ALIBABA CLOUD

# Alibaba Cloud

## Express Connect
## Best Practices

Document Version: 20200820

Alibaba Cloud

# Legal disclaimer

Alibaba Cloud reminds you to carefully read and fully understand the terms and conditions of this legal disclaimer before you read or use this document. If you have read or used this document, it shall be deemed as your total acceptance of this legal disclaimer.

1. You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.

2. No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company or individual in any form or by any means without the prior written consent of Alibaba Cloud.

3. The content of this document may be changed because of product version upgrade, adjustment, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and an updated version of this document will be released through Alibaba Cloud-authorized channels from time to time. You should pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.

4. This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides this document based on the "status quo", "being defective", and "existing functions" of its products and services. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity, applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not take legal responsibility for any errors or lost profits incurred by any organization, company, or individual arising from download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, take responsibility for any indirect, consequential, punitive, contingent, special, or punitive damages, including lost profits arising from the use or trust in this document (even if Alibaba Cloud has been notified of the possibility of such a loss).

5. By law, all the contents in Alibaba Cloud documents, including but not limited to pictures, architecture design, page layout, and text description, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of this document shall be used, modified, reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates. The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates.

6. Please directly contact Alibaba Cloud for any errors of this document.

# Document conventions

| Style | Description | Example |
| --- | --- | --- |
| Danger | A danger notice indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results. | Danger: Resetting will result in the loss of user configuration data. |
| Warning | A warning notice indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results. | Warning: Restarting will cause business interruption. About 10 minutes are required to restart an instance. |
| Notice | A caution notice indicates warning information, supplementary instructions, and other content that the user must understand. | Notice: If the weight is set to 0, the server no longer receives new requests. |
| Note | A note indicates supplemental instructions, best practices, tips, and other content. | Note: You can use Ctrl + A to select all files. |
| > | Closing angle brackets are used to indicate a multi-level menu cascade. | Click **Settings**> **Network**> **Set network type**. |
| **Bold** | Bold formatting is used for buttons , menus, page names, and other UI elements. | Click **OK**. |
| `Courier font` | Courier font is used for commands | Run the `cd /d C:/window` command to enter the Windows system folder. |
| *Italic* | Italic formatting is used for parameters and variables. | `bae log list --instanceid` *Instance_ID* |
| [] or [a\|b] | This format is used for an optional value, where only one item can be selected. | `ipconfig [-all\|-t]` |
| {} or {a\|b} | This format is used for a required value, where only one item can be selected. | `switch {active\|stand}` |

# Table of Contents

1.Use Express Connect physical connections to connect your n... 05
2.Access an ECS instance from an on-premises data center th... 09
3.Configure health checks and routes for redundant physical ... 15

# 1.Use Express Connect physical connections to connect your network to Alibaba Cloud

This topic describes how to connect your network to Alibaba Cloud by using Express Connect physical connections. Through Express Connect physical connections, you can enable highly reliable intranet communication between your on-premises data center and Alibaba Cloud VPCs that belong to different regions.

## Features of Express Connect

Express Connect provides the following key feature:

Physical connection

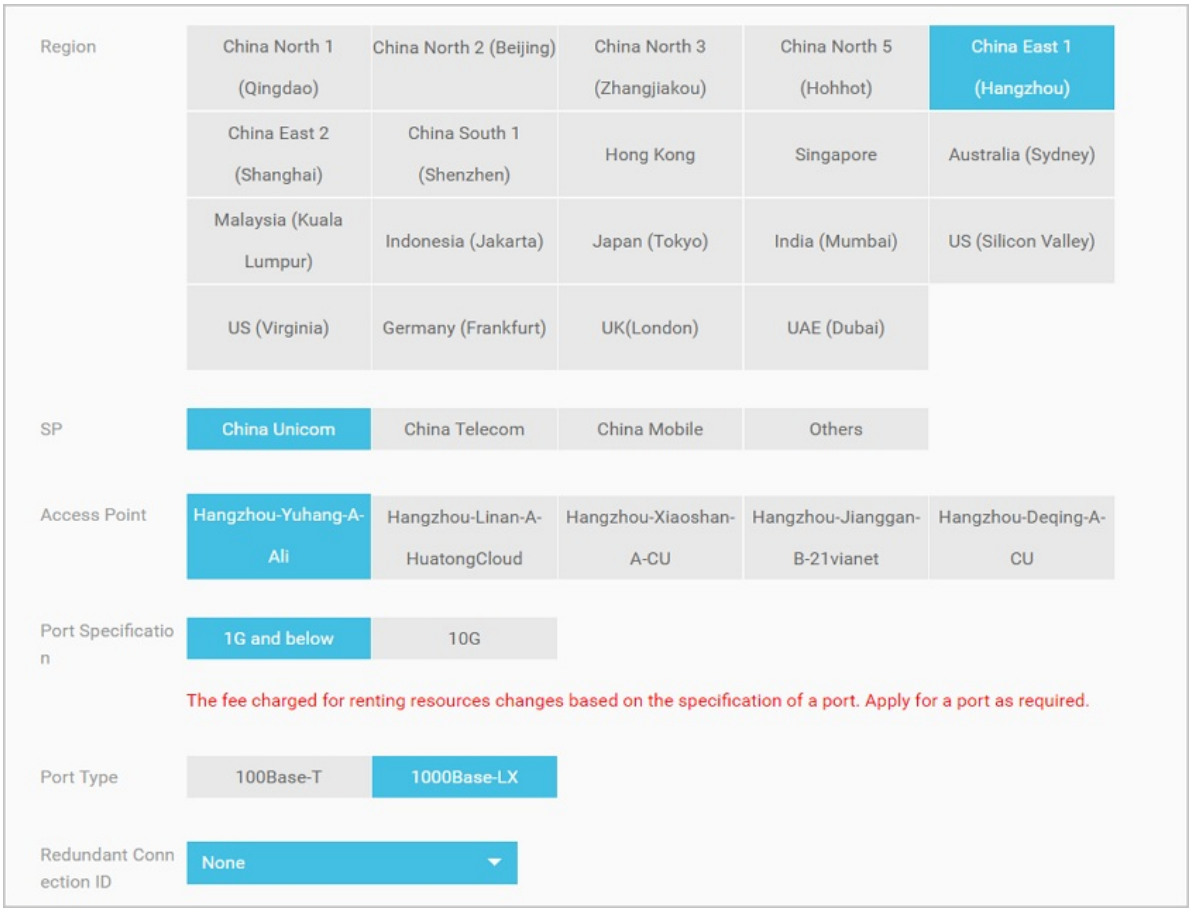
You can use a dedicated line leased from a service provider to physically connect your on-premises data center to Alibaba Cloud. After that, you can create a Virtual Border Router (VBR) and router interfaces (RIs) to achieve communication between the on-premises data center and a VPC in Alibaba Cloud.

