-1 ~]# ping support.huaweicloud.com  
PING cdn-plmz674n.sched.s2.tdnsv5.com (117.41.241.211) 56(84) bytes of data.  
64 bytes from 117.41.241.211 (117.41.241.211): icmp_seq=1 ttl=52 time=17.10 ms  
64 bytes from 117.41.241.211 (117.41.241.211): icmp_seq=2 ttl=52 time=17.7 ms  
64 bytes from 117.41.241.211 (117.41.241.211): icmp_seq=3 ttl=52 time=17.6 ms  
64 bytes from 117.41.241.211 (117.41.241.211): icmp_seq=4 ttl=52 time=17.8 ms  
64 bytes from 117.41.241.211 (117.41.241.211): icmp_seq=5 ttl=52 time=17.7 ms  
64 bytes from 117.41.241.211 (117.41.241.211): icmp_seq=6 ttl=52 time=17.6 ms  
64 bytes from 117.41.241.211 (117.41.241.211): icmp_seq=7 ttl=52 time=17.7 ms  
^C  
--- cdn-plmz674n.sched.s2.tdnsv5.com ping statistics ---  
7 packets transmitted, 7 received, 0% packet loss, time 8ms  
rtt min/avg/max/mdev = 17.636/17.716/17.951/0.144 ms
```

- 步骤3 重复执行步骤1~步骤2，验证其他VPC之间的网络互通情况。

----结束

# 14 将 VPC 对等连接组网迁移至企业路由器

## 14.1 VPC 对等连接组网迁移方案概述

### 应用场景

华为云未上线企业路由器ER之前，客户通常使用VPC对等连接连通同一个区域内的不同虚拟私有云VPC。对等连接适用于简单的组网，因为每连通两个VPC，就需要创建一个对等连接。那么对于复杂的组网，大量的对等连接将会导致组网结构非常繁复冗余，不利于网络扩容，同时增加运维成本。

而企业路由器作为一个云上高性能集中路由器，可以同时接入多个VPC，实现同区域VPC互通。企业路由器连接VPC构成中心辐射性组网，网络结构简单明了，方便扩容和运维。

如果您的组网当前使用VPC对等连接构建，并且需要连通的VPC数量较多，那么推荐您将网络迁移到企业路由器上。

#### 📖 说明

关于企业路由器更详细的介绍，请参见[企业路由器产品介绍](#)。

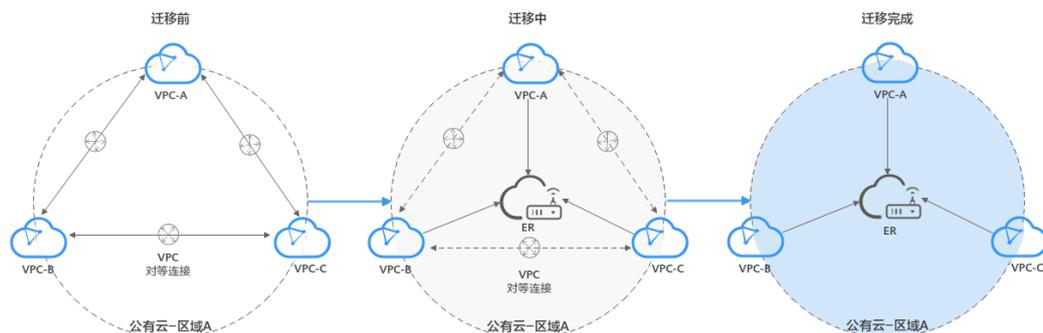
### 方案架构

VPC-A、VPC-B、VPC-C位于区域A，通过对等连接连通三个VPC的网络，为了提升网络可扩展性、降低运维成本，现在需要将这三个VPC的网络迁移至企业路由器上。

迁移共分为迁移前、迁移中、迁移完成三个阶段，迁移架构图如[图14-1](#)所示。具体说明如下：

1. 迁移前，VPC-A、VPC-B、VPC-C，通过VPC对等连接连通网络。
2. 迁移中，VPC-A、VPC-B、VPC-C将会同时接入对等连接和企业路由器中，通过大小网段确保对等连接和企业路由器的路由不冲突。
3. 迁移完成后，VPC-A、VPC-B、VPC-C可以通过企业路由器实现网络互通，此时可以删除原有VPC对等连接资源。

图 14-1 VPC 对等连接迁移架构图

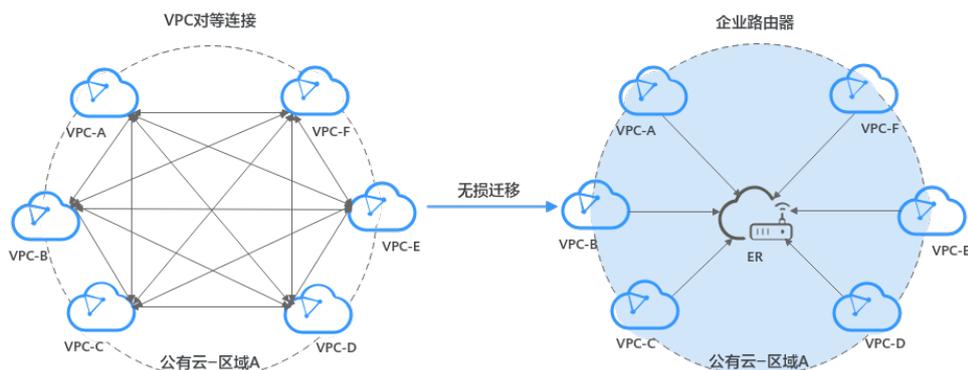


## 方案优势

简化组网结构和扩展能力，降低运维成本。

如图 14-2 所示，通过 VPC 对等连接构建的组网复杂程度高于企业路由器，当您有 6 个 VPC 的时候，您需要创建 15 个对等连接，组网结构已经非常复杂。而使用企业路由器时，只需要将 VPC 分别接入 ER 即可，网络架构简洁明了，方便运维，同时具备较高的可扩展性。

图 14-2 对等连接和企业路由器组网对比



## 约束与限制

- 如果您对等连接下的 VPC 属于不同的账号，那么迁移的时候，您可以使用[企业路由器的共享功能](#)，将不同账号下的 VPC 迁移至同一个企业路由器中构建组网。
- 由于网络组网的复杂程度不同，将 VPC 对等连接迁移至企业路由器时，可能会造成业务中断，请您[提交工单](#)联系华为云客服，评估迁移方案。  
当业务 VPC 下存在共享型弹性负载均衡、VPC 终端节点、私网 NAT 网关、分布式缓存服务、混合云 DNS 解析时，不建议直接将业务 VPC 接入 ER。

了解企业路由器的约束与限制详细信息，请参见[企业路由器约束与限制](#)。

## 14.2 VPC 对等连接组网迁移资源规划

将 VPC 对等连接迁移至企业路由器，迁移开始前，您需要规划资源和组网，本示例中为您详细介绍迁移前、迁移中以及迁移完成后的资源和组网情况。

- 网络规划说明：**规划 VPC 及其子网的网段、VPC 路由表和 ER 路由表信息。

- **源规划说明：**规划云上资源的数量、名称以及主要参数等信息，云上资源包括 VPC、ECS 以及 ER。

## 网络规划说明

迁移过程中，除了添加 ER 和 VPC 之间通信的路由，还需要添加一些迁移过程中的验证路由和临时通信路由，迁移完成可以删掉不需要的路由，VPC 对等连接迁移组网规划总体说明请参见表 14-1。

不同迁移过程中组网示意图如下所示：

- **迁移前组网示意图**
- **迁移中组网示意图**
- **迁移完成后组网示意图**

### 说明

以下路由规划详情仅为示例，供您参考，您需要根据实际业务情况规划路由。

图 14-3 迁移前组网示意图

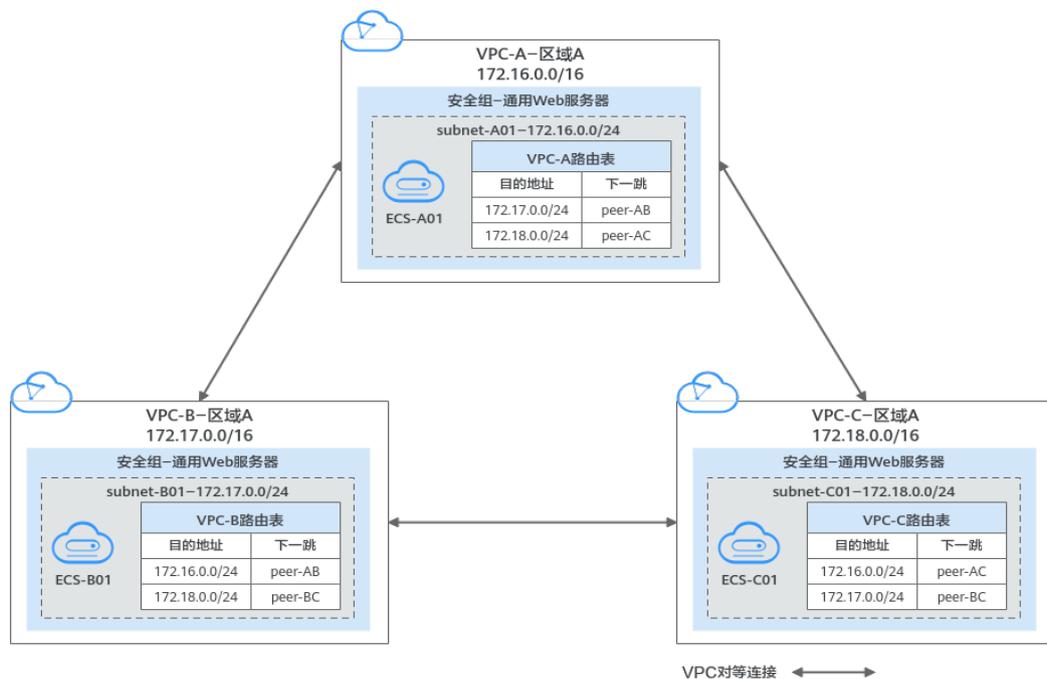


图 14-4 迁移中组网示意图

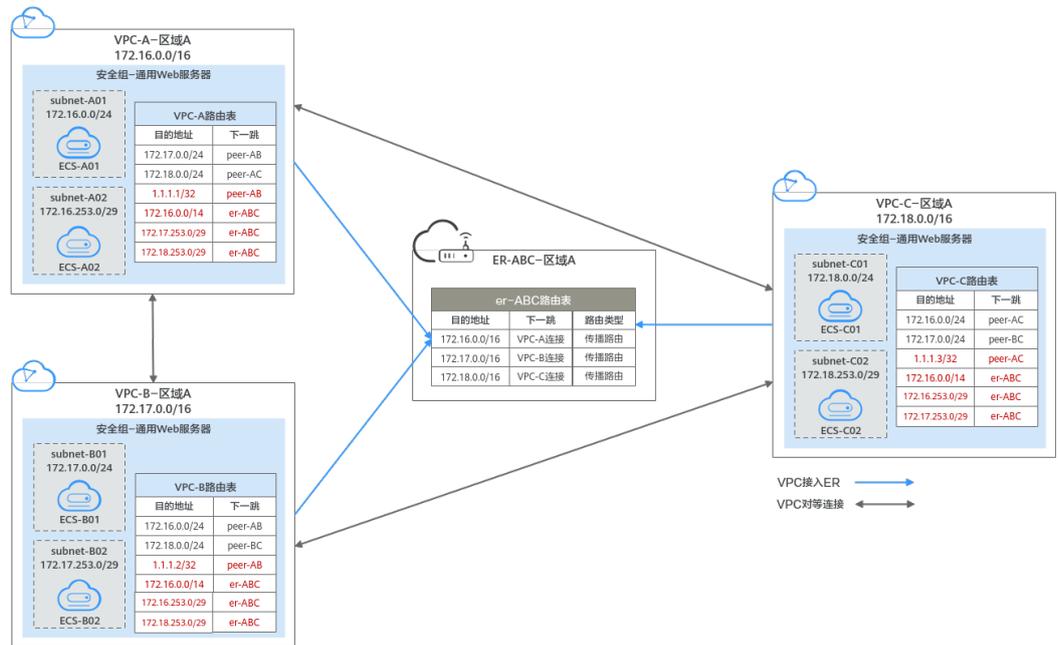


图 14-5 迁移完成后组网示意图

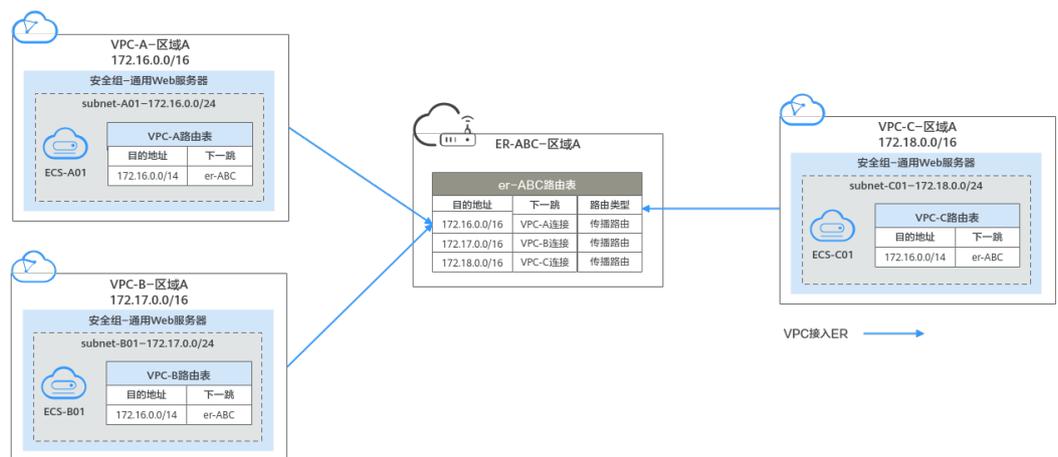


表 14-1 VPC 对等连接迁移组网规划总体说明

路由表	说明
VPC路由表	<p>VPC路由表的规划详情如表14-2所示。</p> <ol style="list-style-type: none"> <li>1. 迁移前，在VPC的路由表中，指向对等连接的路由目的地址为VPC的子网网段，未覆盖整个VPC网段，因此该对等连接不是连通整个VPC网段，而是连通VPC的子网。</li> <li>2. 迁移中，需要在VPC路由表中，添加指向VPC对等连接的临时通信路由、指向ER的大网段路由和验证路由。 <ul style="list-style-type: none"> <li>● 指向VPC对等连接的临时通信路由，确保迁移过程中，删除原有VPC对等连接路由时流量不中断。该路由的下一跳可以选择VPC关联的任意对等连接，目的地址不能被其他业务占用，可以选择不常用的任意路由地址。本示例中的地址为1.1.1.1/32、1.1.1.2/32、1.1.1.3/32。</li> <li>● 指向ER的大网段路由，用作VPC和ER的通信。该路由的目的地址即需要覆盖待迁移的所有VPC网段，又不能被其他业务占用。本示例中大网段的地址为172.16.0.0/14，覆盖172.16.0.0/16、172.17.0.0/16和172.18.0.0/16三个VPC网段。</li> <li>● 指向ER的验证路由，用于验证VPC和ER的通信。验证路由网段不能被VPC对等连接覆盖，无法通过对等连接通信，用来验证VPC和ER之间的网络通信情况。本示例中验证路由的地址为172.16.253.0/29、172.17.253.0/29、172.18.253.0/29。</li> </ul> <p><b>须知</b></p> <ul style="list-style-type: none"> <li>● 请务必添加指向VPC对等连接的临时通信路由，由于VPC对等连接功能的限制，此路由可以确保迁移过程中，删除VPC对等连接路由时流量不中断。此处流量不中断仅针对本文的方案，您的实际迁移过程中可能会中断流量，请务必联系华为云客服评估迁移方案。</li> <li>● 指向ER的大网段路由需要覆盖业务范围内的所有VPC网段，如果一个大网段路由不够，您可以根据实际情况规划多个大网段路由。</li> </ul> </li> <li>3. 迁移完成后，需要在VPC路由表中删除验证路由和临时通信路由。 <p><b>须知</b></p> <p>迁移完成后，您可以根据实际业务需要，选择继续使用大网段路由，或者添加和原有路由目的地址一致的路由后，再删除大网段路由。</p> </li> </ol>

路由表	说明
ER路由表	<p>ER路由表的规划详情如表14-3所示。</p> <p>迁移中，在ER路由表中，增加指向VPC网段的路由，用于ER和VPC的通信。</p> <p>开启ER的“默认路由表关联”和“默认路由表传播”功能，那么在ER中添加“虚拟私有云（VPC）”连接，系统会自动添加ER指向VPC的路由，无需手动添加。</p> <p><b>注意</b> 如果VPC对等连接两端的VPC网段存在重叠，则不能开启企业路由器的“默认路由表传播”功能。由于该功能是将整个VPC网段学习到ER路由表中用作目的地址，那么VPC网段重叠时，会导致ER路由表内路由冲突。此时，您需要手动在ER路由表中添加指向VPC连接的路由。</p>

表 14-2 VPC 路由表规划

VPC 名称	VPC 路由表名称	目的地址	下一跳类型	下一跳	路由类型	路由作用	存在阶段
vpc-A	rtb-vpc-A	172.17.0/24	对等连接	peer-AB	自定义	<ul style="list-style-type: none"> <li>目的地址指向 vpc-B的子网 subnet-B01</li> <li>连通子网 subnet-A01和 subnet-B01</li> </ul>	迁移前/迁移中
		172.18.0/24	对等连接	peer-AC	自定义	<ul style="list-style-type: none"> <li>目的地址指向 vpc-C的子网 subnet-C01</li> <li>连通子网 subnet-A01和 subnet-C01</li> </ul>	迁移前/迁移中
		1.1.1.1/32	对等连接	peer-AB	自定义	<ul style="list-style-type: none"> <li>目的地址指向任意未被业务占用的IP地址</li> <li>确保迁移时，VPC对等连接流量不中断</li> </ul>	迁移中
		172.16.0/14	企业路由器	er-ABC	自定义	<ul style="list-style-type: none"> <li>目的地址指向覆盖3个VPC的大网段</li> <li>连通vpc-A和 er-ABC</li> </ul>	迁移中/迁移完成

VPC 名称	VPC 路由表名称	目的地址	下一跳类型	下一跳	路由类型	路由作用	存在阶段
		172.17.253.0/29	企业路由器	er-ABC	自定义	<ul style="list-style-type: none"> <li>目的地址指向 vpc-B 的子网 subnet-B02</li> <li>连通 subnet-B02 和 er-ABC</li> </ul>	迁移中
		172.18.253.0/29	企业路由器	er-ABC	自定义	<ul style="list-style-type: none"> <li>目的地址指向 vpc-C 的子网 subnet-C02</li> <li>连通 subnet-C02 和 er-ABC</li> </ul>	迁移中
vpc-B	rtb-vpc-B	172.16.0/24	对等连接	peer-AB	自定义	<ul style="list-style-type: none"> <li>目的地址指向 vpc-A 的子网 subnet-A01</li> <li>连通子网 subnet-A01 和 subnet-B01</li> </ul>	迁移前/迁移中
		172.18.0/24	对等连接	peer-BC	自定义	<ul style="list-style-type: none"> <li>目的地址指向 vpc-C 的子网 subnet-C01</li> <li>连通子网 subnet-B01 和 subnet-C01</li> </ul>	迁移前/迁移中
		1.1.1.2/32	对等连接	peer-AB	自定义	<ul style="list-style-type: none"> <li>目的地址指向任意未被业务占用的 IP 地址</li> <li>确保迁移时，VPC 对等连接流量不中断</li> </ul>	迁移中
