# Alibaba Cloud
# Cloud Enterprise Network

## Best Practices

Issue: 20190530

# 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 due to product version upgrades , adjustments, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and the updated versions of this document will be occasionally released through Alibaba Cloud-authorized channels. You shall 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 the document in the context that Alibaba Cloud products and services are provided on an "as is", "with all faults " and "as available" basis. 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 bear any liability for any errors or financial losses incurred by any organizations, companies, or individuals arising from their download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, bear responsibility for any indirect, consequential, exemplary, incidental, 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 content of the Alibaba Cloud website, including but not limited to works, products, images, archives, information, materials, website architecture, website graphic layout, and webpage design, 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 the Alibaba Cloud website, product programs, or content 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 contact Alibaba Cloud directly if you discover any errors in this document.

# Generic conventions

Table -1: Style conventions

| Style | Description | Example |
| --- | --- | --- |
|  | This warning information indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results. |  Danger:<br>Resetting will result in the loss of user configuration data. |
|  | This warning information indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results. |  Warning:<br>Restarting will cause business interruption. About 10 minutes are required to restore business. |
|  | This indicates warning information, supplementary instructions, and other content that the user must understand. |  Notice:<br>Take the necessary precautions to save exported data containing sensitive information. |
| | This indicates supplemental instructions, best practices, tips, and other content that is good to know for the user. |  Note:<br>You can use Ctrl + A to select all files. |
| > | Multi-level menu cascade. | Settings > Network > Set network type |
| Bold | It is used for buttons, menus , page names, and other UI elements. | Click OK. |
| `Courier font` | It is used for commands. | Run the `cd / d C :/ windows` command to enter the Windows system folder. |
| *Italics* | It is used for parameters and variables. | `bae log list --instanceid` *Instance_ID* |
| [] or [a\|b] | It indicates that it is a optional value, and only one item can be selected. | `ipconfig` *[-all\|-t]* |

| Style | Description | Example |
| --- | --- | --- |
| {} or {a\|b} | It indicates that it is a required value, and only one item can be selected. | `swich {stand \| slave}` |

# Contents

# 1 Connect a local data center to Alibaba Cloud using BGP active/standby links

This tutorial introduces how to use physical connections and CEN to connect a local data center to Alibaba Cloud, and enable the local data center to communicate with VPCs in different regions.

## Overview

To configure active/standby links to access Alibaba Cloud, follow these steps:

1. Build redundant physical connections

   Create redundant physical connections to connect the local data center to Alibaba Cloud. Configure BGP routing between the local data center and the VBRs.
2. Configure health checks

   Configure health checks so that when the active link fails, traffic is distributed to the standby link. For more information, see *Health check*.
3. Attach the VBRs and VPCs that the local data center requires to connect to the created CEN instance.
4. Configure routes

   You can set the routing priority by configuring the length of the AS-Path. For more information, see *Advertise BGP routes and set the routing weights at the local data center*.

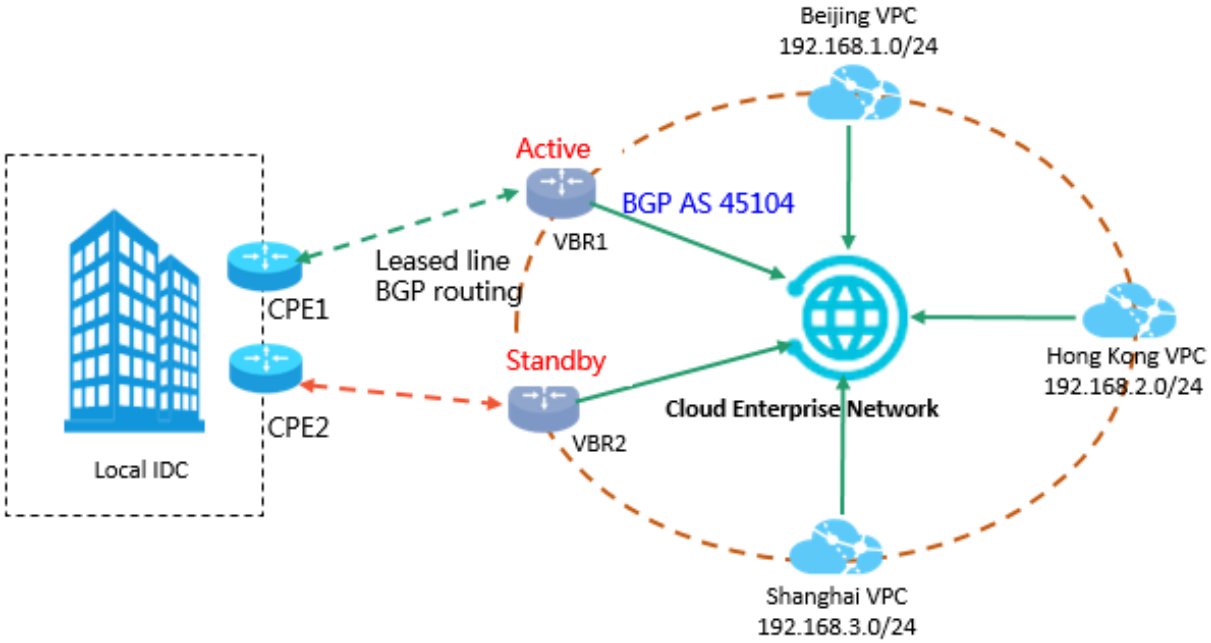
## Network topology

The network topology used in this tutorial is as follows:

- The local data center is already connected to different VBRs through redundant physical connections. The BGP protocol is used between the local data center and the VBRs.
- Separate VPCs are already created in the China (Beijing), China (Shanghai), and Hong Kong regions.
- The CIDR blocks used in this tutorial are as follows:

| Network | CIDR block |
| --- | --- |
| Local data center | 10.1.1.0/24 |
| Beijing VPC | 192.168.1.0/24 |

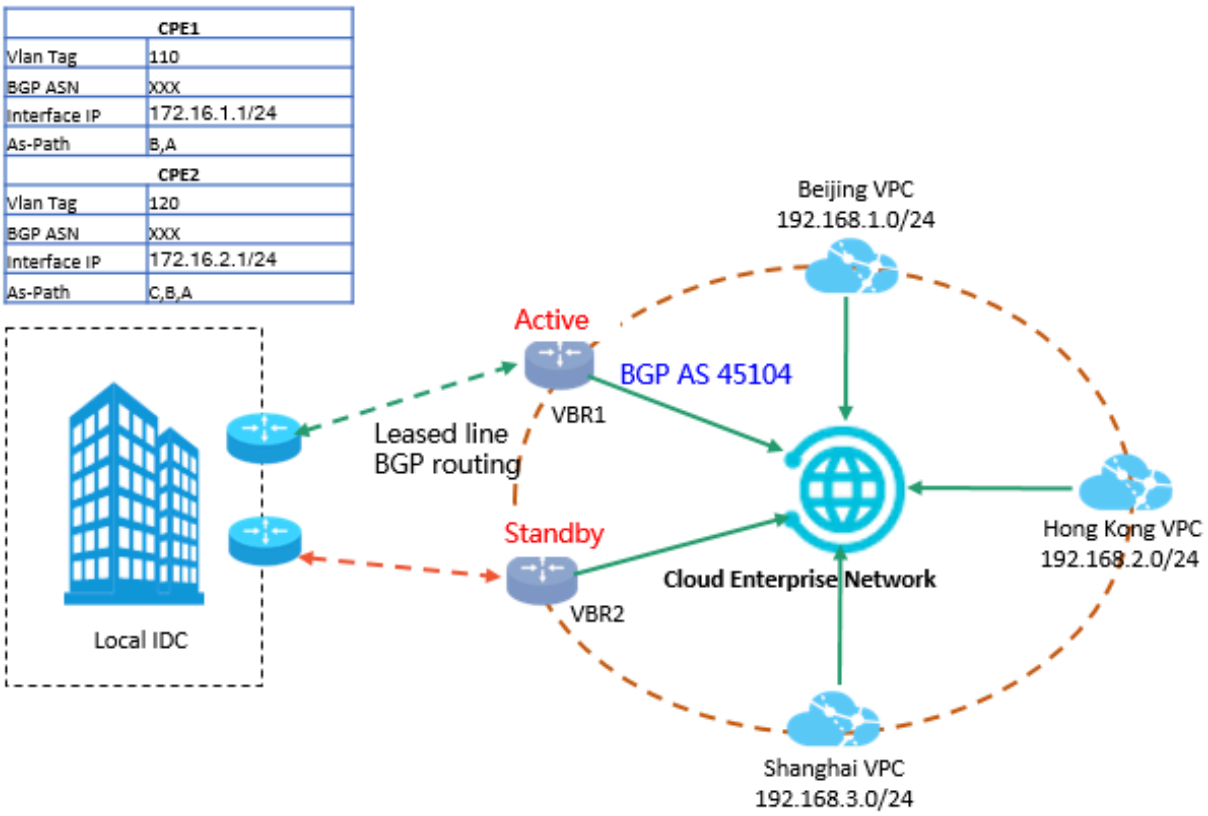
| Network | CIDR block |
| --- | --- |
| Hong Kong VPC | 192.168.2.0/24 |
| Shanghai VPC | 192.168.3.0/24 |




Advertise BGP routes and set the routing weights at the local data center

Assume that BGP peering sessions have been established between the local data center and each VBR (for more information, see *Create a BGP peer*).

You must configure the BGP route (10.1.1.0/24) advertised to Alibaba Cloud and set the AS-Path to determine the routing weights at the local data center to implement active/standby routes from Alibaba Cloud to IDC.



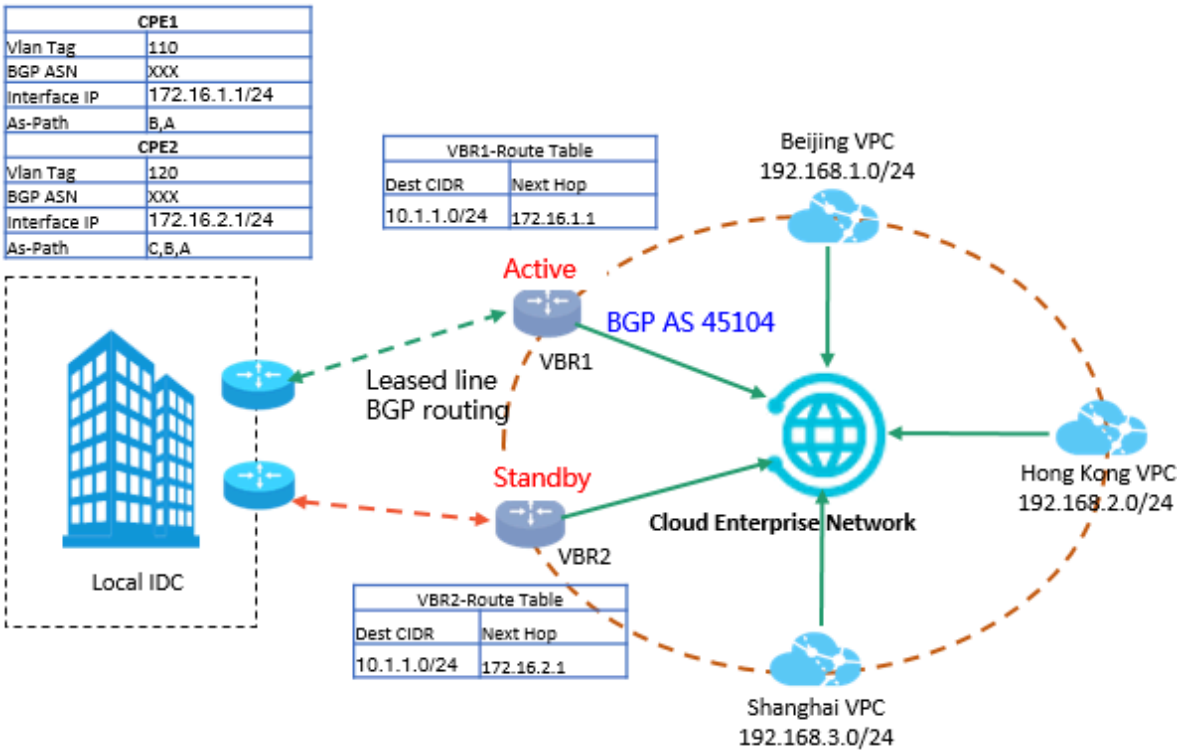

As shown in the preceding figure, the green line (CPE1) is the active link and the red line (CPE2) is the standby link. The BGP configurations of the two CPEs are as follows.