## Access points

If you use a dedicated line to connect an on-premises data center to an Alibaba Cloud VPC, you only need to select an access point that is closest in geographic proximity to your on-premises data center and connect the on-premises data center to the access point. You do not need to build a physical connection between your on-premises data center and Alibaba Cloud VPC. Access points include Alibaba Cloud access points and access points provided by Alibaba Cloud partners.

- Alibaba Cloud access points

  You can view all access points of Alibaba Cloud in the Express Connect console. If an access point is available in the city where your on-premises data center is located, you can select this access point for the dedicated line connection.




- Access points of Alibaba Cloud partners

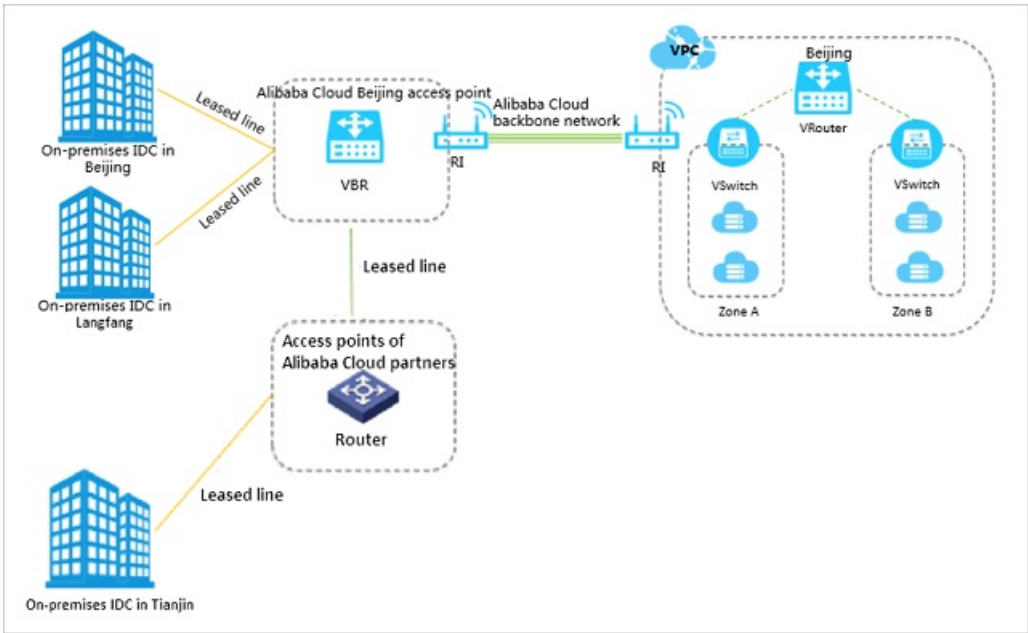
  Some access points are also provided by Alibaba Cloud partners, and are connected with Alibaba Cloud through dedicated physical lines. This means that if no Alibaba Cloud access point is available, you can select an access point provided by one of our partners. You can view the access points of Alibaba Cloud partners in the Express Connect console and contact the Alibaba Cloud partner to obtain the information about your selected dedicated line.

  As a best practice, if no Alibaba Cloud access point or access point provided by an Alibaba Cloud partner is available in the city where your on-premises data center is located, we recommend that you select an access point that is nearest to the city where your on-premises data center is based.

  For example, the following figure shows three on-premises data centers (one in Beijing, one in Langfang, and one in Tianjin) connected to access points.

  - Alibaba Cloud provides access points in Beijing. Therefore, the on-premises data center in Beijing can be connected to an Alibaba Cloud access point in Beijing.
  - No Alibaba Cloud access point is available in Tianjin, but Alibaba Cloud partners provide access points in Tianjin. Therefore, the on-premises data center in Tianjin can be connected to an access point provided by Alibaba Cloud partner.
  - In Langfang, neither Alibaba Cloud access points nor access points are provided by Alibaba Cloud partners are available. However, Langfang is close to Beijing. Therefore, the on-premises data center in Langfang can be connected to an Alibaba Cloud access point in Beijing.

- **Note** The lines in yellow are dedicated lines that need to be installed by your service provider.