		172.16.0/14	企业路由器	er-ABC	自定义	<ul style="list-style-type: none"> <li>目的地址指向覆盖 3 个 VPC 的大网段</li> <li>连通 vpc-B 和 er-ABC</li> </ul>	迁移中/迁移完成
		172.16.253.0/29	企业路由器	er-ABC	自定义	<ul style="list-style-type: none"> <li>目的地址指向 vpc-A 的子网 subnet-A02</li> <li>连通 subnet-A02 和 er-ABC</li> </ul>	迁移中

VPC 名称	VPC 路由表名称	目的地址	下一跳类型	下一跳	路由类型	路由作用	存在阶段
		172.18.253.0/29	企业路由器	er-ABC	自定义	<ul style="list-style-type: none"> <li>目的地址指向 vpc-C 的子网 subnet-C02</li> <li>连通 subnet-C02 和 er-ABC</li> </ul>	迁移中
vpc-C	rtb-vpc-C	172.16.0/24	对等连接	peer-AC	自定义	<ul style="list-style-type: none"> <li>目的地址指向 vpc-A 的子网 subnet-A01</li> <li>连通子网 subnet-A01 和 subnet-C01</li> </ul>	迁移前/迁移中
		172.17.0/24	对等连接	peer-BC	自定义	<ul style="list-style-type: none"> <li>目的地址指向 vpc-B 的子网 subnet-B01</li> <li>连通子网 subnet-B01 和 subnet-C01</li> </ul>	迁移前/迁移中
		1.1.1.3/32	对等连接	peer-AC	自定义	<ul style="list-style-type: none"> <li>目的地址指向任意未被业务占用的 IP 地址</li> <li>确保迁移时，VPC 对等连接流量不中断</li> </ul>	迁移中
		172.16.0/14	企业路由器	er-ABC	自定义	<ul style="list-style-type: none"> <li>目的地址指向覆盖 3 个 VPC 的大网段</li> <li>连通 vpc-C 和 er-ABC</li> </ul>	迁移中/迁移完成
		172.16.253.0/29	企业路由器	er-ABC	自定义	<ul style="list-style-type: none"> <li>目的地址指向 vpc-A 的子网 subnet-A02</li> <li>连通 subnet-A02 和 er-ABC</li> </ul>	迁移中
		172.17.253.0/29	企业路由器	er-ABC	自定义	<ul style="list-style-type: none"> <li>目的地址指向 vpc-B 的子网 subnet-B02</li> <li>连通 subnet-B02 和 er-ABC</li> </ul>	迁移中

表 14-3 ER 路由表规划

ER名称	ER路由表名称	目的地址	下一跳	连接资源	路由类型	路由作用	存在阶段
er-ABC	default RouteTable	172.16.0.0/16	er-attach-A	vpc-A	传播路由	<ul style="list-style-type: none"> <li>目的地址指向vpc-A</li> <li>连通vpc-A和er-ABC</li> </ul>	迁移中/迁移完成
		172.17.0.0/16	er-attach-B	vpc-B	传播路由	<ul style="list-style-type: none"> <li>目的地址指向vpc-B</li> <li>连通vpc-B和er-ABC</li> </ul>	迁移中/迁移完成
		172.18.0.0/16	er-attach-C	vpc-C	传播路由	<ul style="list-style-type: none"> <li>目的地址指向vpc-C</li> <li>连通vpc-C和er-ABC</li> </ul>	迁移中/迁移完成

## 源规划说明

迁移过程中，除了创建企业路由器，还需要创建一些迁移所需要的临时资源，迁移完成可以释放资源，VPC对等连接迁移资源规划总体说明请参见表14-4。

### 说明

以下资源规划详情仅为示例，供您参考，您需要根据实际业务情况规划资源。

表 14-4 VPC 对等连接迁移资源规划总体说明

资源	说明
虚拟私有云 VPC	<p>VPC的资源规划详情如表14-5所示。</p> <ul style="list-style-type: none"> <li>迁移前，原有3个VPC，每个VPC各有一个子网，关联至VPC默认路由表。</li> <li>迁移中，在原有VPC下，各新增一个迁移验证子网，该子网网络不能被业务占用。迁移验证子网无法通过对等连接通信，用来验证VPC和ER之间的网络通信情况。</li> <li>迁移完成后，删除迁移验证子网，释放资源。</li> </ul>
VPC对等连接	<p>VPC对等连接的资源规划详情如表14-6所示。</p> <p>迁移完成后，删除VPC对等连接，释放资源。</p>

资源	说明
弹性云服务器 ECS	<p>ECS的资源规划详情如表14-7所示。</p> <ul style="list-style-type: none"> <li>迁移前，原有3个云服务器，运行实际业务。</li> <li>迁移中，在VPC迁移验证子网内，各创建一个云服务器，因此用来验证VPC和ER之间的网络通信情况。</li> <li>迁移完成后，删除迁移验证子网内的ECS，释放资源。</li> </ul>
企业路由器ER	<p>ER和待迁移的VPC对等连接位于同一个区域，资源规划详情如表14-8所示。</p> <p>迁移中，创建ER，并添加3个“虚拟私有云（VPC）”连接，连接的资源规划详情如表14-9所示。</p> <ul style="list-style-type: none"> <li>创建ER时，开启“默认路由表关联”和“默认路由表传播”功能，可以免去手动添加路由。</li> </ul> <p><b>注意</b> 如果VPC对等连接两端的VPC网段存在重叠，则不能开启企业路由器的“默认路由表传播”功能。由于该功能是将整个VPC网段学习到ER路由表中用作目的地址，那么VPC网段重叠时，会导致ER路由表中路由冲突。此时，您需要手动在ER路由表中添加指向VPC连接的路由。</p> <ul style="list-style-type: none"> <li>在ER中添加3个“虚拟私有云（VPC）”连接，不开启“配置连接侧路由”功能。 开启该功能后，会在VPC路由表中自动添加指向ER的路由，目的地址固定为10.0.0.0/8，172.16.0.0/12，192.168.0.0/16。迁移时，需要手动在VPC路由表中添加规划的大网段路由，不能使用自动添加的路由。</li> </ul>

表 14-5 VPC 资源规划详情

VPC名称	VPC网段	子网名称	子网网段	关联路由表	子网作用	存在阶段
vpc-A	172.16.0.0/16	subnet-A01	172.16.0.0/24	默认路由表	业务子网	迁移前/迁移完成
		subnet-A02	172.16.253.0/29	默认路由表	迁移验证子网，验证VPC和ER之间的网络通信	迁移中
vpc-B	172.17.0.0/16	subnet-B01	172.17.0.0/24	默认路由表	业务子网	迁移前/迁移完成
		subnet-B02	172.17.253.0/29	默认路由表	迁移验证子网，验证VPC和ER之间的网络通信	迁移中
vpc-C	172.18.0.0/16	subnet-C01	172.18.0.0/24	默认路由表	业务子网	迁移前/迁移完成

VPC名称	VPC网段	子网名称	子网网段	关联路由表	子网作用	存在阶段
		subnet-C02	172.18.253.0/29	默认路由表	迁移验证子网，验证VPC和ER之间的网络通信	迁移中

表 14-6 VPC 对等连接资源规划详情

VPC对等连接名称	本端VPC	对端VPC	对等连接作用	存在阶段
peer-AB	vpc-A	vpc-B	连通vpc-A的子网subnet-A01和vpc-B的子网subnet-B01网络	迁移前/迁移中
peer-AC	vpc-A	vpc-C	连通vpc-A的子网subnet-A01和vpc-C的子网subnet-C01网络	迁移前/迁移中
peer-BC	vpc-B	vpc-C	连通vpc-B的子网subnet-B01和vpc-C的子网subnet-C01网络	迁移前/迁移中

表 14-7 ECS 资源规划详情

ECS名称	VPC名称	子网名称	私有IP地址	镜像	安全组	ECS作用	存在阶段
ecs-A01	vpc-A	subnet-A01	172.16.0.139	公共镜像： Cent OS 8.2 64bit	sg-demo： 通用Web服务器	运行业务的云服务器	迁移前/迁移中/迁移完成
ecs-A02	vpc-A	subnet-A02	172.16.253.3			迁移验证子网内的ECS，验证VPC和ER之间网络通信	迁移中
ecs-B01	vpc-B	subnet-B01	172.17.0.93			运行业务的云服务器	迁移前/迁移中/迁移完成
ecs-B02	vpc-B	subnet-B02	172.17.253.4			迁移验证子网内的ECS，验证VPC和ER之间网络通信	迁移中
ecs-C01	vpc-C	subnet-C01	172.18.0.220			运行业务的云服务器	迁移前/迁移中/迁移完成

ECS 名称	VPC 名称	子网名称	私有 IP 地址	镜像	安全组	ECS 作用	存在阶段
ecs-C02	vpc-C	subnet-C02	172.18.253.5			迁移验证子网内的 ECS，验证 VPC 和 ER 之间网络通信	迁移中

表 14-8 ER 资源规划详情

ER 名称	AS 号	默认路由表关联	默认路由表传播	自动接受共享连接	关联/传播路由表	连接	存在阶段
er-AB C	64512	开启	本示例选择“开启”。如果您的 VPC 网段存在重叠，则不能开启。	本示例不“开启”。如果您要将不同账号下的 VPC 接入 ER 构建组网，则可以开启该功能，具体请参见 <a href="#">企业路由器的共享功能</a> 。	默认路由表	er-attach-A	迁移中/迁移完成
						er-attach-B	
						er-attach-C	

表 14-9 “虚拟私有云（VPC）”连接资源规划详情

连接名称	连接类型	虚拟私有云	子网	配置连接侧路由	存在阶段
er-attach-A	虚拟私有云（VPC）	vpc-A	subnet-A01	不开启	迁移中/迁移完成
er-attach-B		vpc-B	subnet-B01		
er-attach-C		vpc-C	subnet-C01		

## 14.3 VPC 对等连接组网迁移流程

本章节介绍 VPC 对等连接迁移至企业路由器 ER 的总体流程，流程说明如[表 14-10](#)所示。

表 14-10 迁移 VPC 对等连接至 ER 流程说明

步骤	说明
<b>步骤一：创建云服务资源</b>	<ol style="list-style-type: none"><li>1. 创建1个企业路由器，构建一个同区域组网只需要1个企业路由器。</li><li>2. 在每个VPC内，各创建1个迁移验证子网，该子网无法通过VPC对等连接互通，但是可以通过ER互通，用来验证迁移过程中VPC和ER之间的网络通信情况。</li><li>3. 在每个迁移验证子网内，各创建一个ECS，登录ECS执行ping命令验证VPC和ER之间的网络通信情况。</li></ol>
<b>步骤二：在企业路由器中添加VPC连接及路由</b>	<ol style="list-style-type: none"><li>1. 在企业路由器中添加“虚拟私有云（VPC）”连接，即将3个VPC分别接入企业路由器中。 迁移时，需要手动在VPC路由表中添加规划的大网段路由，不开启“配置连接侧路由”功能。</li><li>2. 检查ER路由表中的路由。 本示例中，ER开启了“默认路由表关联”和“默认路由表传播”功能，那么在ER中添加“虚拟私有云（VPC）”连接时，系统会自动添加ER指向VPC的路由，无需手动添加，只需要检查即可。</li></ol>
<b>步骤三：验证VPC和ER之间的网络通信情况</b>	<ol style="list-style-type: none"><li>1. 在VPC路由表中，添加指向ER的迁移验证路由，用于验证VPC和ER的通信情况。</li><li>2. 登录迁移验证ECS，执行ping命令，验证VPC和ER之间的网络通信情况。</li><li>3. 验证完成后，删除迁移验证相关的路由、ECS和子网。</li></ol>