You can set the routing priority by configuring the AS-Path length. The shorter the As-Path length, the higher the priority.

| Configuration | CPE1 | CPE2 |
| --- | --- | --- |
| Vlan Tag | 110 | 120 |
| Network | 10.1.1.0/24 | 10.1.1.0/24 |
| BGP ASN | XXX | XXX |
| Interface IP | 172.16.100.0/24 | 172.16.2.1/24 |
| As-Path | B,A | C,B,A |

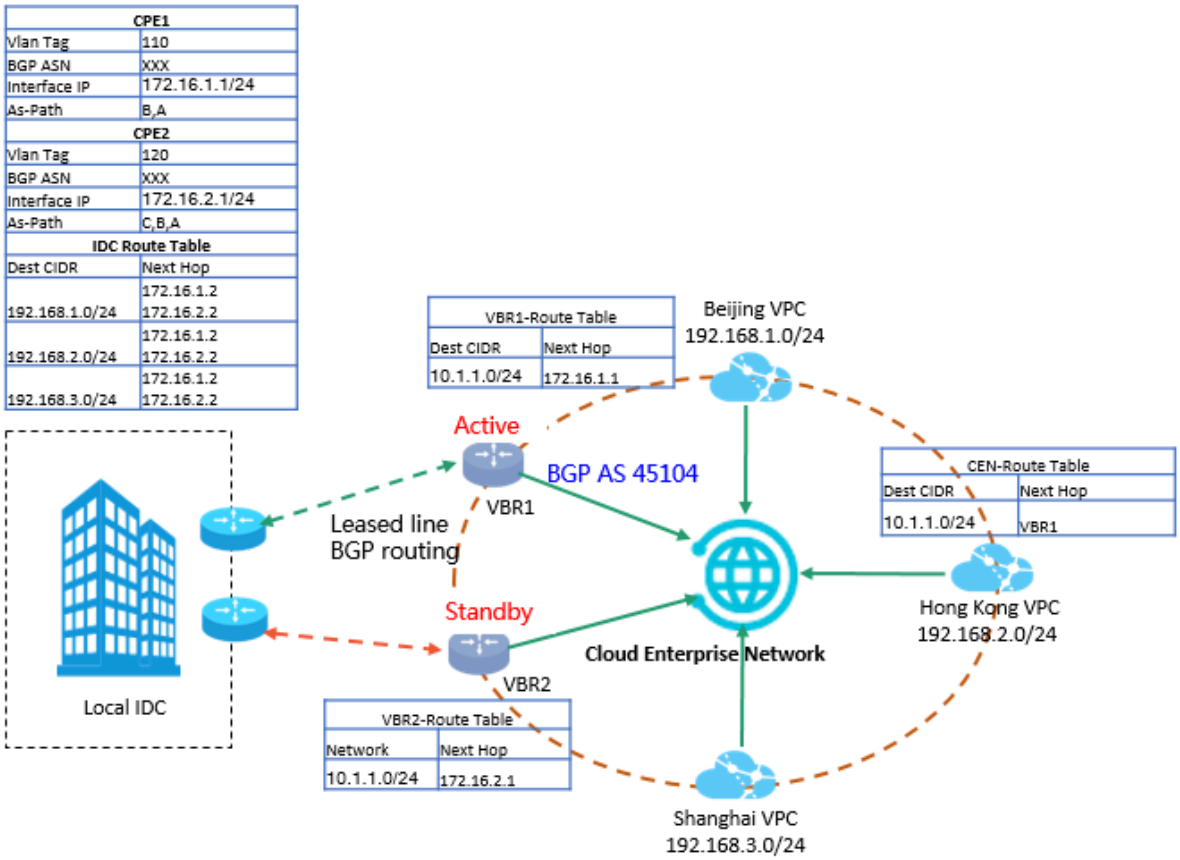
The CEN can automatically learn and distribute route entries. After routes are configured, the CEN synchronizes the routes to attached networks based on the routing weights.

- BGP routes in VBRs




As shown in the following figure, the route tables of VBR1 and VBR2 contain routes and next hops learned from the BGP peers of VBR1 and VBR2. The VBRs, which are attached to the CEN, send the BGP routes learned from the local data center to the CEN, including AS-Path configurations.

- All routes in the CEN




After the VPCs and VBRs are attached to CEN, the BGP routes learned from the VBRs are distributed to the CEN. The CEN then synchronizes the routes to all attached networks based on the routing weights.

The BGP routes that the VBRs learn from the local data center share the same destination CIDR block but have different routing weights. The physical connection connected to VBR1 acts as the active link (the AS-Path is shorter), and the one connected to VBR2 acts as the standby link. CEN will synchronize this routing configuration to other attached networks, such as VPCs. As shown in the route tables of the VPCs, all routes destined for 10.1.1.0/24 point to VBR1.

Additionally, CEN redistributes CEN system routes to the BGP network. Therefore , the BGP route table of the local data center includes the learned CEN routes and the next hops are the interface IPs of the two VBRs.

Similarly, if you want to configure active/standby links that connect the local data center to the Alibaba Cloud IP address (192.168. X. 0/24), you can do this by configuring the BGP AS-Path. Configure weights for the routes learned from different BGP peers (192.168. X. 0/24).

# 2 Connect an on-premises data center to Alibaba Cloud using two leased lines configured with static routes

This topic describes how to use leased lines and CEN to connect an on-premises data center to Alibaba Cloud and enable the data center to communicate with VPCs in different regions.

## Solution overview

To connect an on-premises data center to Alibaba Cloud, complete these steps:

1. Build redundant leased lines

   Create redundant leased lines to connect the on-premises data center to Alibaba Cloud. Configure static routes between the on-premises data center and the VBRs.
2. Configure health checks (required)

   Configure health checks. Therefore, the traffic can be automatically routed to the standby link when the active link fails. When configuring health checks, you can set any unused private IP address in a VPC attached to the CEN instance as the source IP address, and set the IP address of the CPE interface connected to the VBR as the destination IP address. For more information, see *Health check*.
3. Attach networks

   Attach the VBRs and VPCs to the created CEN instance.
4. Configure and publish routes

   Configure routes in the on-premises data center and VPCs. For more information, see *Static route configurations of the on-premises data center and VBRs*.

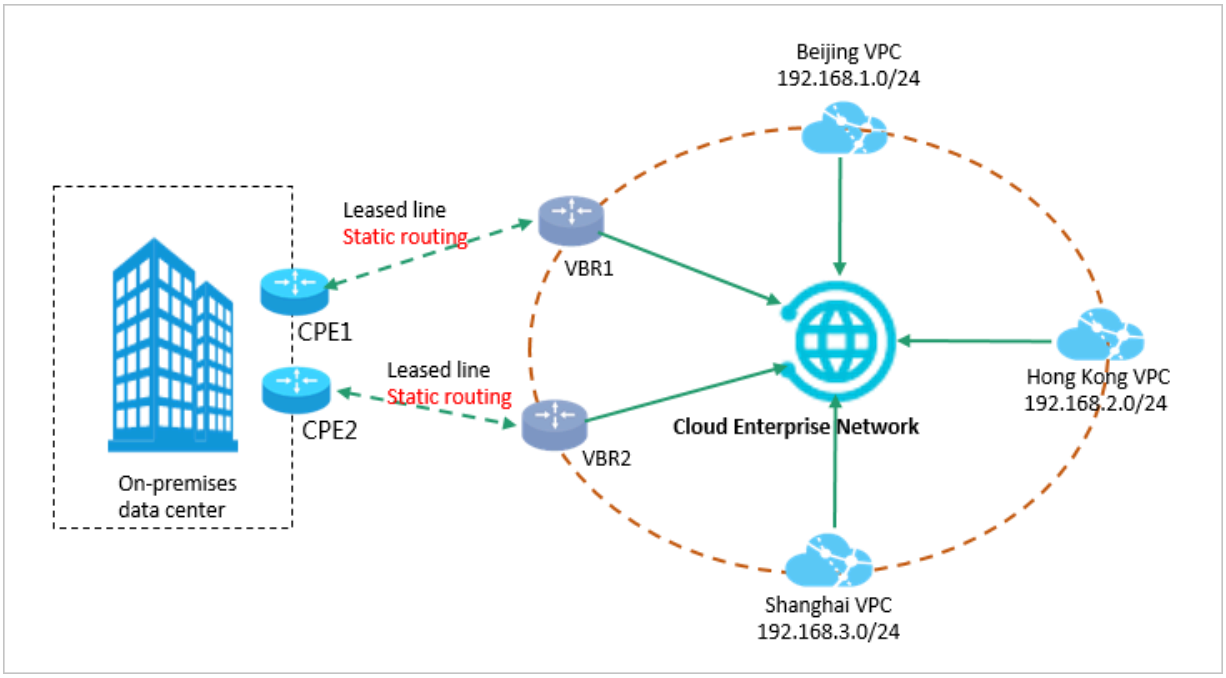
## Network topology

The network topology used in this topic is as follows:

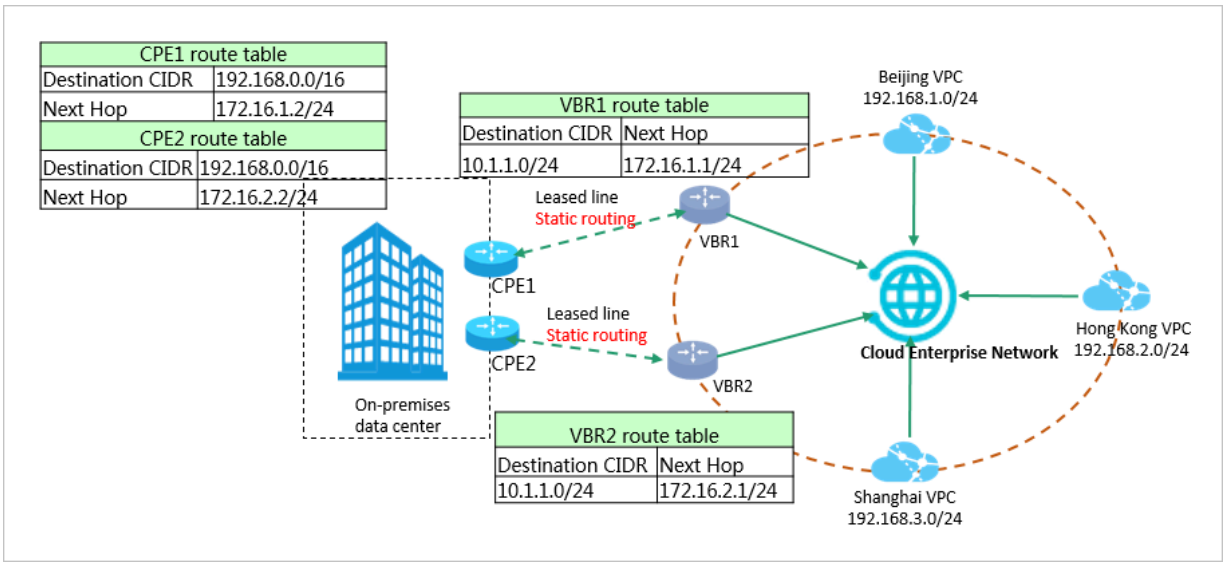
- The on-premises data center is already connected to the VBRs through two leased lines. Configure static routes between the on-premises data center and the VBRs.
- Three VPCs are already created in the China (Beijing), China (Shanghai), and China (Hong Kong) regions.