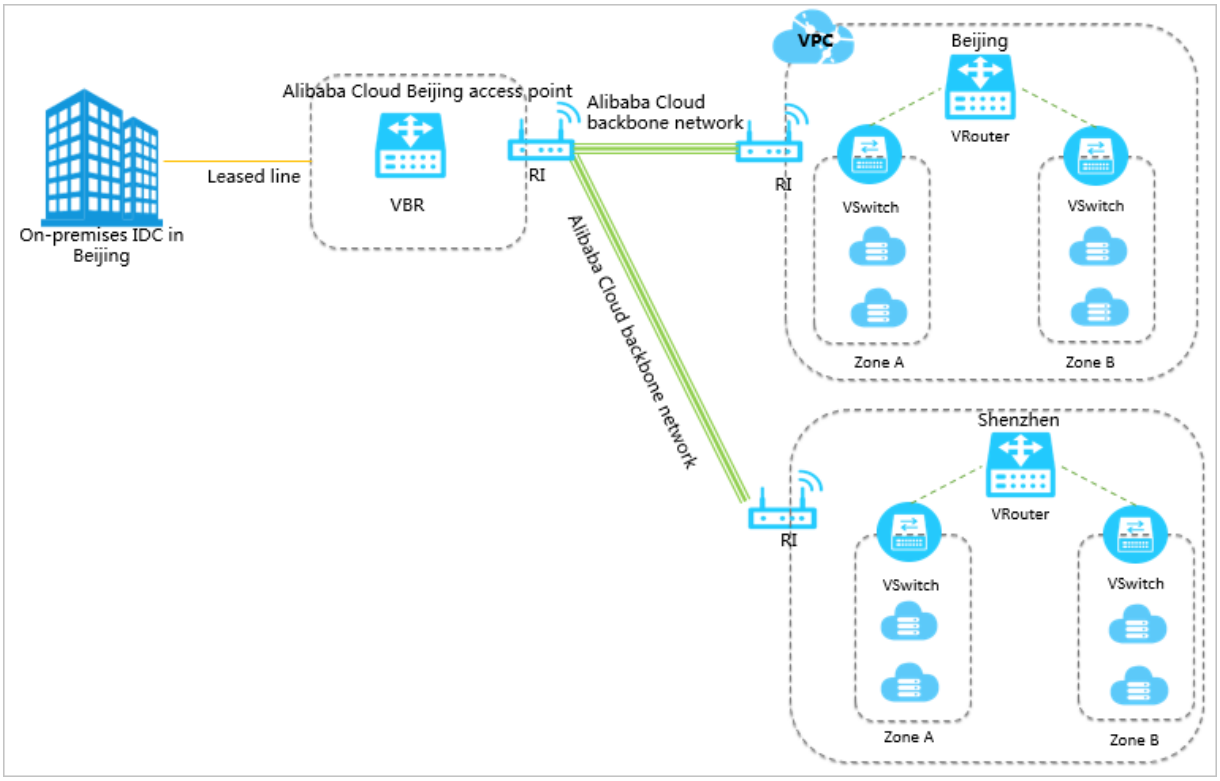



## Access global resources from one point

After you connect your network to one access point, you can connect to Alibaba Cloud VPCs all over the world through this access point.

For example, you want to connect an on-premises data center in Beijing to a VPC in Beijing and a VPC in Shenzhen through a physical connection. To implement that, you only need to use a dedicated line to connect the on-premises data center to an Alibaba Cloud Beijing access point, and create two router interfaces on the VBR to respectively connect to the two VPCs.

**Note** In the following figure, only the lines in yellow need to be installed by your service provider.


VPC
Beijing
VRouter
Alibaba Cloud Beijing access point
Alibaba Cloud backbone network
Leased line
VBR
RI
RI
VSwitch
VSwitch
On-premises IDC in Beijing
Zone A
Zone B
Alibaba Cloud backbone network
Shenzhen
VRouter
RI
VSwitch
VSwitch
Zone A
Zone B

# 2.Access an ECS instance from an on-premises data center through a physical connection

This topic describes how to access an Elastic Compute Service (ECS) instance in an Alibaba Cloud Virtual Private Cloud (VPC) from a server of an on-premises data center by using Express Connect.

## Context

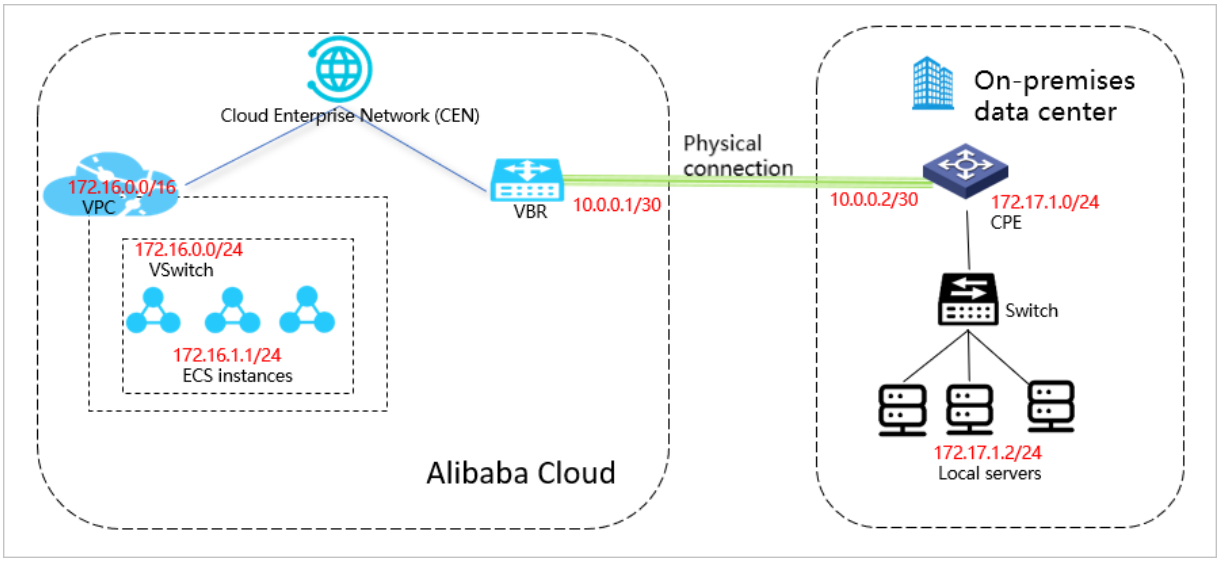
If you need to access the cloud resources in a VPC from your on-premises data center by using a physical connection, you must add a route entry with the destination CIDR block 100.64.0.0/10 and the next hop of the target VPC in the corresponding Virtual Border Router (VBR). Also, you must add a route entry that points to 100.64.0.0/10 with the Alibaba Cloud-side IP address of the VBR as the next hop on the gateway device of your on-premises data center.

The CIDR block 100.64.0.0/10 is reserved for VPCs. It is used by the cloud services in VPCs, such as Domain Name System (DNS), Object Storage Service (OSS), and Log Service.

> **Note** Because the CIDR block 100.64.0.0/10 is reserved for VPCs, you cannot directly add a route entry that points to 100.64.0.0/10 in the VBR. You can divide the CIDR block 100.64.0.0/10 into 100.64.0.0/11 and 100.96.0.0/11, and add two route entries in the VBR.

## Background information

In this topic, the configurations of the VPC and on-premises data center shown in the following figure are used as an example. Assume that your on-premises data center (CIDR block: 172.17.1.0/24) is located in Hangzhou. You have a VPC (CIDR block: 172.16.0.0/16) in the China (Hangzhou) region. You want to use a physical connection to access an ECS instance (IP address: 172.16.1.1) in the VPC from a server (IP address: 172.17.1.2) at the on-premises data center.



| Parameter | Value |
| --- | --- |
| CIDR block of the VPC | 172.16.0.0/16 |
| CIDR block of the VSwitch | 172.16.0.0/24 |
| IP address of the ECS instance | 172.16.1.1/24 |
| CIDR block of the on-premises data center | 172.17.1.0/24 |
| IP addresses used for the connection | • IP address used by the VBR: 10.0.0.1/30<br>• IP address used by the on-premises data center: 10.0.0.2/30 |
| IP address of the local server | 172.17.1.2/24 |
| IP addresses used for health checks | • Source IP address: 172.16.1.2<br>• Destination IP address: 10.0.0.2 |

## Step 1: Establish a physical connection

You can establish an exclusive physical connection by applying for a physical connection interface in the Express Connect console yourself or establish a shared physical connection by using a shared port of an Alibaba Cloud partner. For more information, see Create a dedicated physical connection and Establish a shared physical connection.