<b>步骤四：在VPC路由表中添加路由</b>	<ol style="list-style-type: none"><li>1. 在VPC路由表中，添加指向VPC对等连接的临时通信路由，确保迁移过程中，删除原有VPC对等连接路由时流量不中断。</li><li>2. 在VPC路由表中，添加指向ER的大网段路由，用作VPC和ER的通信。</li></ol>
<b>步骤五：执行迁移操作</b>	在VPC路由表中，删除原有指向VPC对等连接的路由。 迁移过程中需要实时关注业务流量，如果出现流量中断，请立即添加回已删除的路由。
<b>步骤六：删除原有VPC对等连接</b>	对等连接路由删除完成，且业务正常时，建议您再观察一段时间，确保没有问题后，再删除VPC对等连接，本操作会同步删除VPC路由表中关联的临时通信路由。

## 14.4 VPC 对等连接组网迁移实施步骤

### 步骤一：创建云服务资源

本示例中，云服务资源的总体规划说明，请参见表14-4。

**步骤1** 创建迁移过程中验证ER和VPC通信情况的子网。

在每个待迁移的VPC内，各创建一个新的子网。本示例中需要创建3个验证子网，更多资源详情请参见[表14-5](#)。

创建VPC及子网，具体方法请参见[创建虚拟私有云和子网](#)。

**步骤2** 在迁移验证子网内，创建ECS。

在每个待迁移的子网内，各创建一个ECS。本示例中需要创建3个ECS，更多资源详情请参见[表14-7](#)。

创建ECS，具体方法请参见[自定义购买ECS](#)。

**步骤3** 创建1个企业路由器。

本示例中，对等连接两端的VPC网段不重叠，因此创建企业路由器时，同时开启“默认路由表关联”和“默认路由表传播”，更多资源详情请参见[表14-3](#)。

---

#### 注意

如果VPC对等连接两端的VPC网段存在重叠，则不能开启企业路由器的“默认路由表传播”功能。由于该功能是将整个VPC网段学习到ER路由表中用作目的地址，那么VPC网段重叠时，会导致ER路由表内路由冲突。此时，您需要手动在ER路由表中添加指向VPC连接的路由。

---

创建企业路由器，具体方法请参见[创建企业路由器](#)。

----结束

## 步骤二：在企业路由器中添加 VPC 连接及路由

**步骤1** 将3个待迁移的VPC分别接入企业路由器中。

添加连接时，不开启“配置连接侧路由”功能，更多资源详情请参见[表14-3](#)。

---

#### 须知

开启该功能后，会在VPC路由表中自动添加指向ER的路由，目的地址固定为10.0.0.0/8，172.16.0.0/12，192.168.0.0/16。迁移时，需要手动在VPC路由表中添加规划的大网段路由，不能使用自动添加的路由。

---

添加“虚拟私有云（VPC）”连接，具体方法请参见[在企业路由器中添加VPC连接](#)。

**步骤2** 检查ER路由表中指向VPC的路由。

本示例中，ER开启了“默认路由表关联”和“默认路由表传播”功能，那么在ER中添加“虚拟私有云（VPC）”连接时，系统会自动添加ER指向VPC的路由，无需手动添加，只需要检查即可。

---

#### 须知

如果您未开启“默认路由表传播”功能，则需要手动在ER路由表中添加指向VPC的路由，具体方法请参见[创建静态路由](#)。

---

ER路由规划详情，请参见[表14-1](#)和[表14-3](#)。

查看ER路由，具体方法请参见[查看路由](#)。

---结束

### 步骤三：验证 VPC 和 ER 之间的网络通信情况

**步骤1** 在接入ER的VPC的路由表中，添加指向ER的迁移验证路由。

VPC路由规划详情，请参见[表14-1](#)。

配置路由信息，具体方法请参见[在VPC路由表中配置路由](#)。

本示例中添加[表14-2](#)中位于“迁移中”阶段，下一跳为企业路由器的路由。

- 在vpc-A的路由表中，添加172.17.253.0/29和172.18.253.0/29两条路由。
- 在vpc-B的路由表中，添加172.16.253.0/29和172.18.253.0/29两条路由。
- 在vpc-C的路由表中，添加172.16.253.0/29和172.17.253.0/29两条路由。

**步骤2** 在弹性云服务器的远程登录窗口，执行以下步骤，验证VPC和ER的网络通信情况。

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）。

1. 登录ecs-A02，验证vpc-A与vpc-B是否可以通过ER通信。

**ping ecs-B02的私有IP地址**

命令示例：

**ping 172.17.253.4**

回显类似如下信息，表示vpc-A与vpc-B可以通过ER通信。

```
[root@ecs-A02 ~]# ping 172.17.253.4
PING 172.17.253.4 (172.17.253.4) 56(84) bytes of data.
64 bytes from 172.17.253.4: icmp_seq=1 ttl=64 time=0.849 ms
64 bytes from 172.17.253.4: icmp_seq=2 ttl=64 time=0.455 ms
64 bytes from 172.17.253.4: icmp_seq=3 ttl=64 time=0.385 ms
64 bytes from 172.17.253.4: icmp_seq=4 ttl=64 time=0.372 ms
...
--- 172.17.253.4 ping statistics ---
```

2. 登录ecs-A02，验证vpc-A与vpc-C是否可以通过ER通信。

**ping ecs-C02的私有IP地址**

命令示例：

**ping 172.18.253.5**

回显类似如下信息，表示vpc-A与vpc-C可以通过ER通信。

```
[root@ecs-A02 ~]# ping 172.18.253.5
PING 172.18.253.5 (172.18.253.5) 56(84) bytes of data.
64 bytes from 172.18.253.5: icmp_seq=1 ttl=64 time=0.849 ms
64 bytes from 172.18.253.5: icmp_seq=2 ttl=64 time=0.455 ms
64 bytes from 172.18.253.5: icmp_seq=3 ttl=64 time=0.385 ms
64 bytes from 172.18.253.5: icmp_seq=4 ttl=64 time=0.372 ms
...
--- 172.18.253.5 ping statistics ---
```

3. 登录ecs-B02，验证vpc-B与vpc-C是否可以通过ER通信。

**ping ecs-C02的私有IP地址**

命令示例：

**ping 172.18.253.5**

### 步骤3 验证完成后，删除迁移验证相关的路由、ECS和子网。

1. 分别在3个VPC路由表中，删除指向ER的迁移验证路由。  
本示例中删除表14-2中位于“迁移中”阶段，下一跳为企业路由器的路由。
  - 在vpc-A的路由表中，删除172.17.253.0/29和172.18.253.0/29两条路由。
  - 在vpc-B的路由表中，删除172.16.253.0/29和172.18.253.0/29两条路由。
  - 在vpc-C的路由表中，删除172.16.253.0/29和172.17.253.0/29两条路由。删除VPC路由，具体方法请参见[删除路由](#)。
2. 分别删除3个迁移验证子网内的ECS。  
本示例中删除表14-7中位于“迁移中”阶段的ECS，分别为ecs-A02、ecs-B02、ecs-C02。  
删除ECS，具体方法请参见[如何删除、重启弹性云服务器?](#)。
3. 分别删除3个迁移验证子网。  
本示例中删除表14-5中位于“迁移中”阶段的子网，分别为subnet-A02、subnet-B02、subnet-C02。  
删除子网，具体方法请参见[删除子网](#)。

---

#### 须知

删除子网前，请先删除子网内的ECS，否则无法删除子网。

---

----结束

## 步骤四：在 VPC 路由表中添加路由

VPC路由规划详情，请参见表14-1。

### 步骤1 在VPC-A、VPC-B和VPC-C的路由表中，依次添加路由。

配置路由信息，具体方法请参见[在VPC路由表中配置路由](#)。

1. 添加指向任意VPC对等连接的临时通信路由。  
此路由确保迁移过程中，删除原有VPC对等连接路由时流量不中断。  
本示例中添加表14-2中位于“迁移中”阶段，下一跳为对等连接的路由。
  - 在vpc-A的路由表中，添加1.1.1.1/32路由。
  - 在vpc-B的路由表中，添加1.1.1.2/32路由。
  - 在vpc-C的路由表中，添加1.1.1.3/32路由。
2. 添加指向ER的大网段路由。  
该路由的目的地址即需要覆盖待迁移的所有VPC网段，又不能有其他业务占用。  
本示例中添加表14-2中位于“迁移中/迁移完成”阶段，下一跳为企业路由器的路由。
  - 在vpc-A的路由表中，添加172.16.0.0/14路由。
  - 在vpc-B的路由表中，添加172.16.0.0/14路由。
  - 在vpc-C的路由表中，添加172.16.0.0/14路由。

----结束

## 步骤五：执行迁移操作

**步骤1** 分别在3个VPC路由表中，删除原有指向VPC对等连接的路由。

本示例中删除[表14-2](#)中位于“迁移前/迁移中”阶段，下一跳为对等连接的路由。

- 在vpc-A的路由表中，删除172.17.0.0/24和172.18.0.0/24两条路由。
- 在vpc-B的路由表中，删除172.16.0.0/24和172.18.0.0/24两条路由。
- 在vpc-C的路由表中，删除172.16.0.0/24和172.17.0.0/24两条路由。

删除VPC路由，具体方法请参见[删除路由](#)。

---

### 注意

删除原有指向VPC对等连接的路由时，在整个删除过程中，需要登录运行业务的ECS，执行ping命令，观察流量是否中断，如果出现流量中断，请立即添加回已删除的路由。

----结束

## 步骤六：删除原有 VPC 对等连接

---

### 须知

迁移操作执行完成后，建议您再观察一段时间，确保迁移对业务没有影响后，再删除VPC对等连接。

**步骤1** 分别删除3个VPC对等连接。

删除VPC对等连接时，会同步删除VPC路由表中临时通信路由。

- 本示例中待删除的VPC对等连接详情，请参见[表14-6](#)。
- 本示例中删除对等连接时，会自动删除[表14-2](#)中位于“迁移中”阶段，下一跳为对等连接的路由。
  - 在vpc-A的路由表中，删除1.1.1.1/32路由。
  - 在vpc-B的路由表中，删除1.1.1.2/32路由。
  - 在vpc-C的路由表中，删除1.1.1.3/32路由。

删除VPC对等连接，具体方法请参见[删除对等连接](#)。

----结束

# 15 将 DC 直连 VPC 组网迁移至企业路由器 （全域接入网关 DGW）

## 15.1 DC 直连 VPC 组网迁移方案概述

### 应用场景

华为云未上线企业路由器ER之前，客户使用云专线DC构建混合云组网时，需要将DC直接接入虚拟私有云VPC中，连通云上VPC和线下IDC网络。如果客户有多个VPC需要和线下IDC互通，为了提升网络可靠性，同时部署多条专线，则可能存在以下问题：

- 同时部署多条专线链路，导致组网配置复杂，并且使用和维护成本较高。
- 多条专线链路之间相互独立，无法联动形成负载或者主备。

如果您希望提升混合云组网的的可靠性，同时降低使用和维护成本，那么推荐您将网络迁移到企业路由器上。

接下来，将主要为您介绍如何将DC直连VPC组网，迁移到通过企业路由器和全域接入网关构建的混合云组网。

#### 📖 说明

关于企业路由器更详细的介绍，请参见[企业路由器产品介绍](#)。

### 方案架构

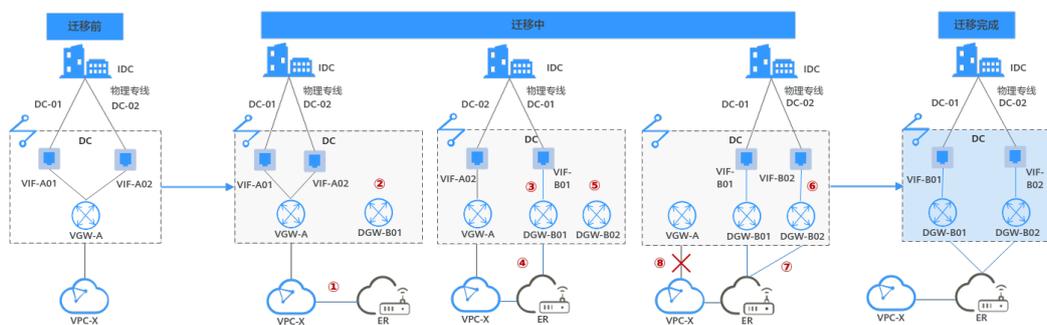
VPC-X和云专线DC的虚拟网关VGW-A、虚拟接口VIF-A01、虚拟接口VIF-A02位于区域A，通过DC连通VPC-X和线下IDC之间的网络，为了提升混合云组网可靠性并降低维护成本，现在需要将VPC-X和云专线网络迁移至企业路由器上，通过全域接入网关连通线下IDC网络。

迁移共分为迁移前、迁移中、迁移完成三个阶段，迁移架构图如[图15-1](#)所示。具体说明如下：

1. 迁移前，VPC-X直接接入DC的虚拟网关VGW-A，通过虚拟接口VIF-A01和VIF-A02连通线下IDC网络。
2. 迁移中：

- a. 将VPC-X同时接入虚拟网关VGW-A和企业路由器中，通过大小网段确保VPC-X的路由表中，虚拟网关和企业路由器的路由不冲突。
  - b. 创建全域接入网关DGW-B01。  
此处DGW-B01将会用作虚拟网关VGW-A迁移后的资源。
  - c. 删除虚拟网关VGW-A上的虚拟接口VIF-A01，在全域接入网关DGW-B01上创建虚拟接口VIF-B01，并将DGW-B01接入到企业路由器中。  