- The CIDR blocks of networks used in this topic are as follows:

| Network | CIDR block |
| --- | --- |
| On-premises data center | 10.1.1.0/24 |
| Beijing VPC | 192.168.1.0/24 |
| Hong Kong VPC | 192.168.2.0/24 |
| Shanghai VPC | 192.168.3.0/24 |




## Static route configurations of the on-premises data center and VBRs




The routing configurations in this topic are as follows:

- On-premises data center route configuration

  Configure a static route pointing to Alibaba Cloud on CPE1 and CPE2 respectively.

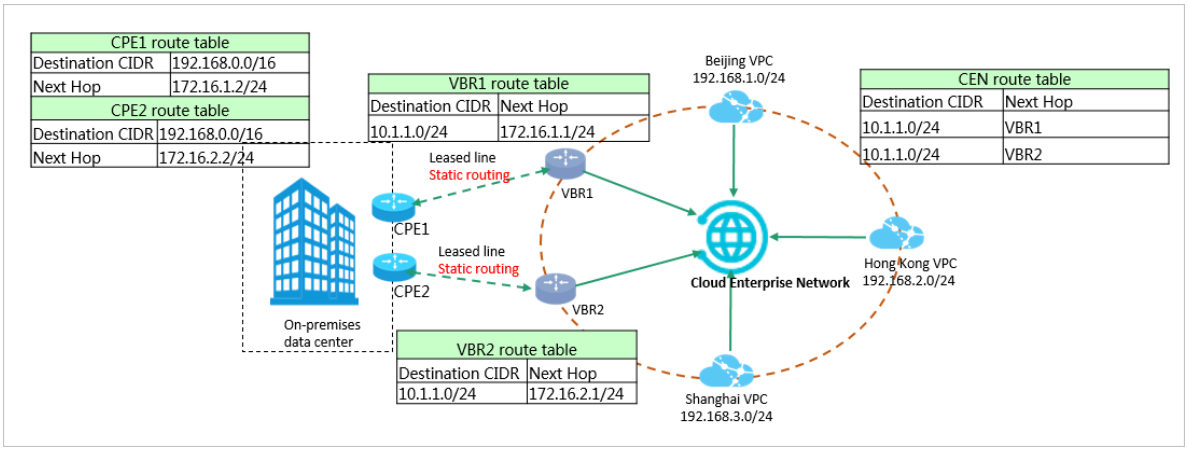
| Configuration | CPE1 | CPE2 |
| --- | --- | --- |
| Destination CIDR block | 192.168.0.0/16 | 192.168.0.0/16 |
| Next hop | 172.16.1.2/24 (VBR1) | 172.16.2.2/24 (VBR2) |

- VBR route configuration

  Configure a static route pointing to the on-premises data center on VBR1 and VBR2 respectively.

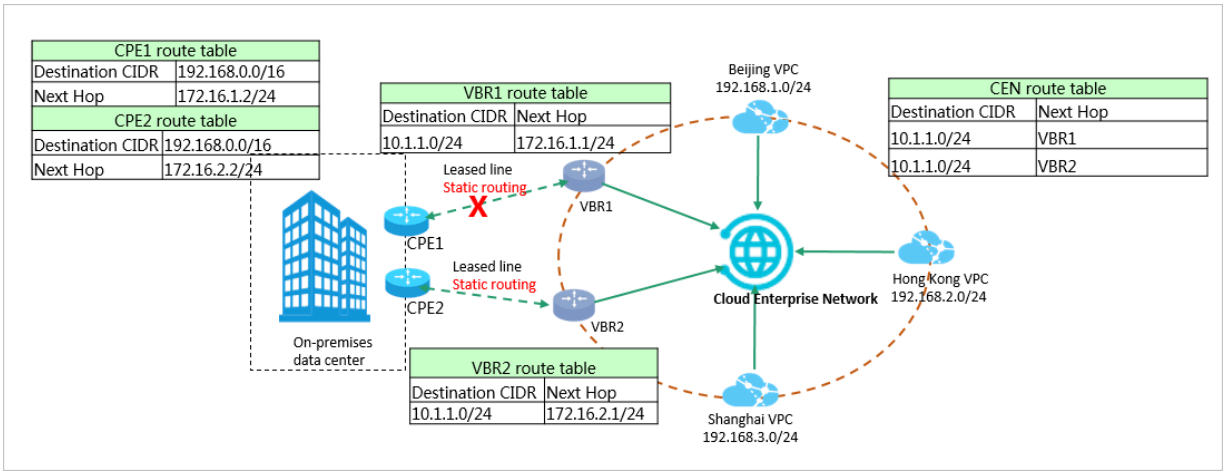
| Configuration | VBR1 | VBR2 |
| --- | --- | --- |
| Destination CIDR block | 10.1.1.0/24 | 10.1.1.0/24 |
| Next hop | 172.16.1.1/24 | 172.16.2.1/24 |

- CEN routes




After configuring routes for the VBRs, the CEN publishes the configured static routes to the CEN. In CEN, the two leased lines form ECMP and are in active-active status.

## Redundant disaster tolerance




When a leased line fails (such as the line from VBR1 to CPE1), data from Alibaba Cloud to the on-premises data center is forwarded to VBR2. This solution achieves disaster tolerance by automatically switching the link.

# 3 Connect a local data center to Alibaba Cloud through a VPN Gateway

This tutorial introduces how to use VPN Gateway and CEN to connect an IDC to Alibaba Cloud and enable the IDC to communicate with VPCs in different regions.

## Solution overview

To connect an IDC to Alibaba Cloud, complete these steps:

1. Configure a VPN Gateway

   Create an IPsec-VPN connection to connect the local IDC to the Alibaba Cloud. For more information, see *Establish a connection between a VPC and an on-premises data center*.

2. Attach networks

   Attach the VBR and VPCs to communicate with one another to the created CEN instance.

3. Configure and publish routes

   You can publish the route entry pointing to the VPN Gateway in the VPC to the CEN , so that other networks attached to the CEN instance can learn the route.

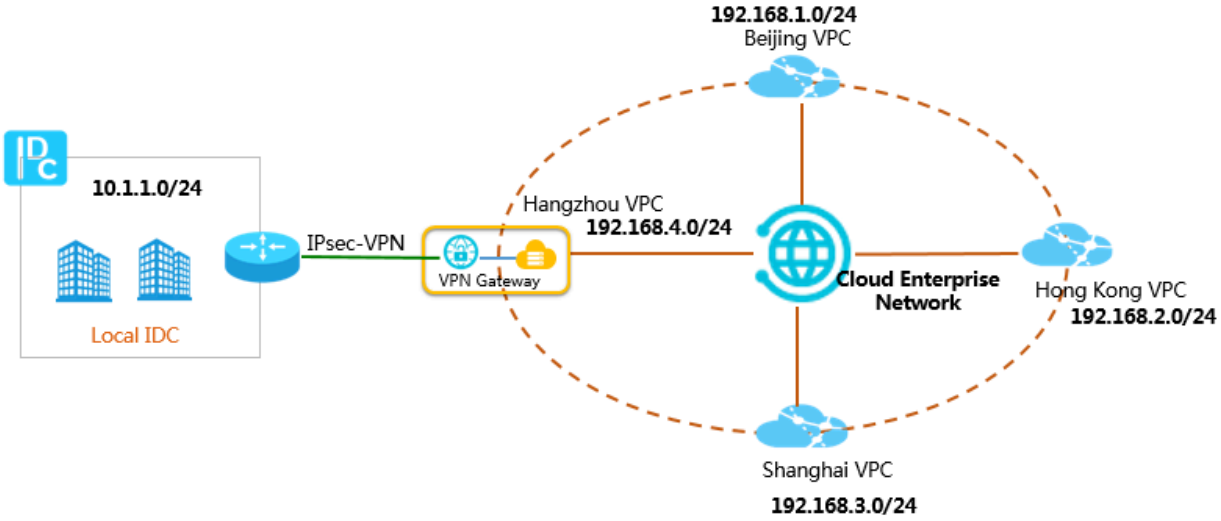
## Network topology

The network topology used in this tutorial is as follows:

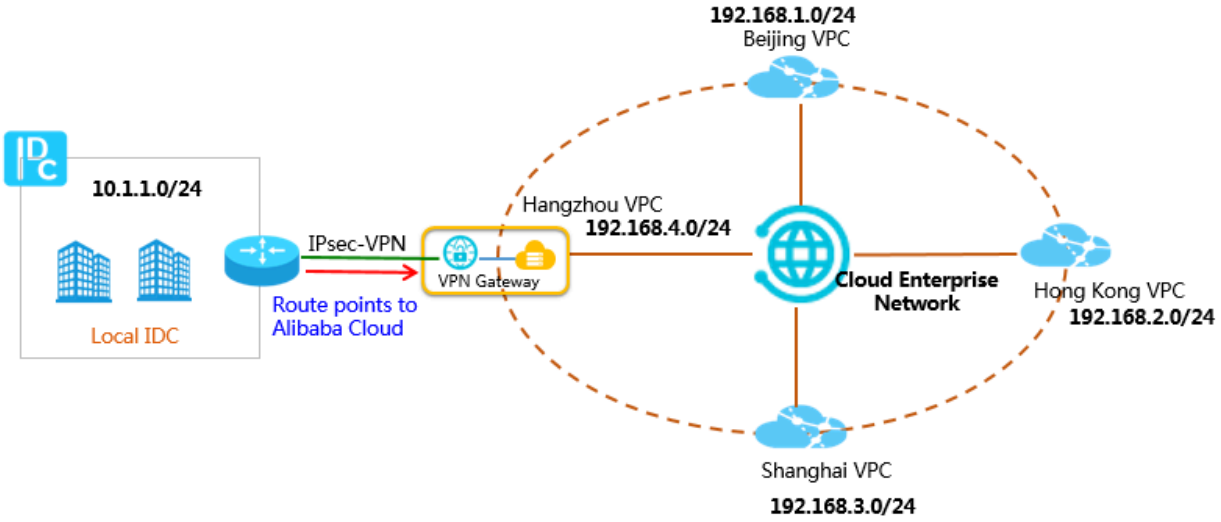
- The local IDC is connected to Alibaba Cloud through the VPN Gateway.
- Four VPCs are already created in the China (Hangzhou), China (Beijing), China ( Shanghai), and China (Hong Kong) regions.
- The CIDR blocks of networks in this tutorial are as follows. Make sure that the CIDR blocks do not conflict with one another.

| Network | CIDR block |
| --- | --- |
| Local data center | 10.1.1.0/24 |
| Beijing VPC | 192.168.1.0/24 |
| Hong Kong VPC | 192.168.2.0/24 |
| Shanghai VPC | 192.168.3.0/24 |

| Network | CIDR block |
| --- | --- |
| Hangzhou VPC | 192.168.4.0/24 |




IDC route configuration




An IPsec-VPN connection has been established between the IDC and the VPN Gateway , and custom or system route entries pointing to the Alibaba Cloud have been configured.