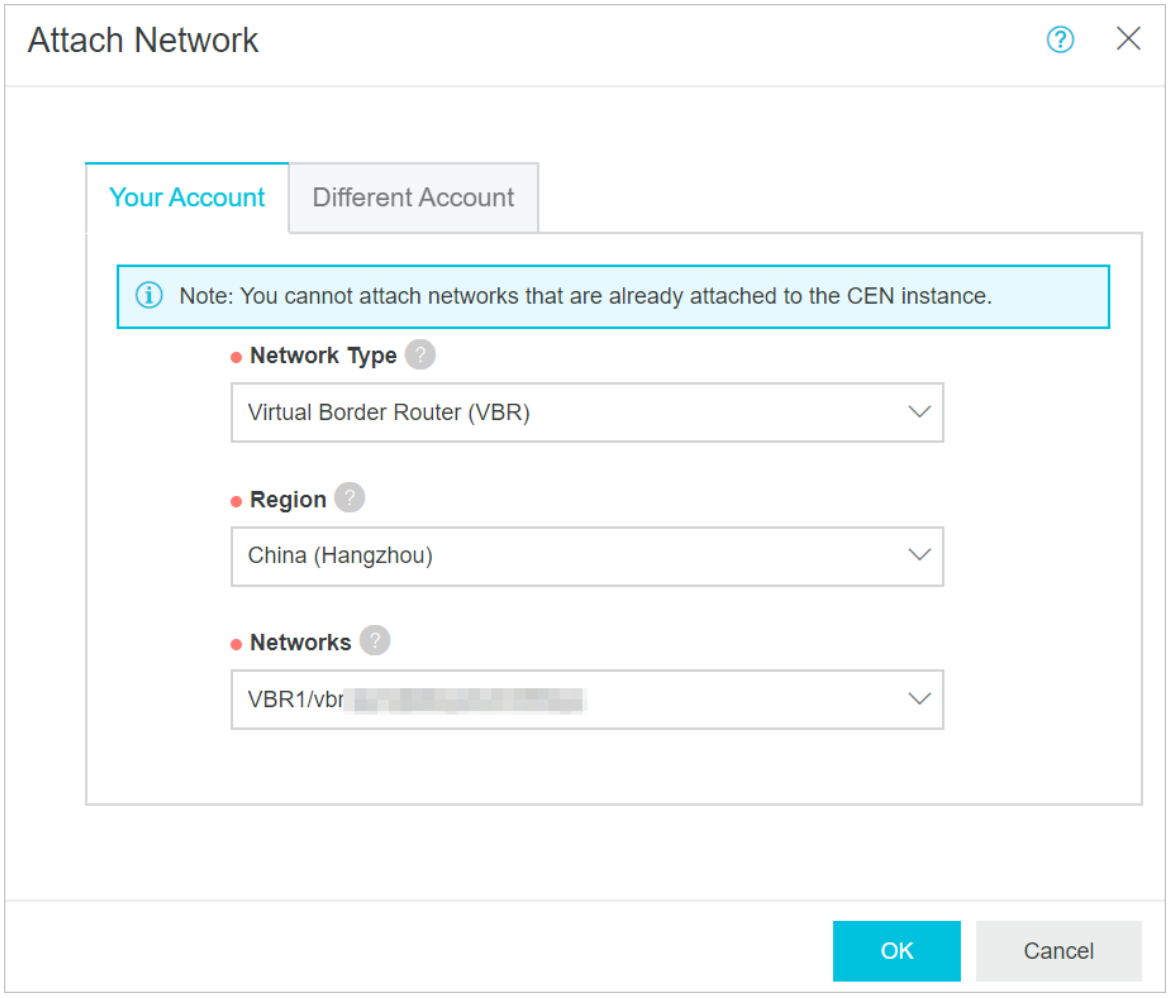
In this example, configure the VBR associated with the physical connection as follows:

| Configuration | Value |
| --- | --- |
| VLANID | 0 |
| Alibaba Cloud-side IP address | 10.0.0.1 |
| Customer-side IP address | 10.0.0.2 |
| Subnet mask | 255.255.255.252 |

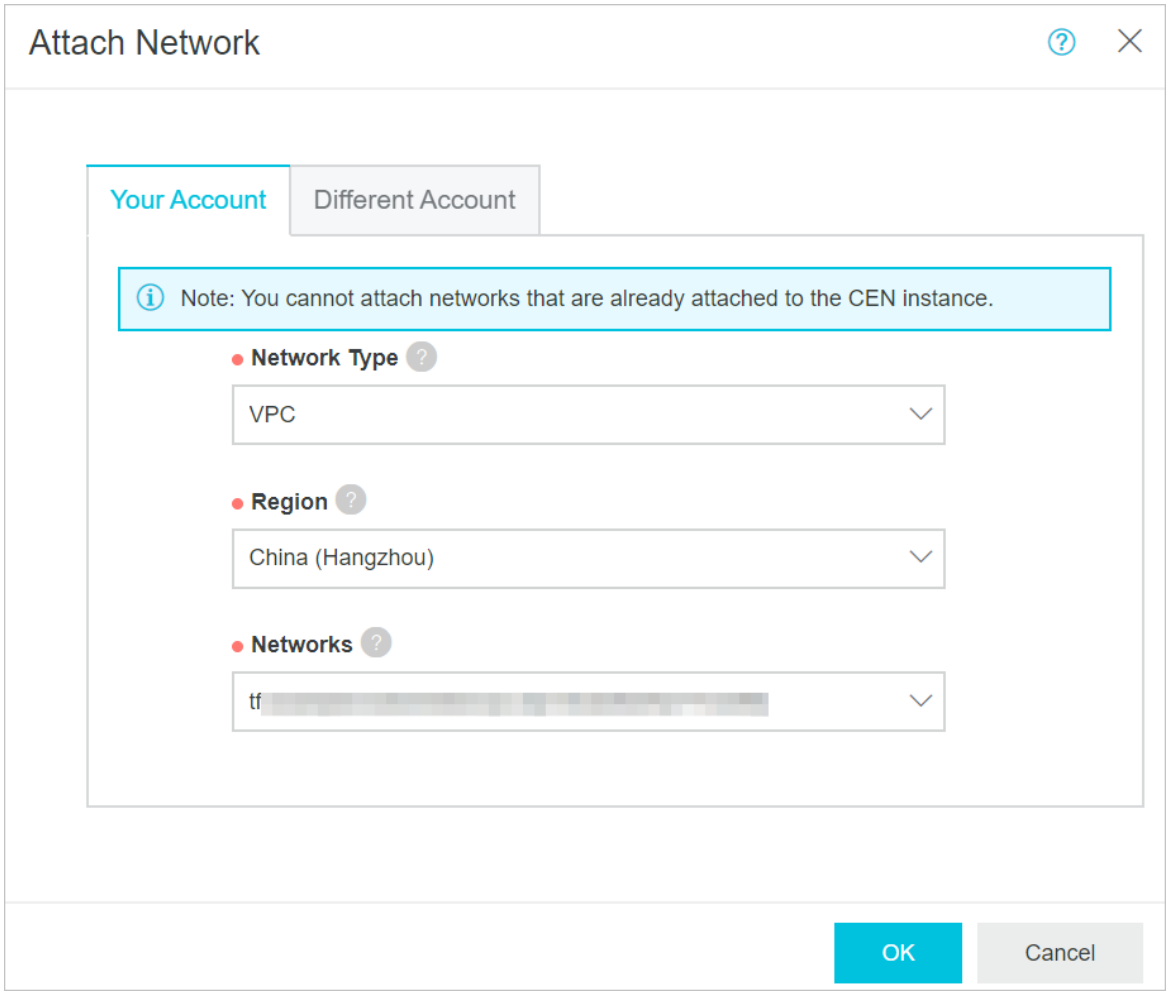
## Step 2: Add the VPC and VBR to a CEN instance