此处虚拟接口VIF-B01是虚拟接口VIF-A01迁移后的资源，当前VPC-X可以通过企业路由器访问线下IDC。
  - d. 创建全域接入网关DGW-B02。  
此处DGW-B02将会用作虚拟网关VGW-A迁移后的资源。
  - e. 删除虚拟网关VGW-A上的虚拟接口VIF-A02，在全域接入网关DGW-B02上创建虚拟接口VIF-B02，并将DGW-B02接入到企业路由器中。  
此处虚拟接口VIF-B02是虚拟接口VIF-A02迁移后的资源。
3. 迁移完成后，VPC-X、全域接入网关DGW-B01和DGW-B02接入企业路由器中并正常通信，此时可以删除虚拟网关VGW-A。

图 15-1 将 DC 直连 VPC 组网迁移至企业路由器



## 方案优势

企业路由器作为一个云上高性能集中路由器，可以连通多种不同网络服务。比如在企业路由器中接入多个VPC以及DC，此时多个VPC可以共享专线。

- 企业路由器支持路由学习，免去繁复配置，降低维护难度。
- 通过用企业路由器实现多条链路之间联动，实现负载分担或互为主备。

## 约束与限制

由于网络组网的复杂程度不同，将DC直连VPC组网迁移至企业路由器时，可能会造成业务中断，请您[提交工单](#)联系华为云客服，评估迁移方案。

当业务VPC下存在共享型弹性负载均衡、VPC终端节点、私网NAT网关、分布式缓存服务、混合云DNS解析时，不建议直接将业务VPC接入ER。

了解企业路由器的约束与限制详细信息，请参见[企业路由器约束与限制](#)。

## 15.2 DC 直连 VPC 组网迁移资源规划

将DC直连VPC组网迁移至企业路由器，迁移开始前，您需要规划资源和组网，本示例中为您详细介绍迁移前、迁移中以及迁移完成后的资源和组网情况。

- **网络规划说明**：规划VPC路由表和ER路由表信息。
- **资源规划说明**：规划云上资源的数量、名称以及主要参数等信息，云上资源包括DC的全域接入网关和虚拟接口、VPC、ECS、ER等。

## 网络规划说明

迁移过程中，您需要在VPC和ER路由表中添加通信所需的路由，迁移组网规划总体说明请参见表15-1。

不同迁移过程中组网示意图如下所示：

- **迁移前组网示意图**
- **迁移中组网示意图**
- **迁移完成后组网示意图**

### 说明

以下路由规划详情仅为示例，供您参考，您需要根据实际业务情况规划路由。

图 15-2 迁移前组网示意图

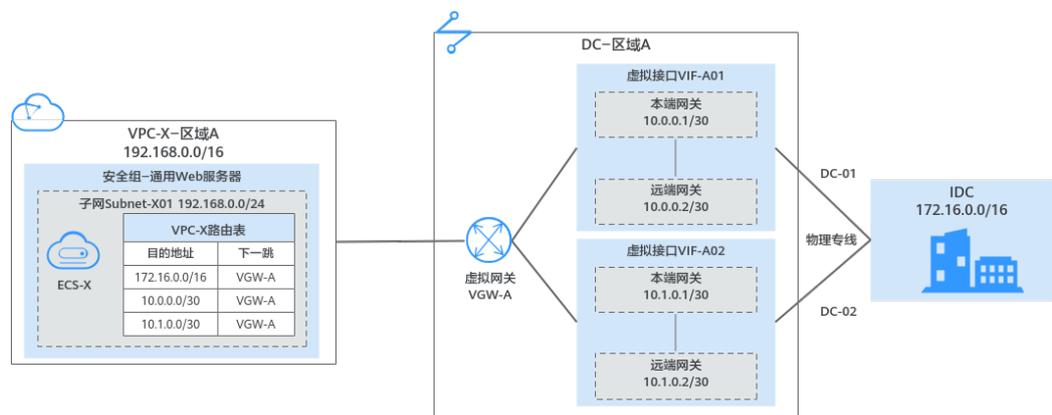


图 15-3 迁移中组网示意图

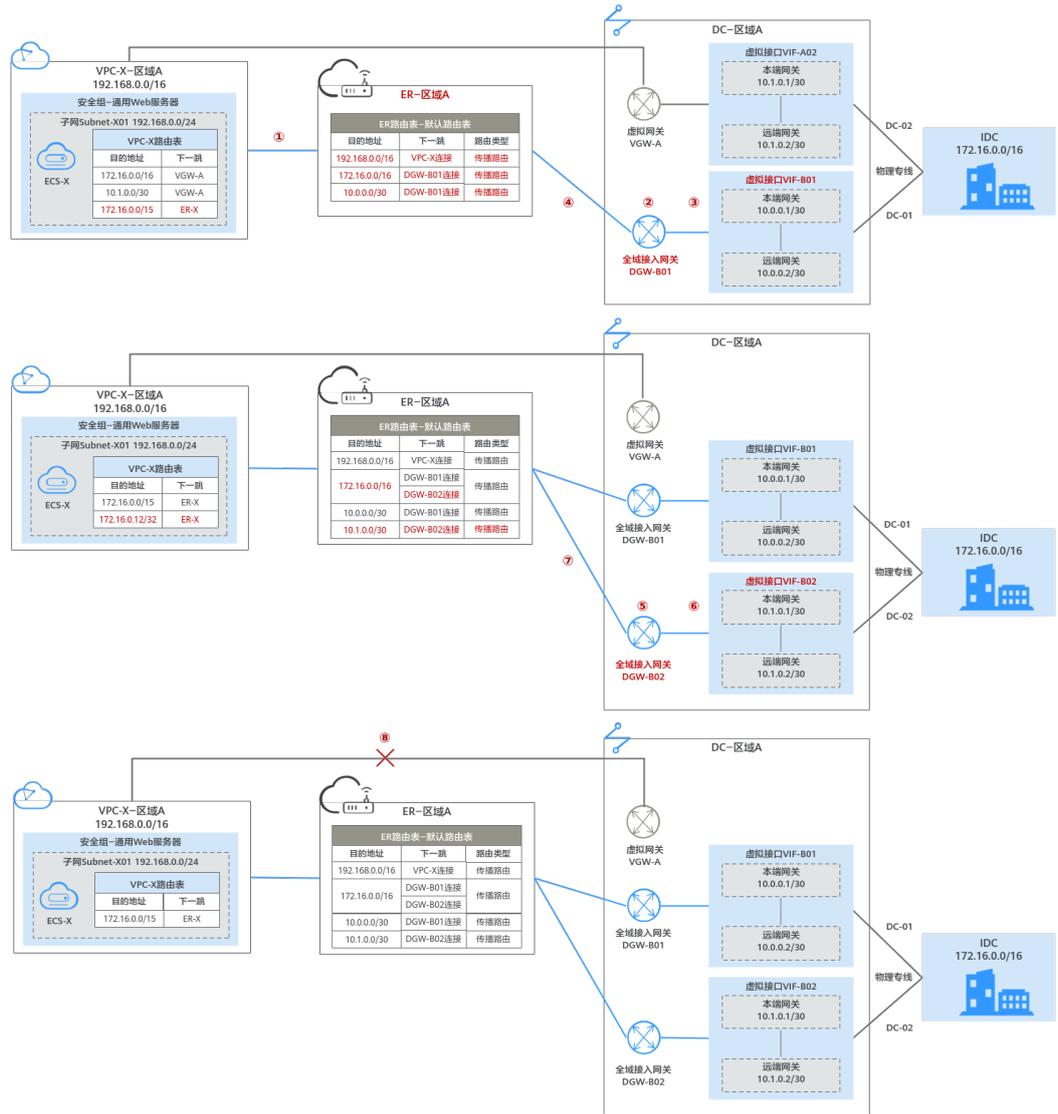


图 15-4 迁移完成后组网示意图

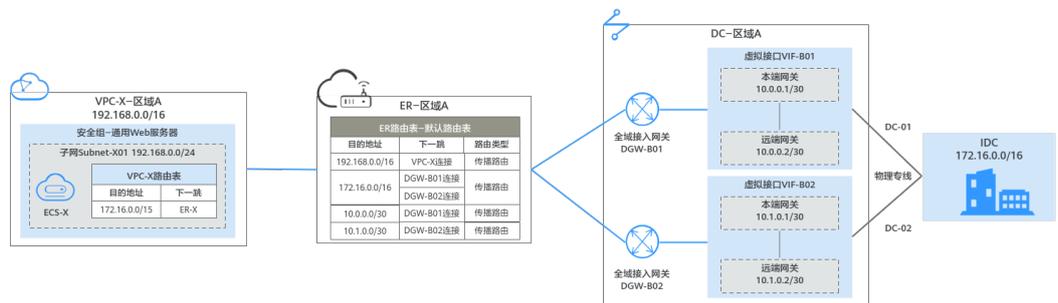


表 15-1 DC 直连 VPC 组网迁移规划总体说明

路由表	说明
VPC路由表	<p>VPC路由表的规划详情如表15-2所示。</p> <ol style="list-style-type: none"><li>迁移前，在VPC的路由表中，存在指向线下IDC侧子网网段以及虚拟接口网关的路由，用作VPC和线下IDC通信。 本示例为172.16.0.0/16、10.0.0.0/30、10.1.0.0/30。</li><li>迁移中，为了避免路由冲突无法添加，需要在VPC路由表中，添加指向ER的大网段的路由以及验证路由<ol style="list-style-type: none"><li>指向ER的大网段路由，用作VPC和ER的通信。 该路由的目的地址即需要覆盖线下IDC侧网段，又不能被其他业务占用。本示例中大网段的地址为172.16.0.0/15，覆盖172.16.0.0/16网段。 <b>须知</b> 指向ER的大网段路由需要覆盖业务范围内的所有IDC侧子网网段，如果一个网段路由不够，您可以根据实际情况规划多个大网段路由。</li><li>指向ER的验证路由，用于验证VPC是否可以通过ER和线下IDC通信，验证完成后即可删除。 该路由的目的地址使用线下任意一台服务器的地址，本示例为172.16.0.12/32。</li></ol></li><li>迁移中及迁移完成后，删除原有虚拟接口和虚拟网关资源时，会同步删除云专线网关相关的路由。 本示例将会删除172.16.0.0/16、10.0.0.0/30、10.1.0.0/30三条路由。 <b>须知</b> 迁移完成后，您可以根据实际业务需要，选择继续使用大网段路由，或者添加和原有路由目的地址一致的路由后，再删除大网段路由。</li></ol>
ER路由表	<p>ER路由表的规划详情如表15-3所示。</p> <p>迁移中，在ER路由表中，添加指向VPC网段和全域接入网关的路由，通过ER转发VPC和云专线之间的流量。</p> <p>开启ER的“默认路由表关联”和“默认路由表传播”功能，那么在ER中添加连接时，系统会自动添加ER指向连接的路由，无需手动添加。</p> <ul style="list-style-type: none"><li>本示例中添加“虚拟私有云（VPC）”连接时，传播路由为192.168.0.0/16。</li><li>本示例中创建虚拟接口，并添加“全域接入网关（DGW）”连接时，传播路由为172.16.0.0/16、10.0.0.0/30、10.1.0.0/30。</li></ul>

表 15-2 VPC 路由表规划

VPC 名称	VPC 路由表名称	目的地址	下一跳类型	下一跳	路由类型	路由说明	存在阶段
vpc-X	rtb-vpc-X	172.16.0.0/16	云专线网关	VGW-A	系统	目的地址指向远端子网，即线下 IDC 侧子网网段	<ul style="list-style-type: none"> <li>迁移前</li> <li>迁移中</li> </ul>
		10.0.0.0/30	云专线网关	VGW-A	系统	目的地址指向 VIF-A01 的本端网关和远端网关	<ul style="list-style-type: none"> <li>迁移前</li> <li>迁移中</li> </ul>
		10.1.0.0/30	云专线网关	VGW-A	系统	目的地址指向 VIF-A02 的本端网关和远端网关	<ul style="list-style-type: none"> <li>迁移前</li> <li>迁移中</li> </ul>
		172.16.0.0/15	企业路由器	ER-X	自定义	目的地址指向线下 IDC 侧子网网段，此处采用大网段	<ul style="list-style-type: none"> <li>迁移中</li> <li>迁移完成</li> </ul>
		172.16.0.12/32	企业路由器	ER-X	自定义	目的地址指向线下 IDC 侧任意一台服务器，用来验证通信	迁移中

表 15-3 ER 路由表规划

ER 名称	ER 路由表名称	目的地址	下一跳	连接资源	路由类型	路由说明	存在阶段
er-X	default RouteTable	192.168.0.0/16	er-attach-VPC-X	VPC-X	传播路由	目的地址指向 VPC-X	<ul style="list-style-type: none"> <li>迁移中</li> <li>迁移完成</li> </ul>

ER名称	ER路由表名称	目的地址	下一跳	连接资源	路由类型	路由说明	存在阶段
		172.16.0.0/16	er-attach-DGW-B01 er-attach-DGW-B02	DGW-B01 DGW-B02	传播路由	目的地址指向远端子网，即线下IDC侧子网网段。当下一跳同时展示两个DGW连接时，表示两个DGW连接为负载均衡模式，同时处于工作状态。如果您不需要负载均衡模式，您可以通过修改路由策略，将两个DCW连接改为主备模式。	<ul style="list-style-type: none"><li>• 迁移中</li><li>• 迁移完成</li></ul>
		10.0.0.0/30	er-attach-DGW-B01	DGW-B01	传播路由	目的地址指向VIF-B01的本端网关和远端网关	<ul style="list-style-type: none"><li>• 迁移中</li><li>• 迁移完成</li></ul>
		10.1.0.0/30	er-attach-DGW-B02	DGW-B02	传播路由	目的地址指向VIF-B02的本端网关和远端网关	<ul style="list-style-type: none"><li>• 迁移中</li><li>• 迁移完成</li></ul>

## 资源规划说明

迁移过程中，您需要创建企业路由器，全域接入网关以及虚拟接口，迁移完成后可以释放原有的资源，DC直连VPC组网迁移资源规划总体说明请参见[表15-4](#)。

### 说明

以下资源规划详情仅为示例，供您参考，您需要根据实际业务情况规划资源。

表 15-4 DC 直连 VPC 组网迁移资源规划总体说明

资源类型	资源数量	说明	存在阶段
虚拟私有云VPC	1	<p>业务VPC，实际运行客户业务的VPC，以实际情况为准。</p> <ul style="list-style-type: none"> <li>• VPC名称：本示例为VPC-X。</li> <li>• IPv4网段：VPC网段与客户IDC侧网段不能重复，本示例为192.168.0.0/16。</li> <li>• 子网名称：本示例为Subnet-X01。</li> <li>• 子网IPv4网段：VPC子网网段与客户IDC侧子网网段不能重复，本示例为192.168.0.0/24。</li> </ul>	<ul style="list-style-type: none"> <li>• 迁移前</li> <li>• 迁移中</li> <li>• 迁移完成</li> </ul>
云专线DC（物理连接）	2	<p>物理连接：本示例中，迁移前客户原有2个物理连接，分别为DC-01和DC-02。</p> <p>本次迁移不重新创建物理连接，该资源仍然继续使用。</p>	<ul style="list-style-type: none"> <li>• 迁移前</li> <li>• 迁移中</li> <li>• 迁移完成</li> </ul>
云专线DC（虚拟网关VGW）	1	<p>以下是迁移前的虚拟网关示例，实际请以客户的资源为准。</p> <ul style="list-style-type: none"> <li>• 名称：本示例为VGW-A。</li> <li>• 关联模式：原虚拟网关直接连接虚拟私有云，此处是“虚拟私有云”。</li> <li>• 虚拟私有云：选择您的业务VPC，本示例为VPC-X。</li> <li>• BGP ASN：本示例AS号为64512。</li> </ul>	<ul style="list-style-type: none"> <li>• 迁移前</li> <li>• 迁移中</li> </ul>
云专线（虚拟网关VGW关联的虚拟接口）	2	<p>以下是迁移前的虚拟接口，关联虚拟网关，共2个，实际请以客户的资源为准，本示例如下：</p> <ul style="list-style-type: none"> <li>• 名称：本示例两个虚拟接口分别为VIF-A01和VIF-A02。</li> <li>• 虚拟网关：本示例两个虚拟接口关联的虚拟网关为VGW-A。</li> <li>• 本端网关：本示例VIF-A01为10.0.0.1/30，VIF-A02为10.1.0.1/30。</li> <li>• 远端网关：本示例VIF-A01为10.0.0.2/30，VIF-A02为10.1.0.2/30。</li> <li>• 远端子网：此处为IDC侧子网网段，本示例为172.16.0.0/16。</li> <li>• 路由模式：本示例选择“BGP”。</li> <li>• BGP邻居AS号：此处为线下IDC侧的AS号，不能和云上虚拟网关的AS号一样，本示例为65525。</li> </ul>	<ul style="list-style-type: none"> <li>• 迁移前</li> <li>• 迁移中</li> </ul>

资源类型	资源数量	说明	存在阶段
云专线 DC（全域接入网关）	2	<p>以下是迁移后的两个全域接入网关，用来取代 VGW-A，本示例说明如下：</p> <ul style="list-style-type: none"> <li>名称：请根据实际情况填写，本示例为 DGW-B01 和 DGW-B02。</li> <li>BGP ASN：建议全域接入网关和企业路由器的 AS 号不一样，本示例中全域接入网关的 AS 号为 64512。</li> <li>地址类型：请根据实际情况选择，本示例为 IPv4。</li> </ul>	<ul style="list-style-type: none"> <li>迁移中</li> <li>迁移完成</li> </ul>