Table 3-1: Customer route entries in the local IDC

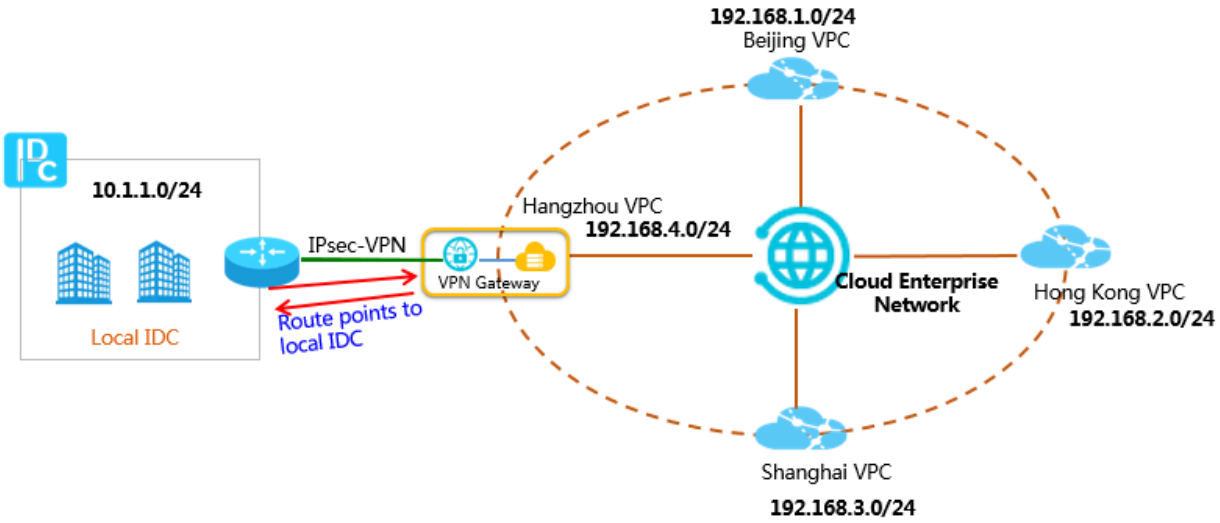
| Destination CIDR block | Next hop |
| --- | --- |
| 192.168.1.0/24 | VPN Gateway |
| 192.168.2.0/24 | VPN Gateway |
| 192.168.3.0/24 | VPN Gateway |

| Destination CIDR block | Next hop |
| --- | --- |
| 192.168.4.0/24 | VPN Gateway |

Table 3-2: Default route entry in the local IDC

| Destination CIDR block | Next hop |
| --- | --- |
| 0.5.0.0/0 | VPN Gateway |

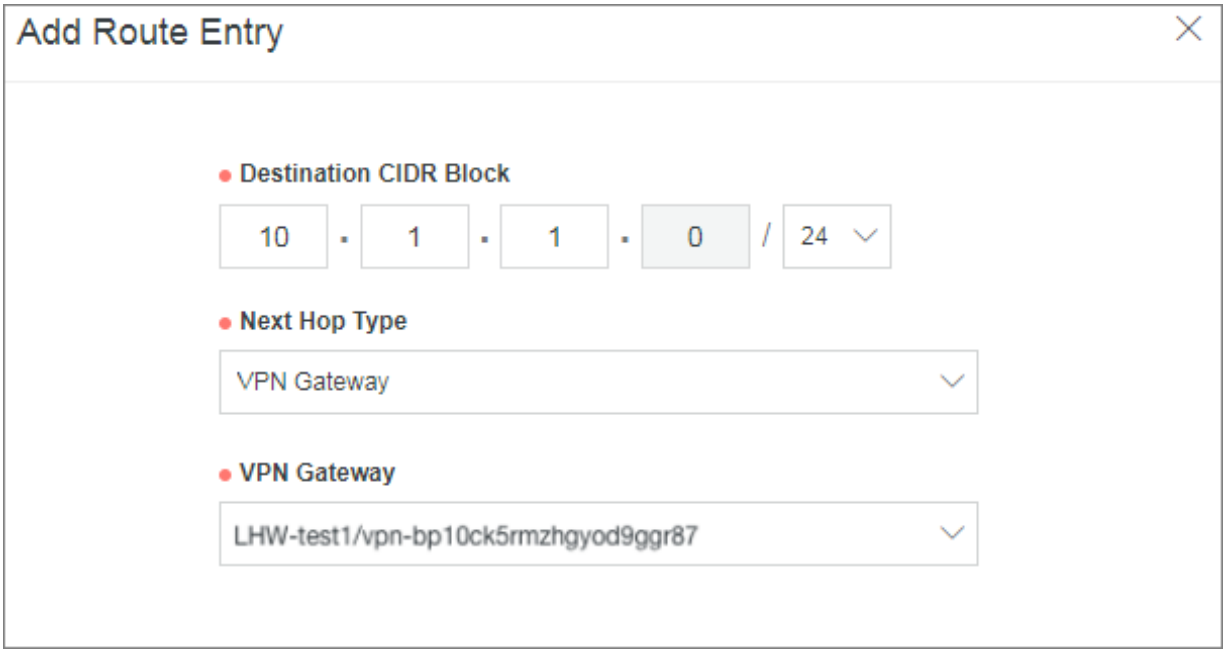
VPC route configuration



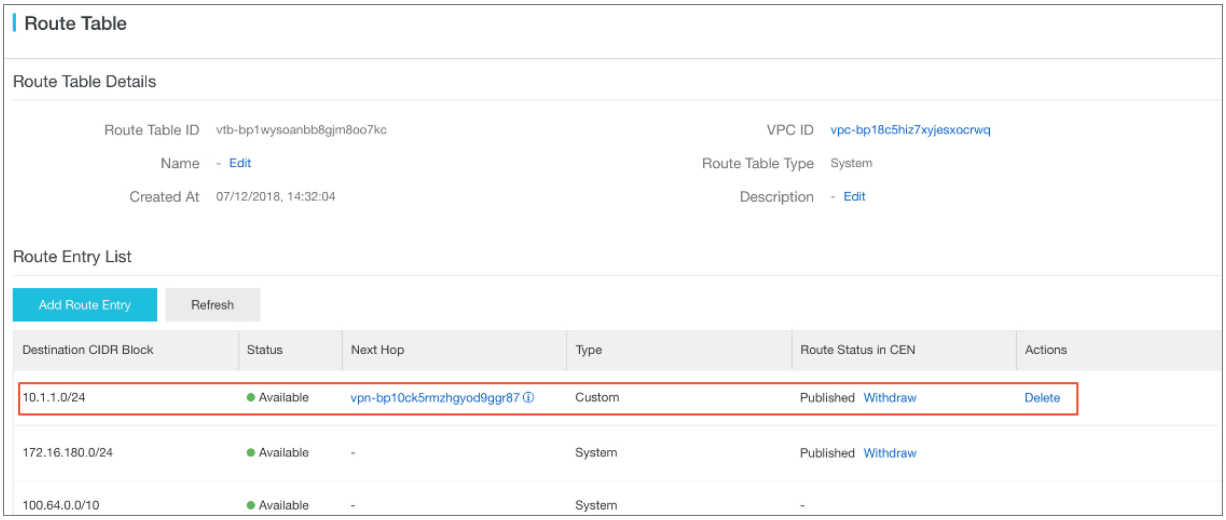

To enable the communication between the IDC and the VPCs, you need to configure a route entry pointing to the IDC (VPN Gateway) in the VPC connected to the VPN Gateway and publish the route to the CEN.

A route entry pointing to Alibaba Cloud is already created in the IDC, so traffic from the IDC can be forwarded to Alibaba Cloud. To forward traffic from the Hangzhou VPC to the IDC, configure a route entry pointing to the VPN Gateway in the Hangzhou VPC.

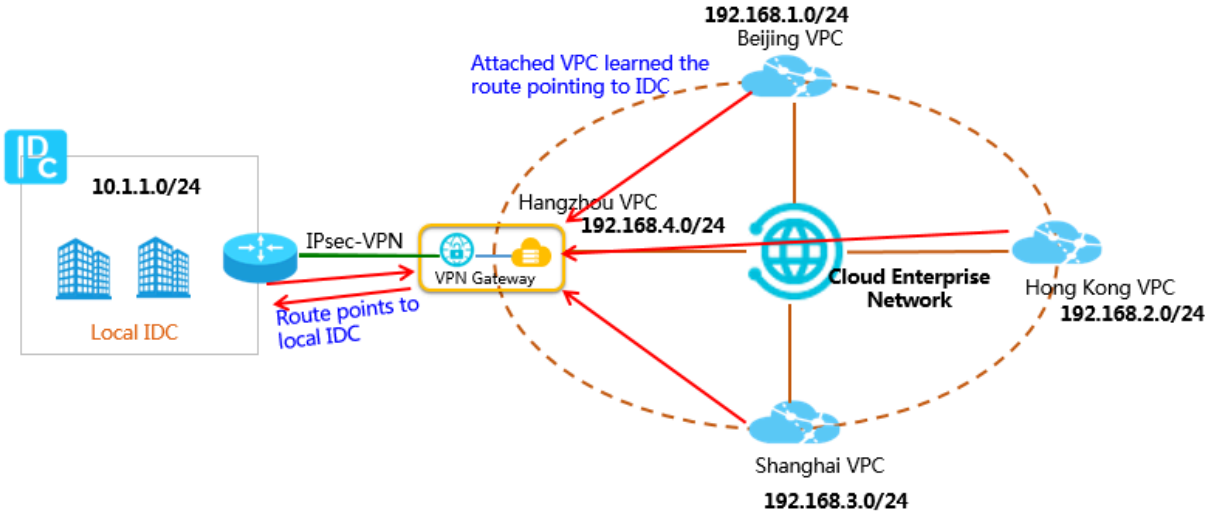
As shown in the following figure, you need to configure a custom route entry pointing to the VPN Gateway (IDC) in the Hangzhou VPC:




**You can see the route entry pointing to the VPN Gateway in the route table of the Hangzhou VPC:**

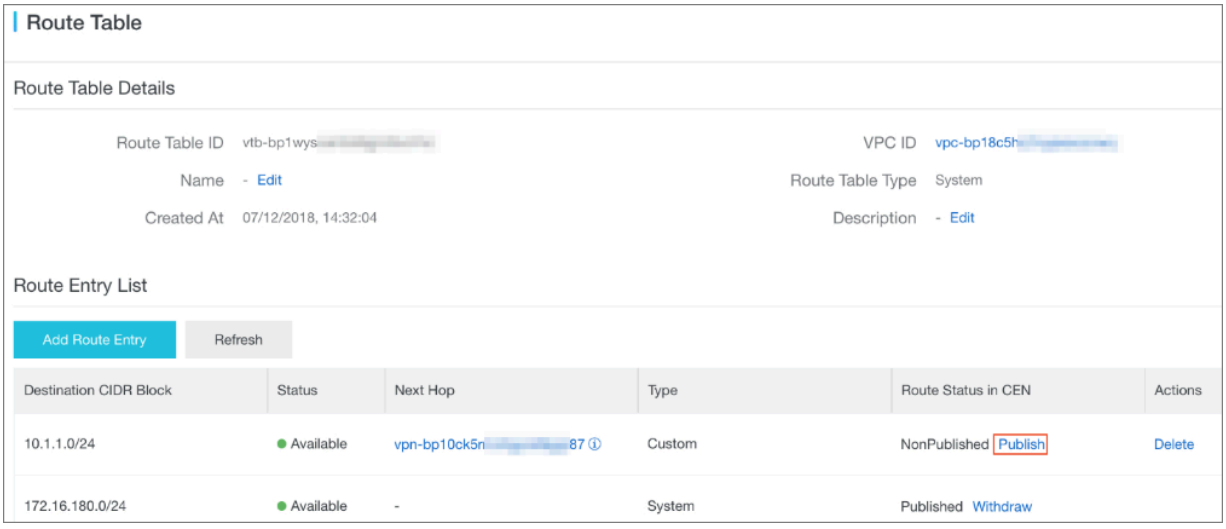


## Publish the route entry to CEN

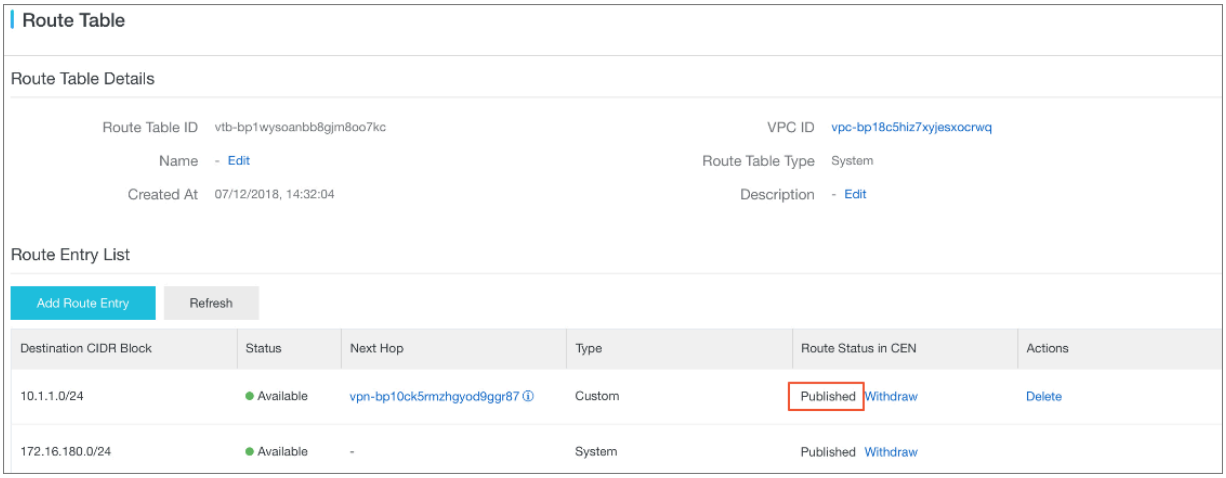



To mark other VPCs attached to the CEN instance learn the route pointing to the IDC, you need to publish the route entry pointing to the VPN Gateway to the CEN instance so that other attached VPCs can learn the route.