After the physical connection is established, add the VBR and VPC to be connected to the same Cloud Enterprise Network (CEN) instance.

1. Log on to the CEN console.
2. On the **Instances** page, find the target CEN instance and click the instance ID. Make sure that a CEN instance is created. For more information, see Create a CEN instance.
3. On the **Networks** tab, click **Attach Network** and add the VBR to the CEN instance. For more information, see Attach networks.




4. Click **Attach More** to add the VPC to the CEN instance.




## Step 3: Configure VBR routes

After you add the VBR and VPC to the same CEN instance, add a route pointing to the on-premises data center in the VBR.

1. Log on to the Express Connect console.
2. In the left-side navigation pane, choose **Virtual Border Routers (VBRs) > Virtual Border Routers (VBRs)**. Find the target VBR and click the instance ID.
3. On the VBR details page, click the **Routes** tab and then click **Add route**.
4. In the **Add Route** dialog box that appears, configure the route as follows:
   - **Destination Subnet**: Enter the CIDR block of the on-premises data center. In this example, enter *172.17.1.0/24*.
   - **Next Hop Type**: Select **Physical Connection Interface**.
   - **Next Hop**: Select the physical connection you established in Step 1.
5. Click **OK**.

## Step 4: Configure health checks

To configure health checks, follow these steps:

1. Log on to the CEN console.
2. In the left-side navigation pane, click **Health Check**.

3. Select the region of the target CEN instance. In this example, select **China (Hangzhou)**. Then, click **Set Health Check**.
4. On the **Set Health Check** page, configure health checks as follows:
   - **Instances**: Select the CEN instance with which the VBR is associated.
   - **Virtual Border Router (VBR)**: Select the VBR to be monitored.
   - **Source IP**: Enter an idle IP address under the VSwitch of the connected VPC, for example, 172.16.1.2.
   - **Destination IP**: Enter the interface IP address of the network device at the on-premises data center, for example, 10.0.0.2.

## Step 5: Configure routes for the on-premises data center

After you complete the preceding steps, the route configurations on Alibaba Cloud are completed. You must configure a route pointing to the VPC on the network device of the on-premises data center. You can configure a static route or BGP route to forward traffic from the on-premises data center to the VBR.

1. Configure a static route or BGP dynamic route on the gateway device of the on-premises data center.
   - The following is an example of a static route and is for reference only. Configurations for devices of different manufacturers are different.

     ```
     ip route 172.16.0.0 255.255.0.0 10.0.0.1
     ```

   - You can also configure a BGP route. For more information, see Configure BGP.

     The CIDR block to be advertised is the CIDR block of the VPC that needs to communicate with the on-premises data center. The IP address of the next hop, namely, the VBR, is 10.0.0.1. In this example, the CIDR block of the VPC is 172.16.0.0/16.
2. On the local gateway device, **ping** the IP address of the VBR to check the connectivity. Run the **ping** command `ping 10.0.0.1`. If the ping test succeeds, the physical connection between the local gateway and Alibaba Cloud is successful.
3. Run the following command to add a default route that points to the local gateway on the local server:

   ```
   route add default gw 172.17.1.1
   ```

## Step 6: Test the connectivity from the local server

To test the connectivity between the local server and Alibaba Cloud, follow these steps:

1. Open the command prompt on the server of the on-premises data center.
2. Run the **ping** command to ping the IP address of the VBR **10.0.0.1**. If the ping test succeeds, the physical connection from the local server to Alibaba Cloud is successful.

> **Note** At this stage, if you run a ping test on the ECS instance to ping the IP address of the VBR, the ping test will fail.

## Step 7: Test the connectivity from the ECS instance

Make sure that an ECS instance is created. IP addresses of ECS instances are dynamically allocated. Use the actual internal IP address of the ECS instance in this step. In this example, the IP address of the ECS instance is `172.16.1.1`.

1. Open the command prompt on the local server.
2. Run the **ping** command `ping 172.16.1.1`.
3. Open the command prompt on the ECS instance.
4. Run the **ping** command `ping 172.17.1.2`. If the ping test succeeds, the physical connection between the local server and the ECS instance is successful.

# 3.Configure health checks and routes for redundant physical connections

This topic describes how to configure health checks and routes for redundant physical connections. To make sure that traffic is forwarded to the standby physical connection when the active physical connection fails, you must configure health checks for the associated VBR-to-VPC peering connections and configure routes.