云专线 DC（全域接入网关 DGW 关联的虚拟接口）	2	<p>以下是迁移后的虚拟接口，关联全域接入网关，VIF-B01 用来取代 VIF-A01，VIF-B02 用来取代 VIF-A02，本示例如下：</p> <ul style="list-style-type: none"> <li>名称：本示例两个虚拟接口分别为 VIF-B01 和 VIF-B02。</li> <li>虚拟接口优先级：此处两个虚拟接口均保持默认选项，选择“优先”。</li> <li>物理连接：本示例中虚拟接口 VIF-B01 关联的物理连接为 DC-01，VIF-B02 关联 DC-02。</li> <li>全域接入网关：本示例中虚拟接口 VIF-B01 关联的全域接入网关为 DGW-B01，VIF-B02 关联 DGW-B02。</li> <li>本端网关：本示例 VIF-B01 为 10.0.0.1/30，VIF-B02 为 10.1.0.1/30。</li> <li>远端网关：本示例 VIF-B01 为 10.0.0.2/30，VIF-B02 为 10.1.0.2/30。</li> <li>路由模式：本示例选择“BGP”。</li> <li>BGP 邻居 AS 号：此处为线下 IDC 侧的 AS 号，不能和云上全域接入网关、ER 等服务的 AS 号一样，本示例为 65525。</li> </ul>	<ul style="list-style-type: none"> <li>迁移中</li> <li>迁移完成</li> </ul>

资源类型	资源数量	说明	存在阶段
企业路由器ER	1	<p>ER和VPC位于同一个区域，本示例详情如下：</p> <ul style="list-style-type: none"><li>名称：请根据实际情况填写，本示例为ER-X。</li><li>ASN：企业路由器不能和线下IDC的AS号一样，且建议企业路由器和全域接入网关的AS号也不一样，由于64512是全域接入网关的系统预留AS号，因此本示例企业路由器的AS号为64513。</li><li>默认路由表关联：开启</li><li>默认路由表传播：开启</li><li>自动接受共享连接：请根据实际情况选择，本示例选择“开启”。</li><li>连接，本示例需要在企业路由器中添加3个连接：<ul style="list-style-type: none"><li>VPC连接：er-attach-VPC-X</li><li>DGW连接：er-attach-DGW-B01和er-attach-DGW-B02</li></ul></li></ul> <p><b>须知</b></p> <p>在ER中添加“虚拟私有云（VPC）”连接时，不开启“配置连接侧路由”功能。</p> <p>开启该功能后，会在VPC路由表中自动添加指向ER的路由，目的地址固定为10.0.0.0/8，172.16.0.0/12，192.168.0.0/16。迁移时，需要手动在VPC路由表中添加规划的大网段路由，不能使用自动添加的路由。</p>	<ul style="list-style-type: none"><li>迁移中</li><li>迁移完成</li></ul>
弹性云服务器ECS	1	<p>ECS主要用来验证网络通信情况，本示例如下：</p> <ul style="list-style-type: none"><li>名称：根据实际情况填写，本示例为ECS-X。</li><li>镜像：请根据实际情况选择，本示例为公共镜像（CentOS 8.2 64bit）。</li><li>网络：<ul style="list-style-type: none"><li>虚拟私有云：选择业务VPC，本示例为VPC-X。</li><li>子网：选择和线下IDC通信的子网，本示例为Subnet-X01。</li></ul></li><li>安全组：请根据实际情况选择，本示例安全组模板选择“通用Web服务器”，名称为Sg-X。</li><li>私有IP地址：192.168.0.137</li></ul>	<ul style="list-style-type: none"><li>迁移前</li><li>迁移中</li><li>迁移完成</li></ul>

## 15.3 DC 直连 VPC 组网迁移流程

本章节介绍将DC直连VPC组网流程迁移至企业路由器ER的总体流程，流程说明如表15-5所示。

表 15-5 迁移 DC 直连 VPC 组网流程说明

步骤	说明
<b>步骤一：创建企业路由器并添加VPC连接</b>	<ol style="list-style-type: none"><li>1. 在和业务VPC相同的区域内，创建1个企业路由器ER-X。</li><li>2. 在企业路由器中添加“虚拟私有云（VPC）”连接，即将业务VPC接入企业路由器中，连接名称为er-attach-VPC-X。</li><li>3. 检查ER路由表中的路由是否已自动添加。</li><li>4. 在VPC路由表中，添加指向ER的大网段路由。</li></ol>
<b>步骤二：在企业路由器中添加DGW-B01连接</b>	<ol style="list-style-type: none"><li>1. 创建一个全域接入网关DGW-B01。 此处DGW-B01是虚拟网关VGW-A迁移后的资源。</li><li>2. 删除虚拟网关VGW-A上的虚拟接口VIF-A01。 删除虚拟接口VIF-A01之前，务必在线下IDC侧网络设备上 进行配置，确保网络流量不会通过虚拟接口VIF-A01。</li><li>3. 在全域接入网关DGW-B01上创建虚拟接口VIF-B01，并将 DGW-B01接入到企业路由器中。 此处虚拟接口VIF-B01是虚拟接口VIF-A01迁移后的资源。</li><li>4. （可选）在线下IDC侧网络设备上配置，使IDC的网络 流量可以通过新的虚拟接口VIF-B01或者指定的虚拟接口 访问云上资源。</li></ol>
<b>步骤三：验证VPC通过ER和线下IDC之间的网络通信情况</b>	<ol style="list-style-type: none"><li>1. 在VPC路由表中，添加指向线下IDC侧任意一台服务器的路 由，用于验证VPC和线下IDC之间的网络通信情况。</li><li>2. 在需要和线下IDC通信的VPC子网内，创建1个ECS，登录 ECS执行ping命令验证。</li><li>3. 验证完成后，删除迁移验证相关的路由和ECS。</li></ol>
<b>步骤四：在企业路由器中添加DGW-B02连接</b>	<ol style="list-style-type: none"><li>1. 创建一个全域接入网关DGW-B02。 此处DGW-B02是虚拟网关VGW-A迁移后的资源。</li><li>2. 删除虚拟网关VGW-A上的虚拟接口VIF-A02。 删除虚拟接口VIF-A02之前，务必在线下IDC侧网络设备上 进行配置，确保网络流量不会通过虚拟接口VIF-A02。</li><li>3. 在全域接入网关DGW-B02上创建虚拟接口VIF-B02，并将 DGW-B02接入到企业路由器中。 此处虚拟接口VIF-B02是虚拟接口VIF-A02迁移后的资源。</li><li>4. （可选）在线下IDC侧网络设备上配置，使IDC的网络 流量可以通过新的虚拟接口VIF-B02或者指定的虚拟接口 访问云上资源。</li></ol>
<b>步骤五：配置DC双链路工作模式</b>	DC双链路可以配置成负载均衡模式或者主备模式，请您根据 实际需求配置路由策略。
<b>步骤六：删除原有虚拟网关</b>	待迁移完成后，VPC-X、全域接入网关DGW-B01和DGW-B02 接入企业路由器中并正常通信，此时可以删除虚拟网关VGW- A。

## 15.4 DC 直连 VPC 组网迁移实施步骤

### 步骤一：创建企业路由器并添加 VPC 连接

**步骤1** 在和业务VPC相同的区域内，创建1个企业路由器ER-X。

创建企业路由器时，同时开启“默认路由表关联”和“默认路由表传播”，更多资源详情请参见[表15-4](#)。

创建企业路由器，具体方法请参见[创建企业路由器](#)。

**步骤2** 在企业路由器中添加“虚拟私有云（VPC）”连接，即将业务VPC接入企业路由器中，连接名称为er-attach-VPC-X。

迁移时，需要手动在VPC路由表中添加规划的大网段路由，因此添加连接时不开启“配置连接侧路由”功能。

添加“虚拟私有云（VPC）”连接，具体方法请参见[在企业路由器中添加VPC连接](#)。

**步骤3** 检查ER路由表中的路由，查看路由表中指向VPC连接的路由。

本示例中，ER开启了“默认路由表关联”和“默认路由表传播”功能，那么在ER中添加“虚拟私有云（VPC）”连接时，系统会自动添加ER指向VPC的路由，无需手动添加，只需要检查即可。

#### 须知

如果您未开启“默认路由表传播”功能，则需要手动在ER路由表中添加指向VPC的路由，具体方法请参见[创建静态路由](#)。

ER路由规划详情，请参见[表15-1](#)和[表15-3](#)。

查看ER路由，具体方法请参见[查看路由](#)。

**步骤4** 在VPC路由表中，添加指向ER的大网段路由。

VPC路由规划详情，请参见[表15-1](#)和[表15-2](#)。

本示例添加的大网段地址为172.16.0.0/15，下一跳为企业路由器。

配置路由信息，具体方法请参见[在VPC路由表中配置路由](#)。

----结束

### 步骤二：在企业路由器中添加 DGW-B01 连接

**步骤1** 创建全域接入网关DGW-B01。

具体方法请参见[创建全域接入网关](#)。

**步骤2** 执行以下操作，在线下IDC网络设备、管理控制台依次删除虚拟网关VGW-A上的虚拟接口VIF-A01。

1. 登录线下IDC侧网络设备，删除虚拟接口VIF-A01的相关配置。

在控制台删除虚拟接口VIF-A01之前，务必在线下IDC侧网络设备上配置，确保网络流量不会通过虚拟接口VIF-A01。

2. 删除虚拟接口VIF-A01。

具体方法请参见[删除虚拟接口](#)。

虚拟接口删除后，在VPC路由表中，指向VGW-A，目的地址为VIF-A01本端网关和远端网关的系统路由将会被同步删除，VPC路由规划详情，请参见[表15-2](#)。

本示例中目的地址为10.0.0.0/30，下一跳为云专线网关的路由将会自动删除。

**步骤3** 在企业路由器中添加“全域接入网关（DGW）”连接。

1. 在云专线管理控制台，执行以下操作：

- a. 创建虚拟接口VIF-B01。
- b. 将全域接入网关DGW-B01接入企业路由器，即添加“全域接入网关（DGW）”连接。

具体方法请参见[创建全域接入网关](#)。

2. 在企业路由器控制台，查看“全域接入网关（DGW）”连接的添加情况。

具体方法请参见[查看连接](#)。

“全域接入网关（DGW）”连接的状态“正常”，表示已成功接入企业路由器中。

由于本示例创建ER时，开启“默认路由表关联”和“默认路由表传播”，因此添加完“全域接入网关（DGW）”连接后，以下均为系统自动配置：

- 在ER默认路由表中创建关联。
- 在ER默认路由表中创建传播，并自动学习IDC侧的路由信息。

需要执行以下步骤连通DC后，才可以在ER路由表中查看到IDC侧的路由信息。

**步骤4**（可选）在线下IDC侧网络设备上配置，使IDC的网络流量可以通过新的虚拟接口VIF-B01或者指定的虚拟接口访问云上资源。

- 如果虚拟接口VIF-B01的路由模式选择“BGP”，则完成[步骤3](#)后，IDC网络流量已可以通过VIF-B01访问云上资源，无需执行当前步骤。
- 如果虚拟接口VIF-B01的路由模式选择“静态路由”，则需要执行当前步骤配置完成后，IDC网络流量才可以通过VIF-B01访问云上资源。
- 如果您不想IDC网络流量访问云上资源经过虚拟接口VIF-B01，则需要执行当前步骤，配置指定的虚拟接口。

----结束

### 步骤三：验证 VPC 通过 ER 和线下 IDC 之间的网络通信情况

**步骤1** 在VPC路由表中，添加指向线下IDC侧任意一台服务器的路由，用于验证VPC和线下IDC之间的网络通信情况。

VPC路由规划详情，请参见[表15-2](#)。

本示例中添加目的地址为172.16.0.12/32，下一跳为企业路由器的路由。

配置路由信息，具体方法请参见[在VPC路由表中配置路由](#)。

**步骤2** 在需要和线下IDC通信的VPC子网内，创建1个ECS。

本示例中需要创建1个ECS，资源详情请参见[表15-4](#)。

创建ECS，具体方法请参见[自定义购买ECS](#)。

**步骤3** 在弹性云服务器的远程登录窗口，执行以下步骤，验证网络通信情况。

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](#)。

**ping 线下IDC侧云服务器地址**

本示例中的云服务器地址务必执行**步骤1**添加到VPC路由表中，命令示例如下：

**ping 172.16.0.12**

回显类似如下信息，表示vpc-X与线下IDC侧可以通过ER通信。

```
[root@ecs-X ~]# ping 172.16.0.12
PING 172.16.0.12 (172.16.0.12) 56(84) bytes of data.