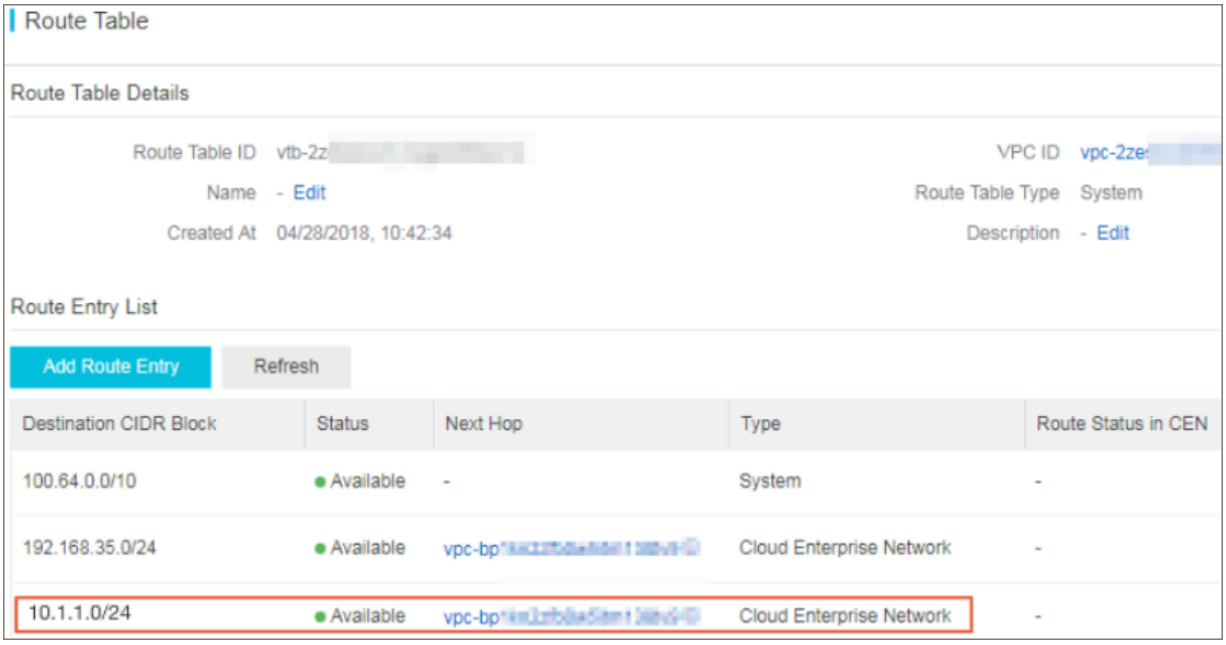
The following figure shows the route table before the route entry is published.




The following figure shows the route table after the route entry is published.




The following figure shows the route table of other VPCs attached to the CEN.




After the previous operations, other VPCs attached to the CEN instance have learned the route entry pointing to the IDC. Therefore, the IDC can communicate with any VPC attached to the CEN instance.

### CEN route publishing

This solution describes one of the scenarios where a network attached to a CEN instance publishes a route entry to or withdraw a route entry from the instance. For VPCs/VBRs attached to a CEN instance, the following operations are supported:

| Route type | Network | Publish to CEN by default |
| --- | --- | --- |
| A route entry pointing to an ECS instance | VPC | No |

| Route type | Network | Publish to CEN by default |
| --- | --- | --- |
| A route entry pointing to a VPN Gateway | VPC | No |
| A route entry pointing to a HaVip | VPC | No |
| A VPC system route entry | VPC | Yes |
| A route entry pointing to a local IDC | VBR | Yes |
| A BGP route entry | VBR | Yes |

All these route entries published to CEN can be withdrawn. After a route entry is withdrawn, the route entry no longer exists in CEN.

If a custom route entry is published to a CEN and then is deleted from the VPC to which it belongs, the route entry is also deleted from the CEN.

Note:

Currently, the console only supports publishing and withdrawing VPC route entries and does not support publishing and withdrawing VBR route entries. You can publish and withdraw VBR route entries by calling the Open API *PublishRouteEntries*.

# 4 Connect a local data center to Alibaba Cloud using active/standby links formed by a leased line and a Smart Access Gateway

This topic introduces how to use CEN, a leased line and a Smart Access Gateway to connect a local IDC to Alibaba Cloud and enable the local IDC to communicate with VPCs in different regions through active/standby links formed by a leased line and a Smart Access Gateway.

You can connect a local IDC to Alibaba Cloud through active/standby redundant links formed by a leased line and a Smart Access Gateway. The leased line is connected to the VBR through BGP protocol and acts as the active link. The Smart Access Gateway is connected to the CEN through CCN and acts as the standby link. When the leased line fails, the traffic is automatically distributed to the link of the Smart Access Gateway to achieve high availability.

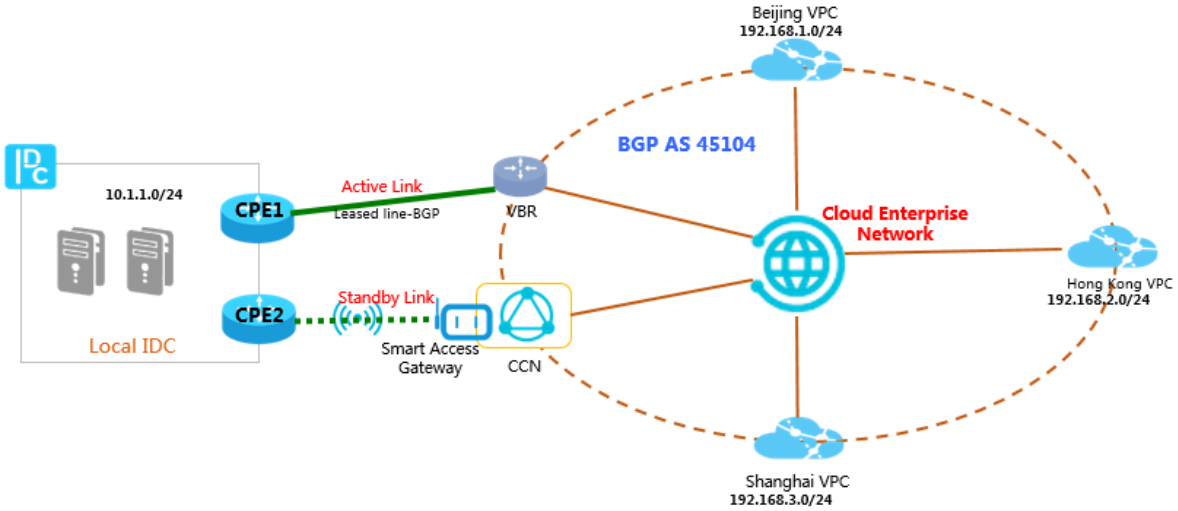
## Network topology

The network topology is as follows:

- The local IDC is connected to Alibaba Cloud through redundant links formed by the leased line and the Smart Access Gateway. The leased line uses BGP protocol.
- Cloud services are deployed in Beijing, Hong Kong, and Shanghai respectively.
- Ensure that the CIDR blocks of VPCs in different regions do not conflict with the CIDR block of the local IDC. The CIDR blocks of the VPCs and local IDC in this topic are as follows:

| Network | CIDR block |
| --- | --- |
| Beijing VPC | 192.168.1.0/24 |
| Hong Kong VPC | 192.168.2.0/24 |
| Shanghai VPC | 192.168.3.0/24 |
| Local IDC | 10.1.1.0/24 |

- The Smart Access Gateway and the VBR connected to the leased line are attached to the CEN.




## Overview

### Route priority within the CEN

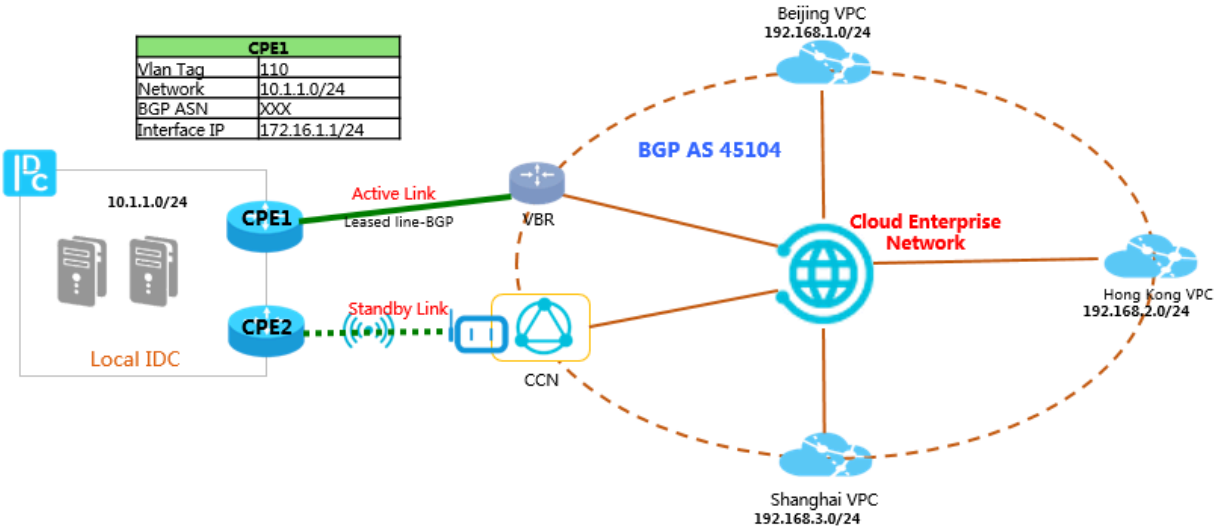
When a leased line and a Smart Access Gateway destined to the same CIDR block are connected to a CEN, the route priority within the CEN is: the leased line takes precedence over Smart Access Gateway.

1. The leased line advertises a BGP route

Assume that the local IDC and the VBR are each other's BGP peer.

Now you need to configure the BGP CIDR block 10.1.1.0/24 advertised to Alibaba Cloud in the local IDC. The CPE1 configurations of the local IDC are as follows.