## Prerequisites

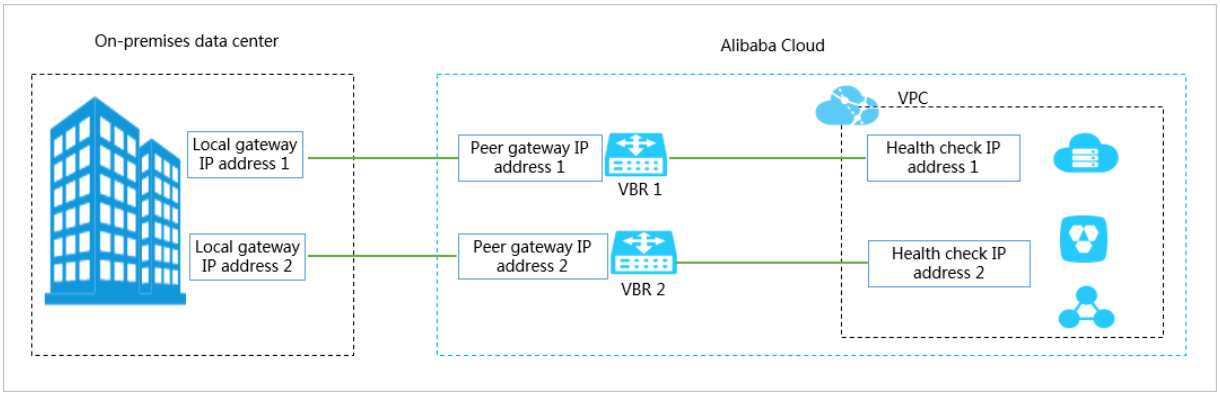
Before you configure health checks and routes, make sure that the following operations are completed:

- Two physical connection interfaces are applied for and the connection between the on-premises data center and Alibaba Cloud is established.
- Two VBR-to-VPC peering connections are created. For more information, see Create a dedicated physical connection and Interconnect a VPC and a VBR.
- Static routing is configured between the Virtual Border Routers (VBRs) and the on-premises data center. No BGP is used.

## Context

Alibaba Cloud sends a ping packet once every two seconds from the health check IP address to the customer-side IP address of the on-premises data center. If no response is received for the ping packet for eight consecutive times on the physical connection, traffic is switched to the other physical connection.

> **Note** If Control Plane Policing (Copp) (such as Cisco devices) or Local Attack Defense Policy (such as Huawei devices) is configured on the on-premises data center network device, health check packets may be discarded and the health check link shocks. Therefore, we recommend that you cancel the speed limitation on the network device of the on-premises data center.




In this topic, the following network configurations are used as an example:

| Configuration | CIDR block |
| --- | --- |
| The connected VPC | 192.168.0.0/16 |

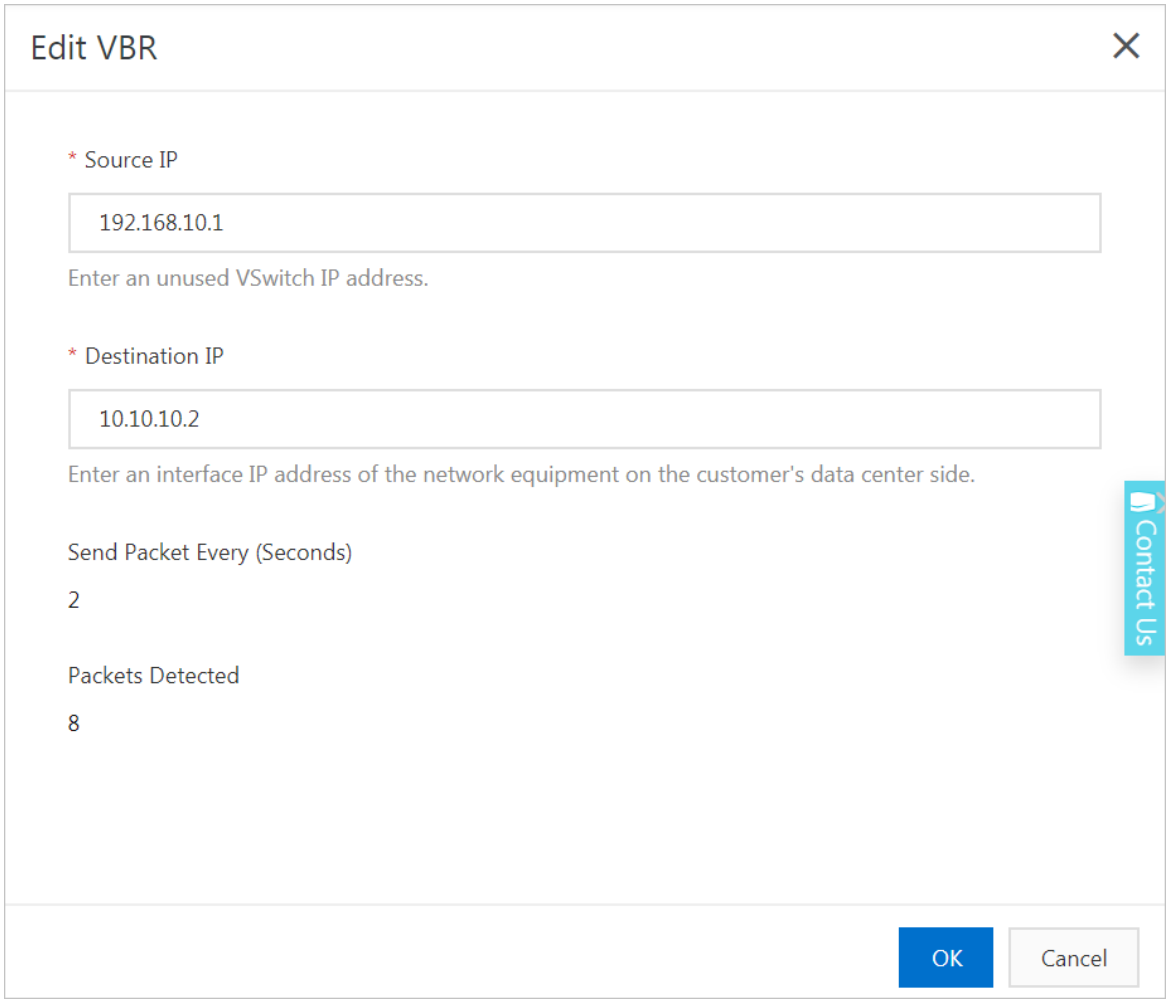
| Configuration | CIDR block |
| --- | --- |
| On-premises data center | 172.16.0.0/16 |
| The connection between one VBR and the on-premises data center | • VBR gateway IP address: 10.10.10.1<br>• Gateway IP address of the on-premises data center: 10.10.10.2<br>• Subnet mask: 255.255.255.252 |
| The connection between the other VBR and the on-premises data center | • VBR gateway IP address: 10.10.11.1<br>• Gateway IP address of the on-premises data center: 10.10.11.2<br>• Subnet mask: 255.255.255.252 |
| Health checks for one VBR-to-VPC peering connection | • Source IP address: 192.168.10.1<br>• Destination IP address: 10.10.10.2 |
| Health checks for the other VBR-to-VPC peering connection | • Source IP address: 192.168.10.2<br>• Destination IP address: 10.10.11.2 |

## Step 1: Configure health checks

You must configure health checks for the two peering connections. To do so, follow these steps:

1.
2.
3. In the left-side navigation pane, choose **VPC Peering Connections** > **VBR-to-VPC**.
4. Find the target peering connection and choose  > **Health Check** in the **Actions** column.
5. On the **Health Check** page, click **Configure**.
6. On the **Edit VBR** page, configure health checks. The following table shows the required parameters.

| Parameter | Description |
| --- | --- |
| Source IP | Any idle private IP address in the connected VPC. |
| Destination IP | The interface IP address of the network device of the on-premises data center.<br>If you need to perform ICMP health checks from the on-premises data center to the VPC, enter the health check IP address of the VPC as the destination IP address and configure a route that points to this new health check destination. |




7. Click **OK**.
8. Repeat the preceding steps to configure health checks for the other peering connection.

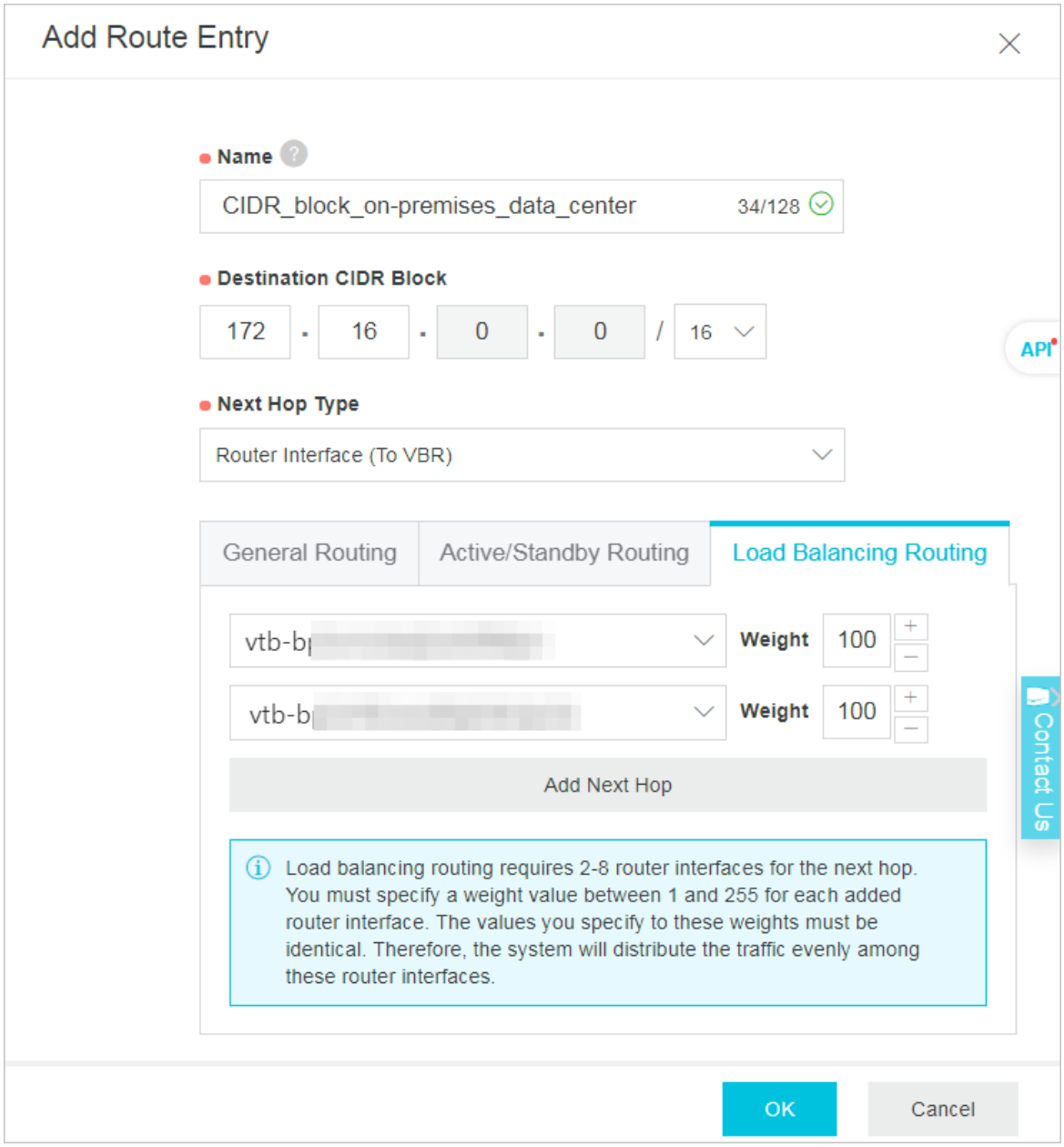
> **Note** The source IP address of the health checks for the other peering connection cannot be the same as that for the first peering connection.

## Step 2: Configure routes

In this example, load balancing routing is configured.

1.
2.
3. In the left-side navigation pane, choose **Route Tables**.
4. Find the target VPC and click the ID of the corresponding route table.
5. On the **Route Table** page, click **Add Route Entry** and configure the load balancing route. Configure the load balancing route according to the following information:
   - **Destination CIDR Block**: Enter the destination CIDR block to which traffic is forwarded.
   - **Next Hop Type**: Select **Router Interface (To VBR)**, which means forwarding the traffic with a destination IP address that falls into the destination CIDR block to the router interface associated with the VBR.

Select **Load Balancing Routing** for the routing type, select the two VBRs connected with the VPC as the next hop, and set weights for the two VBRs. Value range of the weights of the VBRs: 1 to 255. Default value: 100. The weights of the two VBRs must be the same so that traffic can be evenly distributed to them.



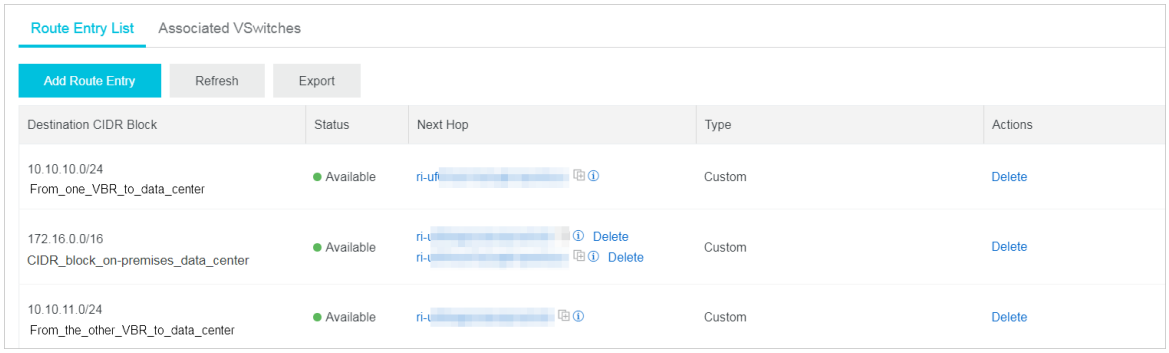

6. Click **Add Route Entry** and add a route from one VBR to the on-premises data center. Configure the route according to the following information:
   - **Destination CIDR Block**: Enter the destination CIDR block.
   - **Next Hop Type**: Select **Router Interface (To VBR)**, which means forwarding the traffic with a destination IP address that falls into the destination CIDR block to the router interface associated with the VBR.