64 bytes from 172.16.0.12: icmp_seq=1 ttl=64 time=0.849 ms
64 bytes from 172.16.0.12: icmp_seq=2 ttl=64 time=0.455 ms
64 bytes from 172.16.0.12: icmp_seq=3 ttl=64 time=0.385 ms
64 bytes from 172.16.0.12: icmp_seq=4 ttl=64 time=0.372 ms
...
--- 172.16.0.12 ping statistics ---
```

**步骤4** 验证完成后，删除迁移验证相关的路由和ECS资源。

1. 在VPC路由表中，删除迁移验证路由。  
删除VPC路由，具体方法请参见[删除路由](#)。
2. 删除验证的ECS。  
删除ECS，具体方法请参见[如何删除、重启弹性云服务器?](#)。

---结束

## 步骤四：在企业路由器中添加 DGW-B02 连接

**步骤1** 创建全域接入网关DGW-B02。

具体方法请参见[创建全域接入网关](#)。

**步骤2** 执行以下操作，在线下IDC网络设备、管理控制台依次删除虚拟网关VGW-A上的虚拟接口VIF-A02。

1. 登录线下IDC侧网络设备，删除虚拟接口VIF-A02的相关配置。  
在控制台删除虚拟接口VIF-A02之前，务必在线下IDC侧网络设备上配置，确保网络流量不会通过虚拟接口VIF-A02。
2. 删除虚拟接口VIF-A02。  
具体方法请参见[删除虚拟接口](#)。  
虚拟接口删除后，在VPC路由表中将会删除指向虚拟网关VGW-A的两条路由，VPC路由规划详情，请参见[表15-2](#)。
  - 目的地址为VIF-A02本端网关和远端网关的系统路由将会被同步删除。  
本示例中目的地址为10.1.0.0/30，下一跳为云专线网关的路由将会自动删除。
  - 目的地址IDC侧子网网段的系统路由将会被同步删除。  
本示例中目的地址为172.16.0.0/16，下一跳为云专线网关的路由将会自动删除。

**步骤3** 在企业路由器中添加“全域接入网关（DGW）”连接。

1. 在云专线管理控制台，执行以下操作：

- a. 创建虚拟接口VIF-B02。
- b. 将全域接入网关DGW-B02接入企业路由器，即添加“全域接入网关（DGW）”连接。

具体方法请参见[创建全域接入网关](#)。

2. 在企业路由器控制台，查看“全域接入网关（DGW）”连接的添加情况。  
具体方法请参见[查看连接](#)。

“全域接入网关（DGW）”连接的状态“正常”，表示已成功接入企业路由器中。

由于本示例创建ER时，开启“默认路由表关联”和“默认路由表传播”，因此添加完“全域接入网关（DGW）”连接后，以下均为系统自动配置：

- 在ER默认路由表中创建关联。
- 在ER默认路由表中创建传播，并自动学习IDC侧的路由信息。

需要执行以下步骤连通DC后，才可以在ER路由表中查看到IDC侧的路由信息。

**步骤4**（可选）在线下IDC侧网络设备上配置，使IDC的网络流量可以通过新的虚拟接口VIF-B02或者指定的虚拟接口访问云上资源。

- 如果虚拟接口VIF-B02的路由模式选择“BGP”，则完成[步骤3](#)后，IDC网络流量已可以通过VIF-B02访问云上资源，无需执行当前步骤。
- 如果虚拟接口VIF-B02的路由模式选择“静态路由”，则需要执行当前步骤配置完成后，IDC网络流量才可以通过VIF-B02访问云上资源。
- 如果您不想IDC网络流量访问云上资源经过虚拟接口VIF-B02，则需要执行当前步骤，配置指定的虚拟接口。

----结束

## 步骤五：配置 DC 双链路工作模式

**步骤1** DC双链路可以配置成负载均衡模式或者主备模式，请您根据实际需求配置路由策略：

- 负载均衡模式，配置方法请参见[通过企业路由器构建DC双链路负载均衡混合云组网（全域接入网关DGW）](#)。
- 主备模式，配置方式请参见[通过企业路由器构建DC双链路主备混合云组网（全域接入网关DGW）](#)。

----结束

## 步骤六：删除原有虚拟网关

### 须知

待迁移完成后，确认VPC-X、全域接入网关DGW-B01和DGW-B02接入企业路由器中并正常通信，此时可以删除虚拟网关VGW-A。

**步骤1** 删除虚拟网关VGW-A。

删除虚拟网关，具体方法请参见[删除虚拟网关](#)。

----结束

# 16 将云连接实例直连 VPC 组网迁移至中心网络和企业路由器

## 16.1 云连接实例直连 VPC 组网迁移方案概述

### 应用场景

华为云未上线企业路由器ER之前，客户使用云连接连通不同区域VPC网络时，需要将VPC直接接入云连接实例中。如果您希望提升跨区域组网的的可扩展性，同时降低维护难度，那么推荐您将网络迁移到云连接中心网络和企业路由器上。

云连接中心网络基于华为云骨干网络面向客户提供全球网络编排能力，帮助用户便捷、安全的创建和管理云上、云下的全球网络资源。您可以将两个及以上不同区域的企业路由器接入中心网络，构成ER对等连接，实现云上跨区域网络互通。

接下来，将主要为您介绍如何将云连接实例直连VPC组网迁移至中心网络和企业路由器。

#### 📖 说明

关于企业路由器更详细的介绍，请参见[企业路由器产品介绍](#)。

### 方案架构

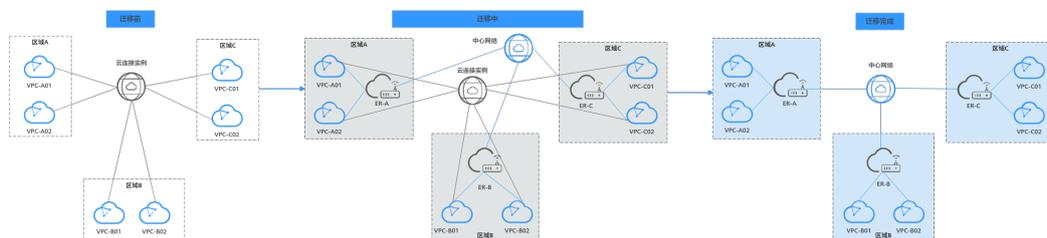
当前组网中，通过云连接实例连通区域A、区域B以及区域C内的VPC网络，为了提升组网的可扩展性，并降低维护难度，现在需要将VPC迁移到企业路由器中，并通过中心网络连通不同区域的企业路由器。

迁移共分为迁移前、迁移中、迁移完成三个阶段，迁移架构图如[图16-1](#)所示。具体说明如下：

1. 迁移前，VPC直接接入云连接实例，通过云连接实例连通不同区域VPC网络。
2. 迁移中：
  - a. 将VPC分别接入对应区域的企业路由器中，通过大小网段确保VPC的路由表中，云连接实例和企业路由器的路由不冲突。
  - b. 创建中心网络，并将不同区域的企业路由器添加到中心网络的策略中，连通不同区域的企业路由器。

- c. 验证VPC通过企业路由器和中心网络是否可以正常通信。
3. 迁移完成后，在云连接实例中依次移除VPC，当所有VPC移除完成后，删除云连接实例。

图 16-1 云连接实例直连 VPC 组网迁移架构图



## 方案优势

企业路由器作为一个云上高性能集中路由器，可以连通多种不同网络服务。

- 通过用企业路由器构建中心辐射性组网，提升网络扩展性。
- 企业路由器支持路由学习，免去繁复配置，降低维护难度。

## 约束与限制

由于组网的复杂程度不同，将云连接实例直连VPC组网迁移至中心网络和企业路由器时，可能会造成业务中断，请您[提交工单](#)联系华为云客服，评估迁移方案。

当业务VPC下存在共享型弹性负载均衡、VPC终端节点、私网NAT网关、分布式缓存服务、混合云DNS解析时，不建议直接将业务VPC接入ER。

了解企业路由器的约束与限制详细信息，请参见[企业路由器约束与限制](#)。

## 16.2 云连接实例直连 VPC 组网迁移资源规划

将云连接实例直连VPC组网迁移至中心网络和企业路由器，迁移开始前，您需要规划资源和组网，本示例中为您详细介绍迁移前、迁移中以及迁移完成后的资源和组网情况。

- **网络规划说明**：规划VPC路由表和ER路由表信息。
- **资源规划说明**：规划云上资源的数量、名称以及主要参数等信息，云上资源包括云连接中心网络、全域互联带宽、ECS、ER等。

### 网络规划说明

迁移过程中，您需要在VPC和ER路由表中添加通信所需的路由，迁移组网规划总体说明请参见[表16-1](#)。

不同迁移过程中组网示意图如下所示：

- [迁移前组网示意图](#)
- [迁移完成后组网示意图](#)

#### 📖 说明

以下路由规划详情仅为示例，供您参考，您需要根据实际业务情况规划路由。

图 16-2 迁移前组网示意图（云连接实例直连 VPC 组网迁移）

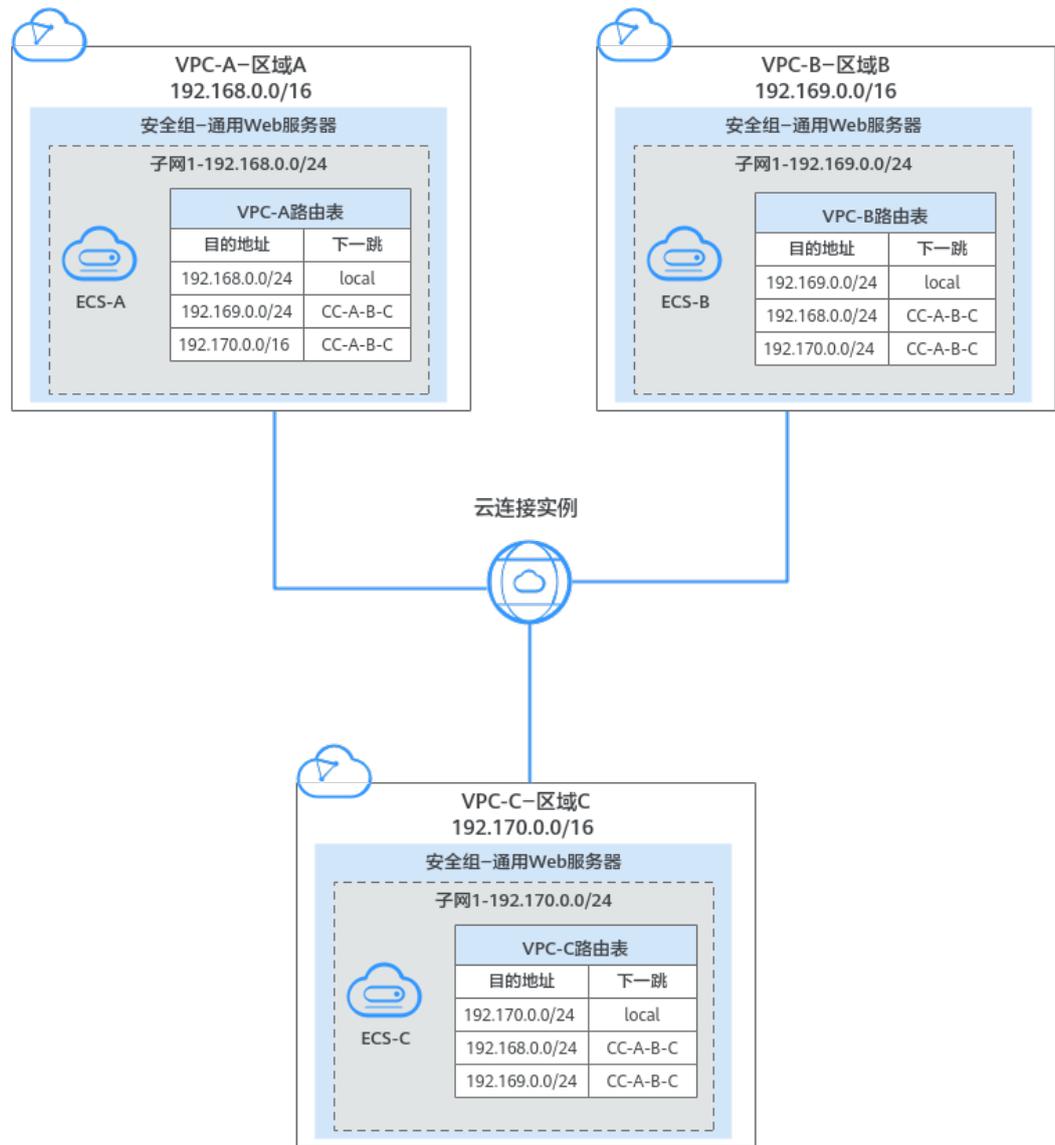


图 16-3 迁移完成后组网示意图（云连接实例直连 VPC 组网迁移）

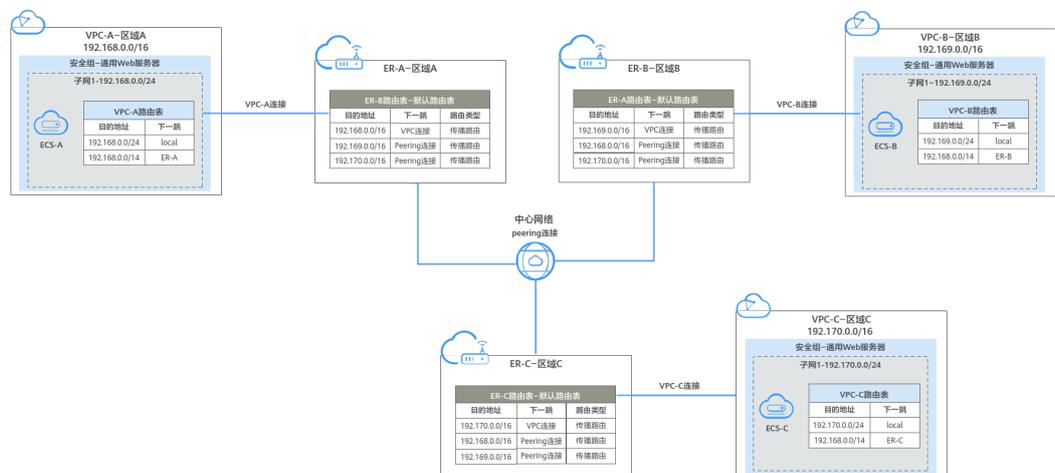


表 16-1 云连接实例直连 VPC 组网迁移规划总体说明

路由表	说明
VPC路由表	<p>VPC路由表的规划详情如表16-2所示。</p> <ol style="list-style-type: none"> <li>迁移前，在VPC的路由表中，存在指向云连接实例的路由，用作不同区域VPC之间通过云连接实例通信。</li> <li>迁移中，为了避免路由冲突无法添加，需要在VPC路由表中，添加指向ER的大网段的路由以及验证路由。 <ol style="list-style-type: none"> <li>指向ER的大网段路由，用作VPC和ER的通信。 该路由的目的地址需要覆盖互通的VPC网段，又不能被其他业务占用。本示例中大网段的地址为192.168.0.0/14，覆盖三个VPC网段，分别为192.168.0.0/16、192.169.0.0/16、192.170.0.0/16。 <b>须知</b> 指向ER的大网段路由需要覆盖业务范围内的所有互通的VPC网段，如果一个网段路由不够，您可以根据实际情况规划多个大网段路由。</li> <li>指向ER的验证路由，用于验证VPC是否可以通过企业路由器和中心网络实现通信，验证完成后即可删除。 该路由的目的地址为网络对端VPC内任意一台ECS的地址。</li> </ol> </li> <li>迁移中，在云连接实例中移除VPC时，会在对应VPC路由表中，同步删除指向云连接的路由。 <b>须知</b> 迁移完成后，您可以根据实际业务需要，选择继续使用大网段路由，或者添加和原有路由目的地址一致的路由后，再删除大网段路由。</li> </ol>
ER路由表	<p>ER路由表的规划详情如表16-3所示。</p> <p>迁移中，在ER路由表中，添加指向ER对等连接的路由，通过ER和中心网络转发VPC之间的流量。</p> <p>当使用中心网络连通ER时，必须开启ER的“默认路由表关联”和“默认路由表传播”功能，那么在ER中添加连接时，系统会自动添加ER指向连接的路由，无需手动添加。</p>
云连接实例路由表	<p>云连接实例的路由表规划详情如表16-4所示。</p> <p>迁移完成后，删除云连接实例时，会同步删除路由。</p>

表 16-2 VPC 路由表规划

VPC名称	VPC路由表名称	目的地址	下一跳类型	下一跳	路由类型	路由说明	存在阶段
VPC-A	rtb-vpc-A	192.169.0.0/24	云连接	CC-A-B-C	系统	目的地址指向VPC-B的子网网段，用作VPC通过云连接实例进行通信	<ul style="list-style-type: none"> <li>迁移前</li> <li>迁移中</li> </ul>

VPC 名称	VPC 路由表名称	目的地址	下一跳类型	下一跳	路由类型	路由说明	存在阶段
		192.170.0.0/24	云连接	CC-A-B-C	系统	目的地址指向 VPC-C 的子网网段，用作 VPC 通过云连接实例进行通信	<ul style="list-style-type: none"> <li>迁移前</li> <li>迁移中</li> </ul>
		192.168.0.0/14	企业路由器	ER-A	自定义	目的地址指向大网段，用作 VPC 通过企业路由器和中心网络进行通信	<ul style="list-style-type: none"> <li>迁移中</li> <li>迁移完成</li> </ul>
		192.169.0.148/32	企业路由器	ER-A	自定义	目的地址指向 VPC-B 中任意一台 ECS，用来验证 VPC-A 和 VPC-B 之间是否可以通过企业路由器和中心网络进行通信	迁移中
		192.170.0.131/32	企业路由器	ER-A	自定义	目的地址指向 VPC-C 中任意一台 ECS，用来验证 VPC-A 和 VPC-C 之间是否可以通过企业路由器和中心网络进行通信	迁移中
VPC-B	rtb-vpc-B	192.168.0.0/24	云连接	CC-A-B-C	系统	目的地址指向 VPC-A 的子网网段，用作 VPC 通过云连接实例进行通信	<ul style="list-style-type: none"> <li>迁移前</li> <li>迁移中</li> </ul>
		192.170.0.0/24	云连接	CC-A-B-C	系统	目的地址指向 VPC-C 的子网网段，用作 VPC 通过云连接实例进行通信	<ul style="list-style-type: none"> <li>迁移前</li> <li>迁移中</li> </ul>