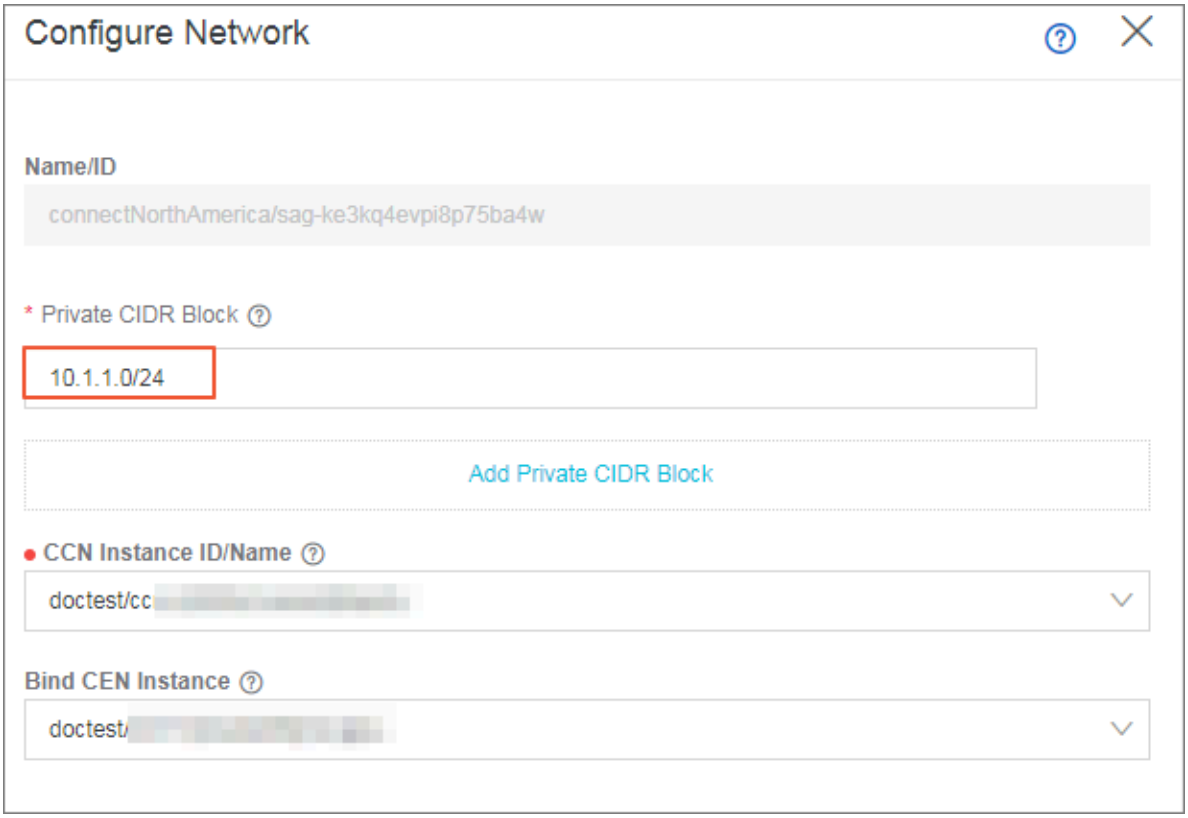
| Configuration | Value |
| --- | --- |
| Vlan Tag | 110 |
| Network | 10.1.1.0/24 |
| BGP ASN | xxx |
| Interface IP | 172.16.1.1/24 |




2. Configure the Smart Access Gateway

1. On the Smart Access Gateway console, select the leased line that forms the active /standby links with the Smart Access Gateway (The leased line always acts as the active link).
2. On the Smart Access Gateway console, configure the CIDR block of the local IDC.

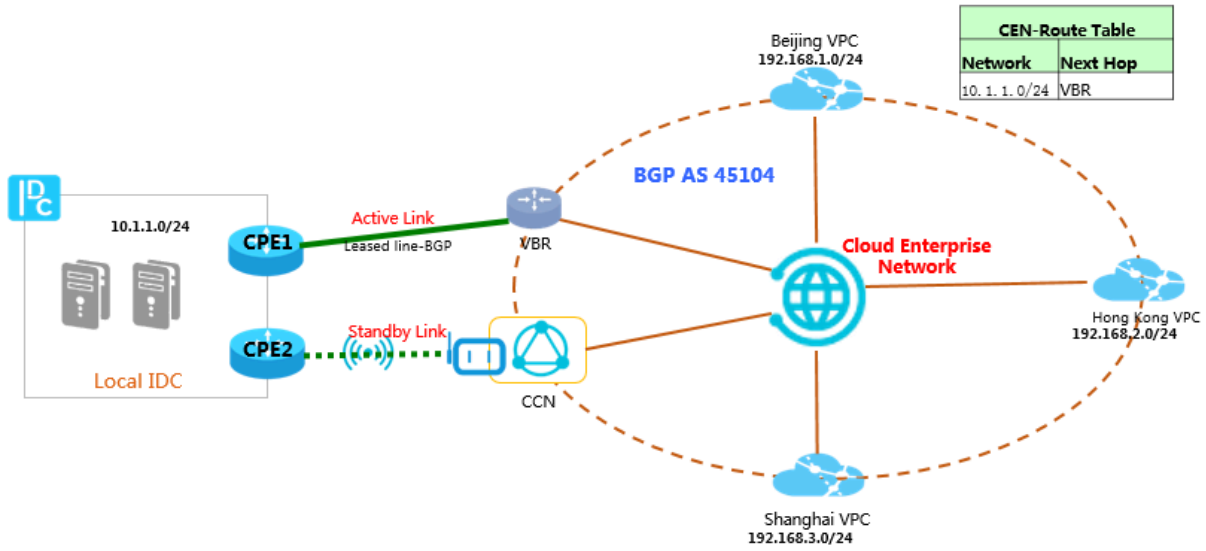
   The Smart Access Gateway has been attached to the CEN. You need to configure the CIDR block 10.1.1.0/24 of the local IDC in the Smart Access Gateway.



**Note:**

**You must follow the preceding order when you configure the active/standby links. You must configure the active/standby links first and configure the local IDC CIDR block in the Smart Access Gateway second. If you configure the local IDC CIDR block in the Smart Access Gateway first, the CIDR block cannot be added because the Smart Access Gateway has been attached to the CEN and address conflict occurs.**

3. Routes in CEN




**In this topic, the leased line advertises the CIDR block 10.1.1.0/24 to CEN through BGP and the CIDR block 10.1.1.0/24 is also configured in Smart Access Gateway. Because both the VBR and the CCN are attached to the CEN, the CIDR block 10.1.1.0/24 is also synchronized to the CEN. For a leased line and a Smart Access Gateway destined to the same CIDR block, CEN adopts the following priority: the leased line takes precedence over Smart Access Gateway. Therefore, the next hop of routes destined for 10.1.1.0/24 in other networks attached to the CEN is the VBR. When the leased line fails, the standby line takes effect and traffic from Alibaba Cloud to IDC will be distributed to the Smart Access Gateway.**

# 5 Build an enterprise-level hybrid cloud in multiple ways

As a basic network platform, CEN can be used together with multiple services (such as Express Connect, VPN Gateway, and Smart Access Gateway) to provide rich hybrid cloud solutions.

## Overview

CEN is devoted to providing a high-quality network transmission environment. By simplifying your networking process, it helps you rapidly build a hybrid cloud network with enterprise-level scale and communication capability. This solution describes how to rapidly build a hybrid cloud network by using CEN together with physical connections of Express Connect, VPN Gateway, and Smart Access Gateway.

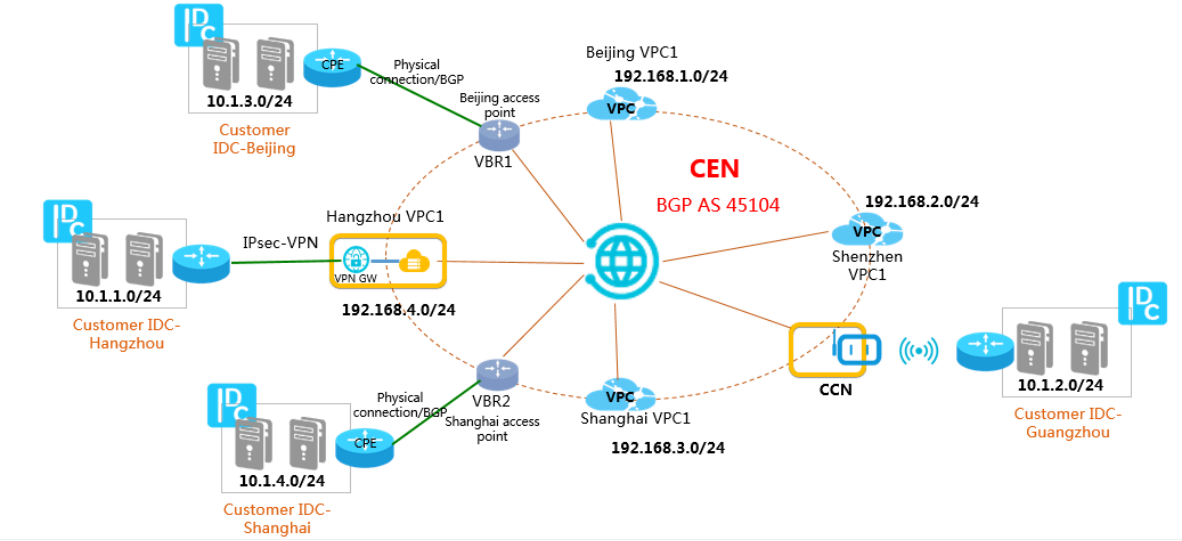
## Network topology

This tutorial takes the following network topology as an example:

- *The Beijing IDC and the Shanghai IDC access Alibaba Cloud through physical connections*
- *The Hangzhou IDC accesses Alibaba Cloud through VPN Gateway*
- *The Guangzhou IDC accesses Alibaba Cloud through Smart Access Gateway*

- A company has deployed local data centers in Beijing, Shanghai, Hangzhou, and Guangzhou.
- The company has also deployed services on the cloud. It has created separate VPCs in Beijing, Shanghai, Hangzhou, and Shenzhen.
- The Beijing IDC and the Shanghai IDC are connected to access points of Alibaba Cloud through physical connections and their corresponding VBRs are attached to the CEN.
- The Hangzhou IDC is connected to the Hangzhou VPC through VPN Gateway.
- The Guangzhou IDC accesses Alibaba Cloud through Smart Access Gateway and the CCN to which the Smart Access Gateway belongs is attached to the CEN.

- The VPCs in Beijing, Shanghai, Shenzhen, and Hangzhou are attached to the CEN.