     Select **General Routing** for the routing type and select one VBR as the next hop.
7. Click **Add Route Entry** and configure a route from the other VBR to the on-premises data center. Configure the route according to the following information:

- **Destination CIDR Block**: Enter the destination CIDR block.
- **Next Hop Type**: Select **Router Interface (To VBR)**, which means forwarding the traffic with a destination IP address that falls into the destination CIDR block to the router interface associated with the VBR.

  Select **General Routing** for the routing type and select the other VBR as the next hop.

The following figure shows the configured routes.




## Step 3: Configure static routes on the network device of the on-premises data center

If no BGP is used, the following static routes need to be configured between the on-premises data center and the VBRs on the network device of the on-premises data center:

- A route entry with the health check source IP address of one peering connection as the destination IP address and the IP address of the corresponding VBR (Alibaba Cloud-side IP address) as the next hop.
- A route entry with the health check source IP address of the other peering connection as the destination IP address and the IP address of the corresponding VBR as the next hop.

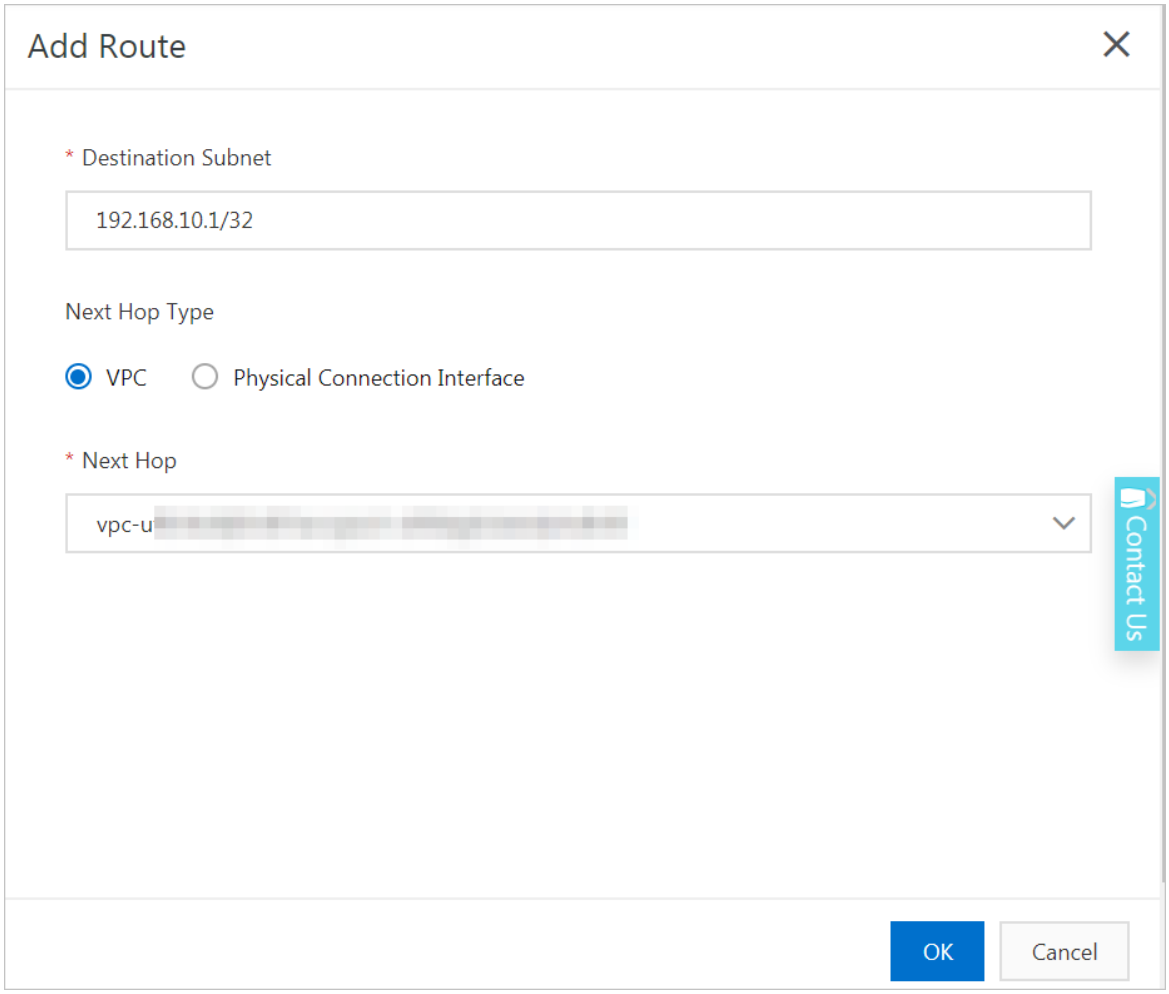
## Step 4: Test the network connectivity

Ping an instance in the VPC when one physical connection fails to check if the redundant physical connection works.

## Advertise BGP CIDR blocks

If you have configured BGP for your on-premises data center and the VBRs, the VBRs need to advertise BGP CIDR blocks.

1.
2.
3. In the left-side navigation pane, choose **Physical Connections** > **Virtual Border Routers (VBRs)**.
4. Find one of the two VBRs and click the VBR ID. On the **Routes** tab, click **Add Route**.
5. On the **Add Route** page, configure a route pointing to the health check source IP address. Configure the route according to the following information:
   - **Destination Subnet**: Enter the source IP address of health checks. In this example, enter 192.168.10.1/32.
   - **Next Hop Type**: Select **VPC**. Then, select the connected VPC as the next hop.




6. Click the **Advertised BGP Subnets** tab and click **Advertise BGP Subnet**.
7. On the **Advertise BGP Subnet** page, enter the source IP address of health checks.


8. Repeat the preceding steps to advertise BGP CIDR blocks for the health check source IP address of the other VBR.