		192.168.0.0/14	企业路由器	ER-B	自定义	目的地址指向大网段，用作 VPC 通过企业路由器和中心网络进行通信	<ul style="list-style-type: none"> <li>迁移中</li> <li>迁移完成</li> </ul>

VPC 名称	VPC 路由表名称	目的地址	下一跳类型	下一跳	路由类型	路由说明	存在阶段
		192.168.0.37/32	企业路由器	ER-B	自定义	目的地址指向 VPC-A 中任意一台 ECS，用来验证 VPC-B 和 VPC-A 之间是否可以通过企业路由器和中心网络进行通信	迁移中
		192.170.0.131/32	企业路由器	ER-B	自定义	目的地址指向 VPC-C 中任意一台 ECS，用来验证 VPC-B 和 VPC-C 之间是否可以通过企业路由器和中心网络进行通信	迁移中
VPC-C	rtb-vpc-C	192.168.0.0/24	云连接	CC-A-B-C	系统	目的地址指向 VPC-A 的子网网段，用作 VPC 通过云连接实例进行通信	<ul style="list-style-type: none"> <li>迁移前</li> <li>迁移中</li> </ul>
		192.169.0.0/24	云连接	CC-A-B-C	系统	目的地址指向 VPC-B 的子网网段，用作 VPC 通过云连接实例进行通信	<ul style="list-style-type: none"> <li>迁移前</li> <li>迁移中</li> </ul>
		192.168.0.0/14	企业路由器	ER-C	自定义	目的地址指向大网段，用作 VPC 通过企业路由器和中心网络进行通信	<ul style="list-style-type: none"> <li>迁移中</li> <li>迁移完成</li> </ul>
		192.168.0.37/32	企业路由器	ER-C	自定义	目的地址指向 VPC-A 中任意一台 ECS，用来验证 VPC-C 和 VPC-A 之间是否可以通过企业路由器和中心网络进行通信	迁移中
		192.169.0.148/32	企业路由器	ER-C	自定义	目的地址指向 VPC-B 中任意一台 ECS，用来验证 VPC-C 和 VPC-B 之间是否可以通过企业路由器和中心网络进行通信	迁移中

表 16-3 ER 路由表规划

ER 名称	ER路由表名称	目的地址	下一跳	连接资源	路由类型	路由说明	存在阶段
ER-A	default RouteTable	192.168.0.0/16	er-attach-VPC-A	VPC-A	传播路由	目的地址指向 VPC-A 的网段, 用作 VPC 和企业路由器的通信	<ul style="list-style-type: none"> <li>• 迁移中</li> <li>• 迁移完成</li> </ul>
		192.169.0.0/16	region-A-region-B	ER-B	传播路由	目的地址指向 VPC-B 的网段, 用作 VPC 通过企业路由器和中心网络进行通信	<ul style="list-style-type: none"> <li>• 迁移中</li> <li>• 迁移完成</li> </ul>
		192.170.0.0/16	region-A-region-C	ER-C	传播路由	目的地址指向 VPC-C 的网段, 用作 VPC 通过企业路由器和中心网络进行通信	<ul style="list-style-type: none"> <li>• 迁移中</li> <li>• 迁移完成</li> </ul>
ER-B	default RouteTable	192.169.0.0/16	er-attach-VPC-B	VPC-B	传播路由	目的地址指向 VPC-B 的网段, 用作 VPC 和企业路由器的通信	<ul style="list-style-type: none"> <li>• 迁移中</li> <li>• 迁移完成</li> </ul>
		192.168.0.0/16	region-B-region-A	ER-A	传播路由	目的地址指向 VPC-A 的网段, 用作 VPC 通过企业路由器和中心网络进行通信	<ul style="list-style-type: none"> <li>• 迁移中</li> <li>• 迁移完成</li> </ul>
		192.170.0.0/16	region-B-region-C	ER-C	传播路由	目的地址指向 VPC-C 的网段, 用作 VPC 通过企业路由器和中心网络进行通信	<ul style="list-style-type: none"> <li>• 迁移中</li> <li>• 迁移完成</li> </ul>
ER-C	default RouteTable	192.170.0.0/16	er-attach-VPC-C	VPC-C	传播路由	目的地址指向 VPC-C 的网段, 用作 VPC 和企业路由器的通信	<ul style="list-style-type: none"> <li>• 迁移中</li> <li>• 迁移完成</li> </ul>
		192.168.0.0/16	region-C-region-A	ER-A	传播路由	目的地址指向 VPC-A 的网段, 用作 VPC 通过企业路由器和中心网络进行通信	<ul style="list-style-type: none"> <li>• 迁移中</li> <li>• 迁移完成</li> </ul>

ER名称	ER路由表名称	目的地址	下一跳	连接资源	路由类型	路由说明	存在阶段
		192.169.0.0/16	region-C-region-B	ER-B	传播路由	目的地址指向VPC-B的网段, 用作VPC通过企业路由器和中心网络进行通信	<ul style="list-style-type: none"><li>• 迁移中</li><li>• 迁移完成</li></ul>

表 16-4 云连接实例路由表规划

云连接实例名称	目的地址	所属实例	路由说明	存在阶段
CC-A-B-C	192.168.0.0/16	VPC-A	目的地址指向VPC-A的网段, 用作VPC通过云连接实例进行通信	<ul style="list-style-type: none"><li>• 迁移前</li><li>• 迁移中</li></ul>
	192.169.0.0/16	VPC-B	目的地址指向VPC-B的网段, 用作VPC通过云连接实例进行通信	<ul style="list-style-type: none"><li>• 迁移前</li><li>• 迁移中</li></ul>
	192.170.0.0/16	VPC-C	目的地址指向VPC-C的网段, 用作VPC通过云连接实例进行通信	<ul style="list-style-type: none"><li>• 迁移前</li><li>• 迁移中</li></ul>

## 资源规划说明

迁移过程中, 您需要创建企业路由器, 中心网络以及全域互联带宽等, 迁移完成后可以释放原有云连接实例, 云连接实例直连VPC组网迁移资源规划总体说明请参见表 16-5。

### 说明

以下资源规划详情仅为示例, 供您参考, 您需要根据实际业务情况规划资源。

表 16-5 云连接实例直连 VPC 组网迁移资源规划总体说明

资源类型	资源数量	说明	存在阶段
虚拟私有云VPC	3	<p>业务VPC，实际运行客户业务的VPC，需要接入ER中，本示例中3个不同区域内各有一个VPC。</p> <ul style="list-style-type: none"><li>● VPC名称：请根据实际情况填写，本示例如下。<ul style="list-style-type: none"><li>- 区域A：VPC-A</li><li>- 区域B：VPC-B</li><li>- 区域C：VPC-C</li></ul></li><li>● IPv4网段：建议不同的VPC网段不能重复，请根据实际情况填写，本示例如下。<ul style="list-style-type: none"><li>- VPC-A：192.168.0.0/16</li><li>- VPC-B：192.169.0.0/16</li><li>- VPC-C：192.170.0.0/16</li></ul></li><li>● 子网名称和IPv4网段：需要互通的VPC子网网段不能重复，否则无法通信。请根据实际情况规划，本示例如下。<ul style="list-style-type: none"><li>- subnet-A01：192.168.0.0/24</li><li>- subnet-B01：192.169.0.0/24</li><li>- subnet-C01：192.170.0.0/24</li></ul></li></ul>	<ul style="list-style-type: none"><li>● 迁移前</li><li>● 迁移中</li><li>● 迁移完成</li></ul>

资源类型	资源数量	说明	存在阶段
企业路由器ER	3	<p>本示例中需要在3个不同区域内各创建一个ER，并接入“对等连接（Peering）”连接和“虚拟私有云（VPC）”连接。</p> <ul style="list-style-type: none"> <li>● 名称：请根据实际情况填写， <ul style="list-style-type: none"> <li>- 区域A：ER-A</li> <li>- 区域B：ER-B</li> <li>- 区域C：ER-C</li> </ul> </li> <li>● ASN：此处建议不同区域企业路由器的AS号不同，本示例如下。 <ul style="list-style-type: none"> <li>- ER-A：64512</li> <li>- ER-B：64513</li> <li>- ER-C：64514</li> </ul> </li> <li>● 默认路由表关联：开启</li> <li>● 默认路由表传播：开启</li> <li>● 自动接受共享连接：请根据实际情况选择，本示例选择“开启”。</li> <li>● 连接：本示例需要在不同区域的企业路由器中分别添加3个连接，本示例如下。 <p><b>ER-A：</b></p> <ul style="list-style-type: none"> <li>- VPC连接：连通VPC-A和ER-A之间的网络，名称为er-attach-VPC-A</li> <li>- Peering连接：连通ER-A和ER-B之间的网络，名称为region-A-region-B</li> <li>- Peering连接：连通ER-A和ER-C之间的网络，名称为region-A-region-C</li> </ul> <p><b>ER-B：</b></p> <ul style="list-style-type: none"> <li>- VPC连接：连通VPC-B和ER-B之间的网络，名称为er-attach-VPC-B</li> <li>- Peering连接：连通ER-B和ER-A之间的网络，名称为region-B-region-A</li> <li>- Peering连接：连通ER-B和ER-C之间的网络，名称为region-B-region-C</li> </ul> <p><b>ER-C：</b></p> <ul style="list-style-type: none"> <li>- VPC连接：连通VPC-C和ER-C之间的网络，名称为er-attach-VPC-C</li> <li>- Peering连接：连通ER-C和ER-A之间的网络，名称为region-C-region-A</li> <li>- Peering连接：连通ER-C和ER-B之间的网络，名称为region-C-region-B</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>● 迁移中</li> <li>● 迁移完成</li> </ul>

资源类型	资源数量	说明	存在阶段
		<p><b>须知</b></p> <ul style="list-style-type: none"> <li>当使用中心网络连通ER时，必须开启ER的“默认路由表关联”和“默认路由表传播”功能。</li> <li>在ER中添加“虚拟私有云（VPC）”连接时，不开启“配置连接侧路由”功能。开启该功能后，会在VPC路由表中自动添加指向ER的路由，目的地址固定为10.0.0.0/8，172.16.0.0/12，192.168.0.0/16。迁移时，需要手动在VPC路由表中添加规划的大网段路由，不能使用自动添加的路由。</li> </ul>	