## IP address planning

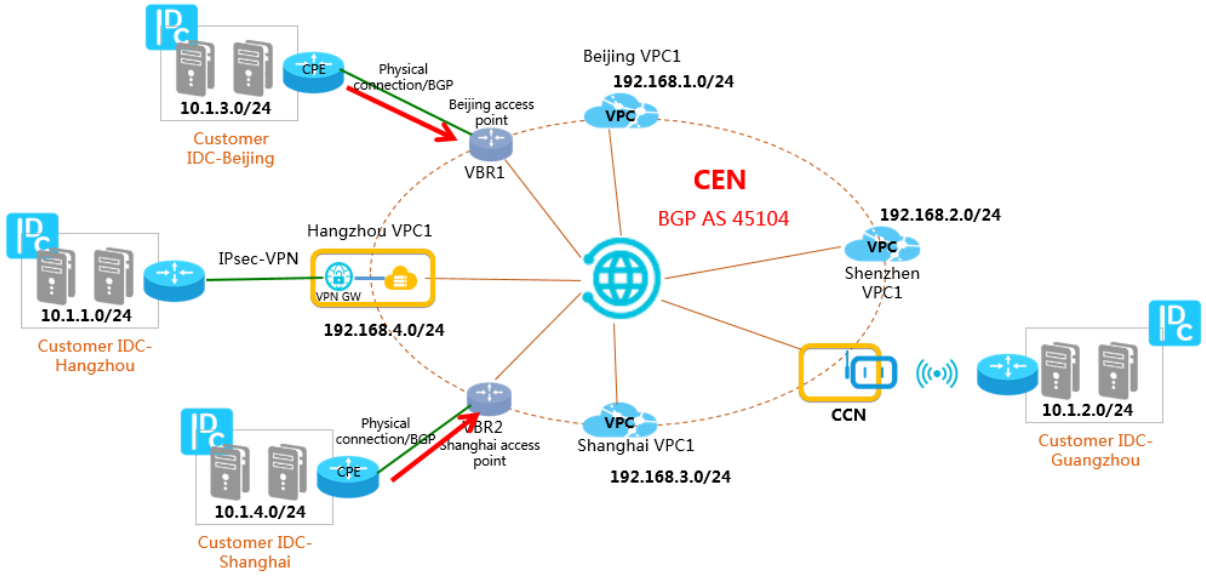
When you build a hybrid cloud, you must ensure that all CIDR blocks do not conflict with one another. The CIDR blocks in this tutorial are as follows:

| Network | CIDR block |
| --- | --- |
| Hangzhou IDC | 10.1.1.0/24 |
| Guangzhou IDC | 10.1.2.0/24 |
| Beijing IDC | 10.1.3.0/24 |
| Shanghai IDC | 10.1.4.0/24 |
| Beijing VPC | 192.168.1.0/24 |
| Shenzhen VPC | 192.168.2.0/24 |
| Shanghai VPC | 192.168.3.0/24 |
| Hangzhou VPC | 192.168.4.0/24 |

## Access mode

In this tutorial, IDCs access Alibaba Cloud through the following ways:

The Beijing IDC and the Shanghai IDC access Alibaba Cloud through physical connections



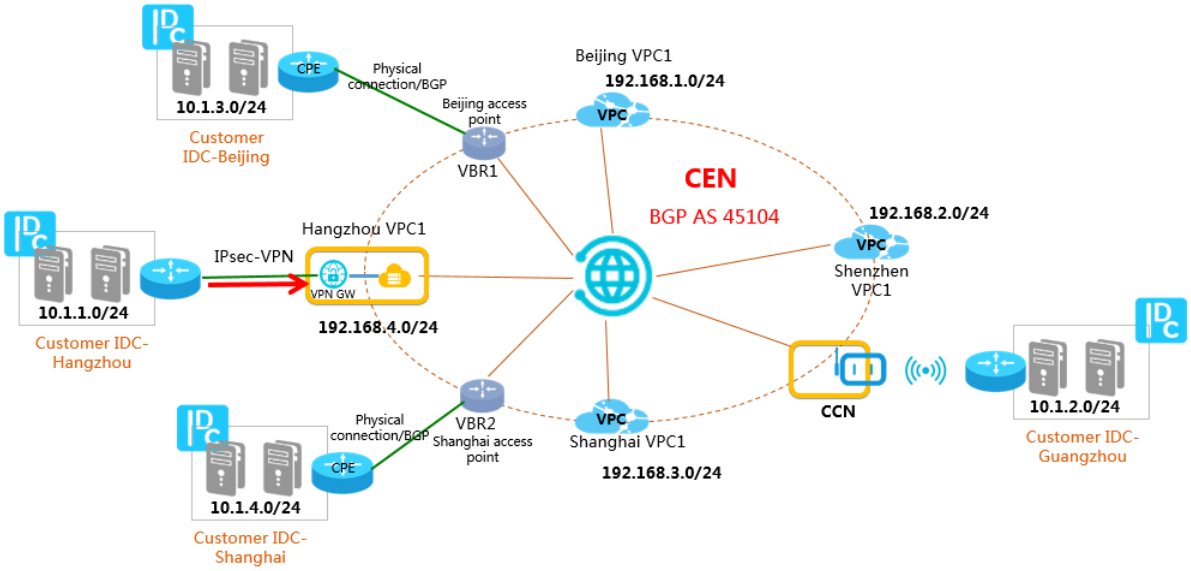

Configuration description:

1. The Beijing IDC and the Shanghai IDC are connected to VBRs through physical connections, and each IDC and the corresponding VBR are each other's BGP peer. For more information, see*Configure BGP*.
2. The CPEs of the Beijing IDC and the Shanghai IDC advertise the CIDR blocks of the IDCs to the CEN through BGP. The main configurations of the CPEs are as follows:

| Configuration | Beijing CPE | Shanghai CPE |
| --- | --- | --- |
| Local BGP ASN | A | B |
| Peer BGP ASN | 45104 | 45104 |
| Network | 10.1.3.0/24 | 10.1.4.0/24 |

After each IDC and the corresponding VBR become each other's peer, the IDC and the VBR can learn each other's routes.

The Hangzhou IDC accesses Alibaba Cloud through VPN Gateway




Configuration description:

1. The Hangzhou IDC accesses the Hangzhou VPC through VPN Gateway. For more information, see*Establish a connection between a VPC and an on-premises data center*.
2. An IPsec-VPN connection has been established between the IDC and the VPN Gateway, and contributing routes or default routes pointing to the cloud have been configured.

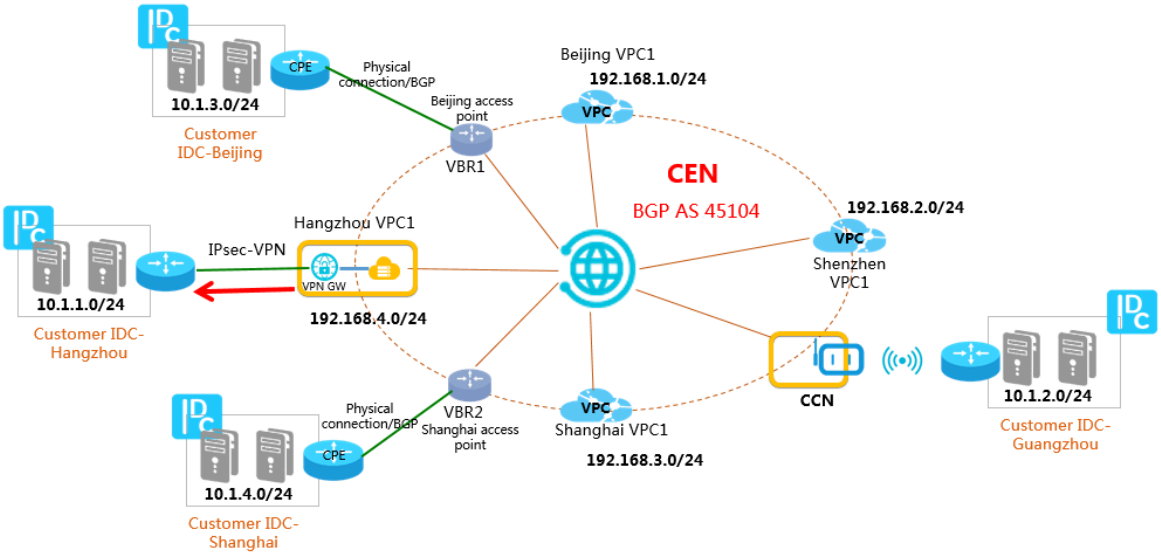
   Contributing routes:

| Destination CIDR block | Next hop |
| --- | --- |
| 10.1.2.0/24 | VPN Gateway |
| 10.1.3.0/24 | VPN Gateway |
| 10.1.4.0/24 | VPN Gateway |
| 192.168.1.0/24 | VPN Gateway |
| 192.168.2.0/24 | VPN Gateway |
| 192.168.3.0/24 | VPN Gateway |
| 192.168.4.0/24 | VPN Gateway |

   Default route:

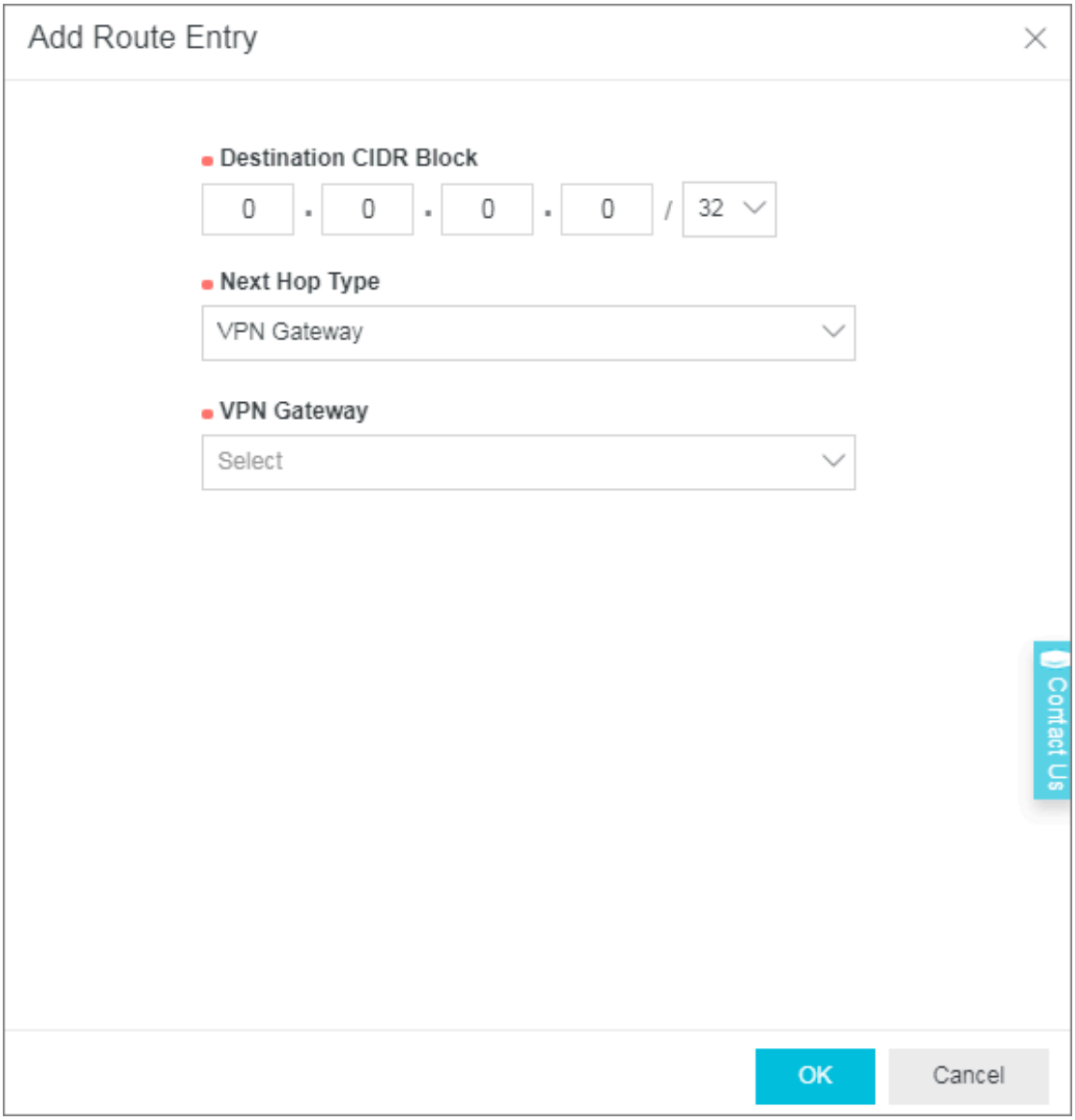
| Destination CIDR block | Next hop |
| --- | --- |
| 0.0.0.0/0 | VPN Gateway |

3. To enable the communication between the IDC and networks attached to the CEN, you must configure a route entry pointing to the IDC (VPN Gateway) in the VPC connected to the VPN Gateway and publish the route to the CEN.

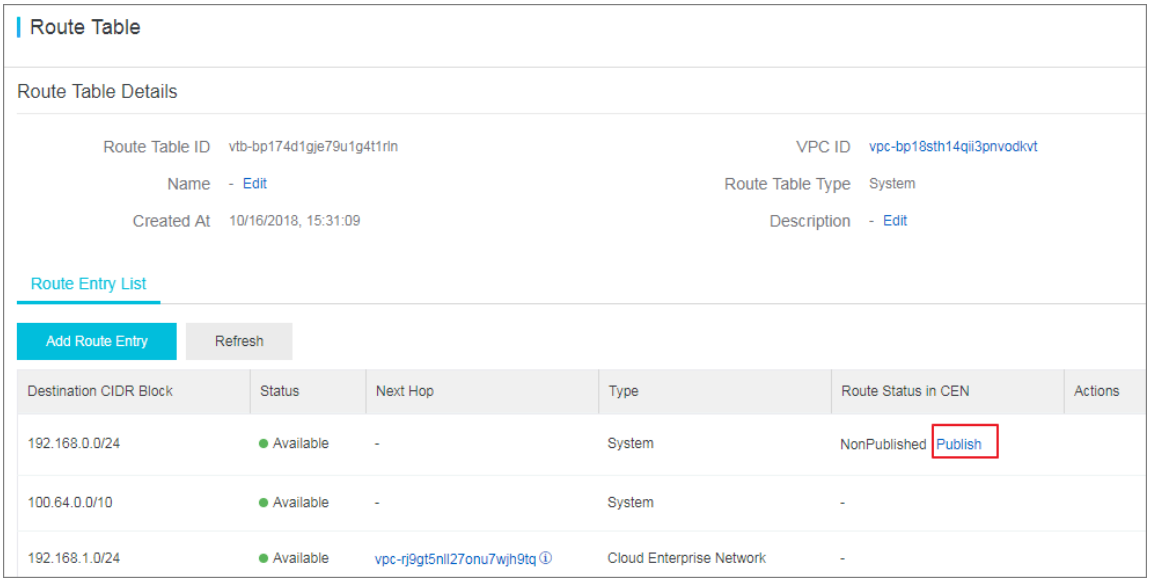



To configure the route, follow these steps:

a. Configure a route of which the destination CIDR block is 10.1.1.0/24 and the next hop is the VPN Gateway in the route table of the VPC.

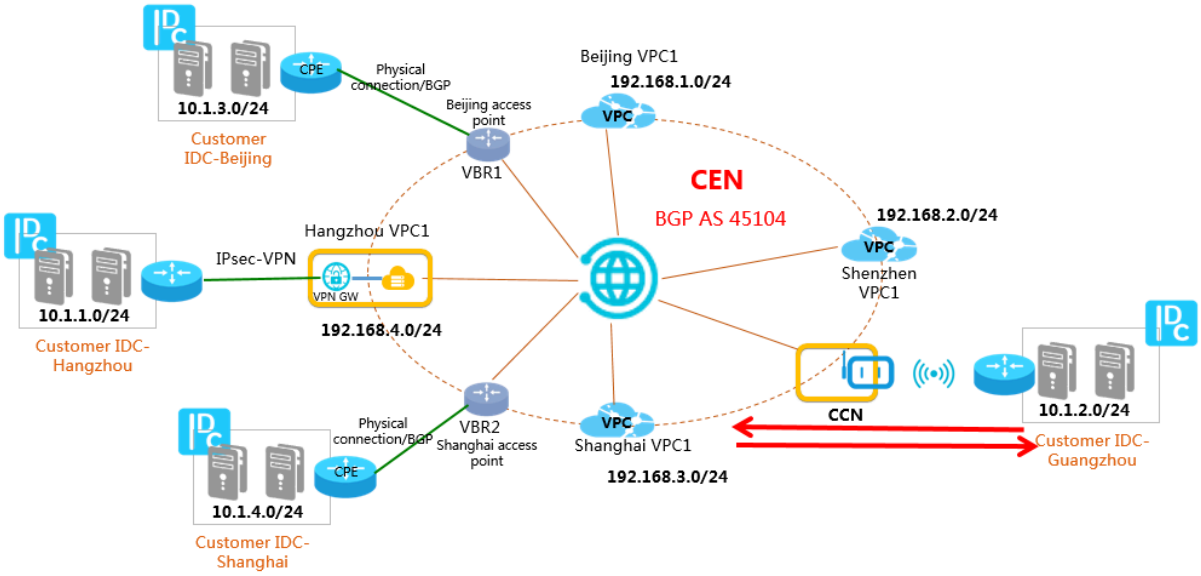



**b. Publish the route to the CEN in the Hangzhou VPC.**



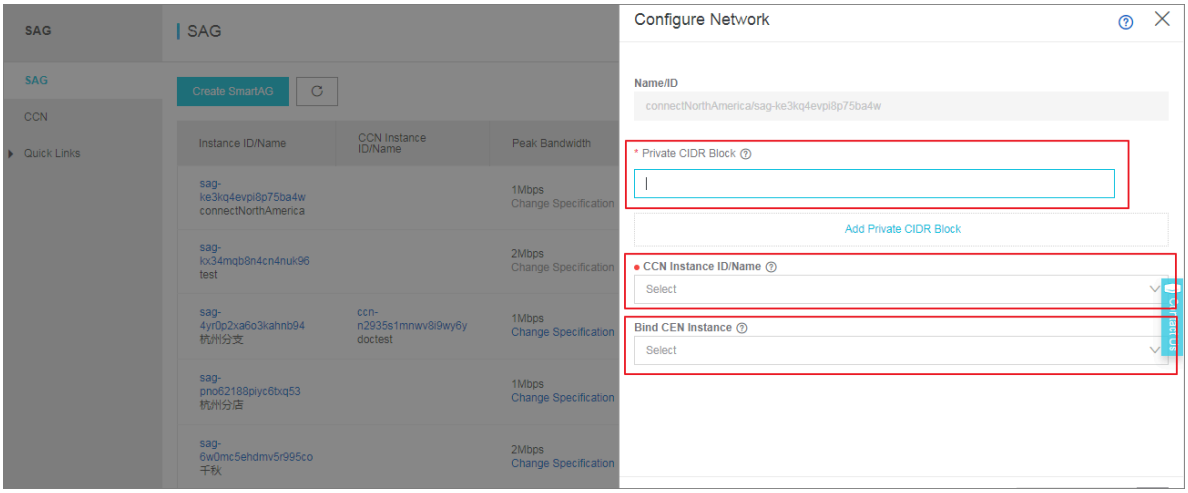
Through the preceding steps, all networks in the CEN can learn the route pointing to the IDC and the IDC can communicate any network in the CEN. For more information, see *Connect a local data center to Alibaba Cloud through a VPN Gateway*.

The Guangzhou IDC accesses Alibaba Cloud through Smart Access Gateway




Configuration description:

1. On the Smart Access Gateway console, configure the CIDR block of the Guangzhou IDC connected to Smart Access Gateway as a private CIDR block.
2. Attach the CCN bound to the Smart Access Gateway to the CEN. Then the Guangzhou IDC can communicate with any network in the CEN.

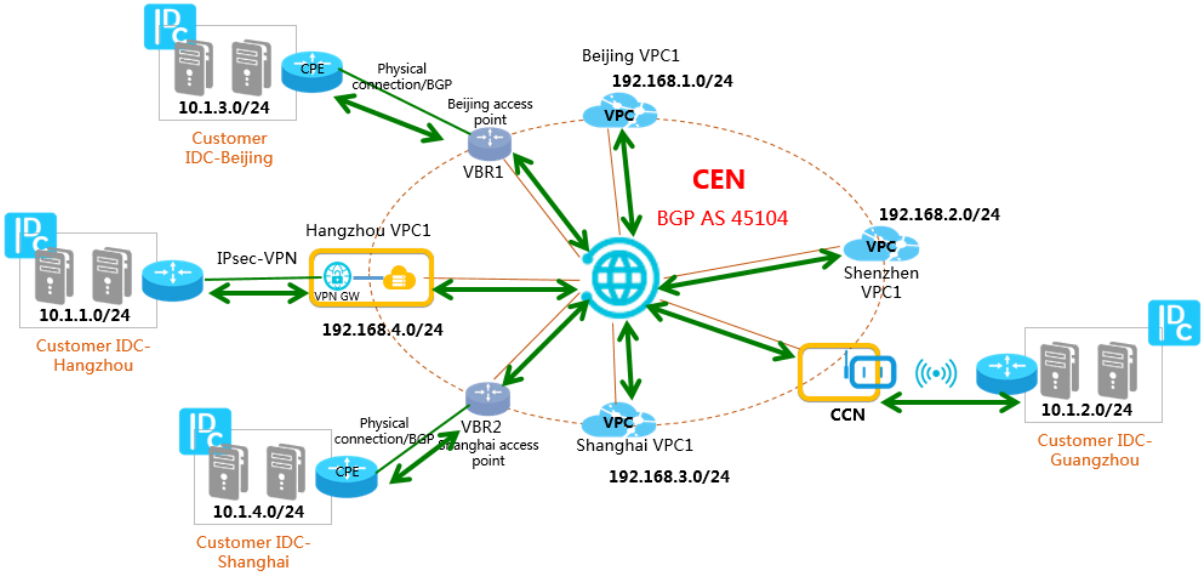



## Interconnection

Through the preceding ways:

- The Beijing IDC and Shanghai IDC access Alibaba Cloud through physical connections and use BGP protocol, and the VBRs of the physical connections are attached to the CEN.
- The Hangzhou IDC accesses Alibaba Cloud through VPN Gateway and the VPC connected to the VPN Gateway is attached to the CEN.
- The Guangzhou IDC accesses Alibaba Cloud through Smart Access Gateway and the CCN associated with the Smart Access Gateway is attached to the CEN.

CEN ignores conflict routes and dynamically forwards routes of attached networks to build a fully connected hybrid cloud.




Take Beijing CPE, Beijing VBR, and Shenzhen VPC as examples and view their route tables.

Table 5-1: Beijing CPE

| Destination CIDR block | Next hop | Route type |
| --- | --- | --- |
| 10.1.1.0/24 | BGP peer (Beijing VBR) | BGP route |
| 10.1.2.0/24 | BGP peer (Beijing VBR) | BGP route |
| 10.1.4.0/24 | BGP peer (Beijing VBR) | BGP route |
| 192.168.1.0/24 | BGP peer (Beijing VBR) | BGP route |
| 192.168.2.0/24 | BGP peer (Beijing VBR) | BGP route |
| 192.168.3.0/24 | BGP peer (Beijing VBR) | BGP route |
| 192.168.4.0/24 | BGP peer (Beijing VBR) | BGP route |

Table 5-2: Beijing VBR

| Destination CIDR Block | Next hop | Route type |
| --- | --- | --- |
| 10.1.3.0/24 | BGP peer (Beijing CPE) | BGP route |
| 10.1.1.0/24 | Hangzhou VPC | CEN route |
| 10.1.2.0/24 | CCN | CEN route |
| 10.1.4.0/24 | Shanghai VPC | CEN route |
| 192.168.1.0/24 | Beijing VPC | CEN route |
| 192.168.2.0/24 | Shenzhen VPC | CEN route |
| 192.168.3.0/24 | Shanghai VPC | CEN route |
| 192.168.4.0/24 | Hangzhou VPC | CEN route |

Table 5-3: Shenzhen VPC

| Destination CIDR block | Next hop | Route type |
| --- | --- | --- |
| 10.1.1.0/24 | Hangzhou VPC | CEN route |
| 3.1.2.0/24 | CCN | CEN route |
| 10.1.3.0/24 | Beijing VBR | CEN route |
| 10.1.4.0/24 | Shanghai VBR | CEN route |
| 192.168.1.0/24 | Beijing VPC | CEN route |
| 192.168.3.0/24 | Shanghai VPC | CEN route |
| 192.168.4.0/24 | Hangzhou VPC | CEN route |