云连接实例	1	<p>本示例中，有一个云连接实例，并在云连接实例中加入需要网络互通的VPC。</p> <ul style="list-style-type: none"> <li>名称：请根据实际情况填写，本示例为CC-A-B-C。</li> <li>使用场景：虚拟私有云</li> <li>加载网络实例： <ul style="list-style-type: none"> <li>区域A：VPC-A</li> <li>区域B：VPC-B</li> <li>区域C：VPC-C</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>迁移前</li> <li>迁移中</li> </ul>
中心网络	1	<p>本示例中，需要创建一个中心网络，并在中心网络中加入需要网络互通的ER。</p> <ul style="list-style-type: none"> <li>名称：请根据实际情况填写，本示例为GCN-A-B-C。</li> <li>策略： <ul style="list-style-type: none"> <li>区域：区域A；企业路由器：ER-A</li> <li>区域：区域B；企业路由器：ER-B</li> <li>区域：区域C；企业路由器：ER-C</li> </ul> </li> <li>跨地域连接带宽：带宽值请您根据实际情况配置，建议和原始配置保持一致。 <ul style="list-style-type: none"> <li>区域A-区域B：10 Mbit/s</li> <li>区域A-区域C：5 Mbit/s</li> <li>区域B-区域C：20 Mbit/s</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>迁移中</li> <li>迁移完成</li> </ul>

资源类型	资源数量	说明	存在阶段
全域互联带宽	3	<p>本示例中，需要创建3个全域互联带宽，用来连通不同区域的云内骨干网络。</p> <ul style="list-style-type: none"><li>名称：请根据实际情况填写，本示例如下。<ul style="list-style-type: none"><li>连通区域A和区域B：bandwidth-A-B。</li><li>连通区域A和区域C：bandwidth-A-C。</li><li>连通区域B和区域C：bandwidth-B-C。</li></ul></li><li>带宽类型：请根据组网实际情况选择，本示例中区域A、区域B以及区域C位于同一个大区，因此选择“大区带宽”。</li><li>互联大区：请根据组网实际情况选择，本示例中区域A、区域B以及区域C均位于中国大陆，因此选择“中国大陆”。</li><li>指定互通区域：请根据组网实际情况选择。</li></ul>	<ul style="list-style-type: none"><li>迁移中</li><li>迁移完成</li></ul>
弹性云服务器ECS	3	<p>本示例中需要在3个不同VPC内各创建一个ECS，主要用来验证网络互通情况。</p> <ul style="list-style-type: none"><li>名称：根据实际情况填写，本示例如下。<ul style="list-style-type: none"><li>区域A：ECS-A</li><li>区域B：ECS-B</li><li>区域C：ECS-C</li></ul></li><li>镜像：请根据实际情况选择，本示例为公共镜像（CentOS 7.9 64bit）。</li><li>网络：请根据实际情况选择虚拟私有云和子网，本示例如下。<ul style="list-style-type: none"><li>ECS-A：VPC-A、subnet-A01</li><li>ECS-B：VPC-B、subnet-B01</li><li>ECS-C：VPC-C、subnet-C01</li></ul></li><li>安全组：请根据实际情况选择，本示例安全组模板选择“通用Web服务器”，名称为sg-demo。</li><li>私有IP地址：<ul style="list-style-type: none"><li>ECS-A：192.168.0.37</li><li>ECS-B：192.169.0.148</li><li>ECS-C：192.170.0.131</li></ul></li></ul>	<ul style="list-style-type: none"><li>迁移前</li><li>迁移中</li><li>迁移完成</li></ul>

## 16.3 云连接实例直连 VPC 组网迁移流程

本章节介绍将云连接实例直连VPC组网迁移至中心网络和企业路由器ER的总体流程，流程说明如表16-6所示。

表 16-6 云连接实例直连 VPC 组网迁移流程

步骤	说明
<b>步骤一：创建企业路由器并添加VPC连接</b>	<ol style="list-style-type: none"><li>1. 在业务VPC对应的区域内，各创建1个企业路由器。</li><li>2. 分别在企业路由器中添加“虚拟私有云（VPC）”连接，即将业务VPC接入企业路由器中。</li><li>3. 检查ER路由表中的路由是否已自动添加。</li><li>4. 在VPC路由表中，添加指向ER的大网段路由。</li></ol>
<b>步骤二：创建中心网络并连接企业路由器</b>	创建1个云连接中心网络，创建中心网络时需要配置策略，此时需要将不同区域的企业路由器添加到策略中，即在企业路由器中添加“对等连接（Peering）”连接。
<b>步骤三：在中心网络内为跨区域网络链路配置带宽</b>	<ol style="list-style-type: none"><li>1. 创建全域互联带宽，本示例中创建3个全域互联带宽连通不同区域网络。</li><li>2. 为中心网络内的跨区域网连接配置带宽，根据业务的实际需要配置，确保带宽满足业务需求。</li></ol>
<b>步骤四：验证VPC基于中心网络和ER的通信情况</b>	<ol style="list-style-type: none"><li>1. 在VPC路由表中，添加指向其他VPC内任意一台ECS的路由，用于验证VPC和其他VPC的通信。</li><li>2. 在每个VPC的子网内，各创建1个用于通信的ECS，登录ECS执行ping命令验证。</li><li>3. 验证完成后，删除迁移验证相关的路由。</li></ol>
<b>步骤五：执行迁移操作并删除原有云连接实例</b>	<ol style="list-style-type: none"><li>1. 在云连接实例中，依次移除原来加载的VPC。</li><li>2. 每移除一个VPC，则需要验证该VPC和其他VPC的通信情况。</li><li>3. 当所有VPC移除完成后，删除云连接实例以及验证通信的ECS。</li></ol>

## 16.4 云连接实例直连 VPC 组网迁移实施步骤

### 步骤一：创建企业路由器并添加 VPC 连接

**步骤1** 在业务VPC对应的区域内，各创建1个企业路由器。

创建企业路由器时，必须开启“默认路由表关联”和“默认路由表传播”，更多资源详情请参见[表16-5](#)。

创建企业路由器，具体方法请参见[创建企业路由器](#)。

**步骤2** 在每个区域的企业路由器中，依次添加“虚拟私有云（VPC）”连接，即将业务VPC接入企业路由器中。

迁移时，需要手动在VPC路由表中添加规划的大网段路由，因此添加VPC连接时不开启“配置连接侧路由”功能。

添加“虚拟私有云（VPC）”连接，具体方法请参见[在企业路由器中添加VPC连接](#)。

**步骤3** 检查ER路由表中的路由，查看路由表中指向VPC连接的路由。

本示例中，ER开启了“默认路由表关联”和“默认路由表传播”功能，那么在ER中添加“虚拟私有云（VPC）”连接时，系统会自动添加ER指向VPC的路由，无需手动添加，只需要检查即可。

ER路由规划详情，请参见[表16-1](#)和[表16-3](#)。

查看ER路由，具体方法请参见[查看路由](#)。

**步骤4** 在VPC路由表中，添加指向ER的大网段路由。

VPC路由规划详情，请参见[表16-1](#)和[表16-2](#)。

本示例添加的大网段地址为192.168.0.0/14，下一跳为企业路由器。

配置路由信息，具体方法请参见[在VPC路由表中配置路由](#)。

---结束

## 步骤二：创建中心网络并连接企业路由器

**步骤1** 创建1个中心网络，并在策略中添加企业路由器。

中心网络的资源详情，请参见[表16-5](#)。

创建中心网络，具体方法请参见[创建中心网络](#)。

**步骤2** 在企业路由器控制台，查看“对等连接（Peering）”连接的添加情况。

具体方法请参见[查看连接](#)。

“对等连接（Peering）”连接的状态“正常”，表示已成功接入企业路由器中。

由于本示例创建ER时，开启“默认路由表关联”和“默认路由表传播”，因此中心网络的策略配置完成后，即添加完“对等连接（Peering）”连接后，系统会自动添加当前ER指向网络对端ER的路由。

---结束

## 步骤三：在中心网络内为跨区域网络链路配置带宽

为中心网络内的跨区域连接配置带宽，根据业务的实际需要配置，确保带宽满足业务需求，跨地域连接带宽的详细规划请参见[表16-5](#)。

### 说明

云连接服务默认为您在各个区域之间分配了10kbps的域间带宽，用来支撑连通性测试。“对等连接（Peering）”连接添加完成后，您就可以验证网络连通性。

为了业务正常使用，您需要继续执行以下操作购买全域互联带宽，并为跨区域连接配置带宽。

**步骤1** 为连通区域A和区域B的连接配置带宽。

基于购买的全域互联带宽为两个互通的区域配置带宽，具体方法请参见[配置跨地域连接带宽](#)。

**步骤2** 为连通区域A和区域C的连接配置带宽。

**步骤3** 为连通区域B和区域C的连接配置带宽。

---结束

## 步骤四：验证 VPC 基于中心网络和 ER 的通信情况

**步骤1** 在VPC路由表中，添加目的地址指向网络对端VPC中任意一台ECS的路由，用来验证VPC之间是否可以通过企业路由器和中心网络进行通信。

VPC路由规划详情，请参见[表16-2](#)。

配置路由信息，具体方法请参见[在VPC路由表中配置路由](#)。

**步骤2** 在需要验证通信的VPC内，各创建1个ECS。

本示例中需要创建3个ECS，资源详情请参见[表16-5](#)。

创建ECS，具体方法请参见[自定义购买ECS](#)。

**步骤3** 登录ECS，执行以下步骤，验证网络通信情况。

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](#)。

**ping 网络对端VPC内的ECS私有IP地址**

本示例中的ECS的私有地址务必执行[步骤1](#)添加到VPC路由表中，以验证VPC-A和VPC-B的通信情况为例，登录ECS-A，执行以下命令：

**ping 192.169.0.148**

回显类似如下信息，表示VPC-A和VPC-B可以通过ER通信。

```
[root@ecs-A ~]# ping 192.169.0.148
PING 192.169.0.148 (192.169.0.148) 56(84) bytes of data:
64 bytes from 192.169.0.148: icmp_seq=1 ttl=64 time=0.849 ms
64 bytes from 192.169.0.148: icmp_seq=2 ttl=64 time=0.455 ms
64 bytes from 192.169.0.148: icmp_seq=3 ttl=64 time=0.385 ms
64 bytes from 192.169.0.148: icmp_seq=4 ttl=64 time=0.372 ms
...
--- 192.169.0.148 ping statistics ---
```

**步骤4** 当所有VPC之间的网络通信验证完成后，在VPC路由表中，删除迁移验证相关的路由。

删除VPC路由，具体方法请参见[删除路由](#)。

----结束

## 步骤五：执行迁移操作并删除原有云连接实例

**步骤1** 在云连接实例中，依次移除原来加载的VPC。

移除云连接中的VPC，具体方法请参见[删除VPC实例](#)。

**步骤2** 每移除一个VPC，则需要参考[步骤3](#)，验证移除的VPC和其他VPC的通信情况。

待验证正常后，再继续移除下一个VPC。

**步骤3** 当所有VPC移除完成，并且待业务正常运行一段时间后，删除云连接实例以及验证通信的ECS。

1. 删除原有的云连接实例。

删除云连接实例，具体方法请参见[删除云连接实例](#)。

2. 删除验证通信的ECS。

删除ECS，具体方法请参见[如何删除、重启弹性云服务器?](#)。

----结束