Alibaba Cloud
Cloud Enterprise Network

Best Practices

Issue: 20190906

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: 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: 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: 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: 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 Migrate Express Connect peering connections to CEN

1.1 Migration overview

You can migrate the VPCs and Virtual Border Routers (VBRs) that are using existing Express Connect peering connections to Cloud Enterprise Network (CEN). By using CEN, you can build private network communication channels between VPCs or between VPCs and on-premises data centers. CEN uses automatic route distribution and learning, which can improve the network convergence and the quality and security of cross-network communication, and achieve the interconnection of all your network resources.

Migration procedure

After you complete necessary preparations, add the VPCs and VBRs that use peering connections to a CEN instance, and then manage routes.

CEN automatically learns and distributes routes of the added networks. After a VPC or VBR in a peering connection is added to a CEN instance, the static route configured for the peering connection takes precedence over the dynamic route of the CEN instance. Specifically, if a static route is configured for the peering connection, no route that is more detailed than or the same as the static route is allowed to be learnt by the CEN instance. In this case, we recommend that you divide a large route segment into smaller route segments and delete these routes after CEN learns the routes to ensure smooth migration. For more information about the migration procedure, see Migrate a VPC in a peering connection to a CEN instance and #unique_6.

Differences between CEN and Express Connect peering connections

The following table compares the basic functions of CEN and Express Connect peering connections.

Item	CEN	Express Connect
Network connection	Network-wide interconnection All networks (VPCs and Virtual Border Routers) associated with a CEN instance are interconnected with each other. A secure, reliable, and high-speed intranet communication channel can be established between any two networks.	Single point interconnection Express Connect connections cannot be extended. Specifically, the VPCs or on-premises data centers that are connected through Express Connect can only communicate with the peer VPCs.
Route management	Dynamic learning Based on the Fullmesh link, CEN dynamically learns and distributes routes, which improves the convergence of routes, and the quality and security of network communication.	Manual configuration Express Connect requires end-to-end manual route configuration.
Bandwidth management	Cross-region shared bandwidth package CEN provides bandwidth packages which are sold by region to facilitate cross-region bandwidth adjustments. Bandwidth packages also help optimize resource allocation and save costs.	Point-to-point purchase The bandwidth of an Express Connect connection must be specified when you create the connection. You can adjust the bandwidth value after you create an Express Connect connection, but you cannot change the connected regions.

1.2 Migrate a VPC in a peering connection to a CEN instance

This topic describes how to migrate a VPC that uses a peering connection to a Cloud Enterprise Network (CEN) instance. By using CEN, you can build private network

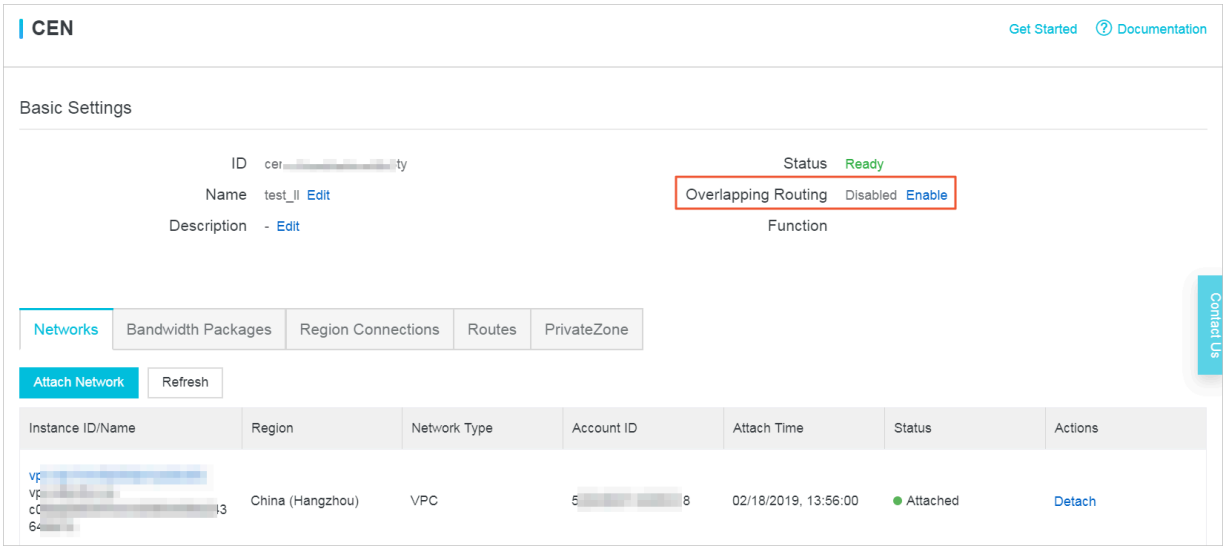
communication channels between VPCs or between VPCs and on-premises data centers. CEN uses automatic route distribution and learning, which can improve the network convergence and the quality and security of cross-network communication, and achieve the interconnection of all network resources.

> **Warning:**
> After you migrate a VPC to a CEN instance, do not freeze or delete the same-region peering connections that belong to the China (Hangzhou) region.

Prerequisites

If you want to use an existing CEN instance, make sure that the overlapping routing function is enabled.

> **Note:**
> If the overlapping routing function is not enabled for the target CEN instance, enable the function first.



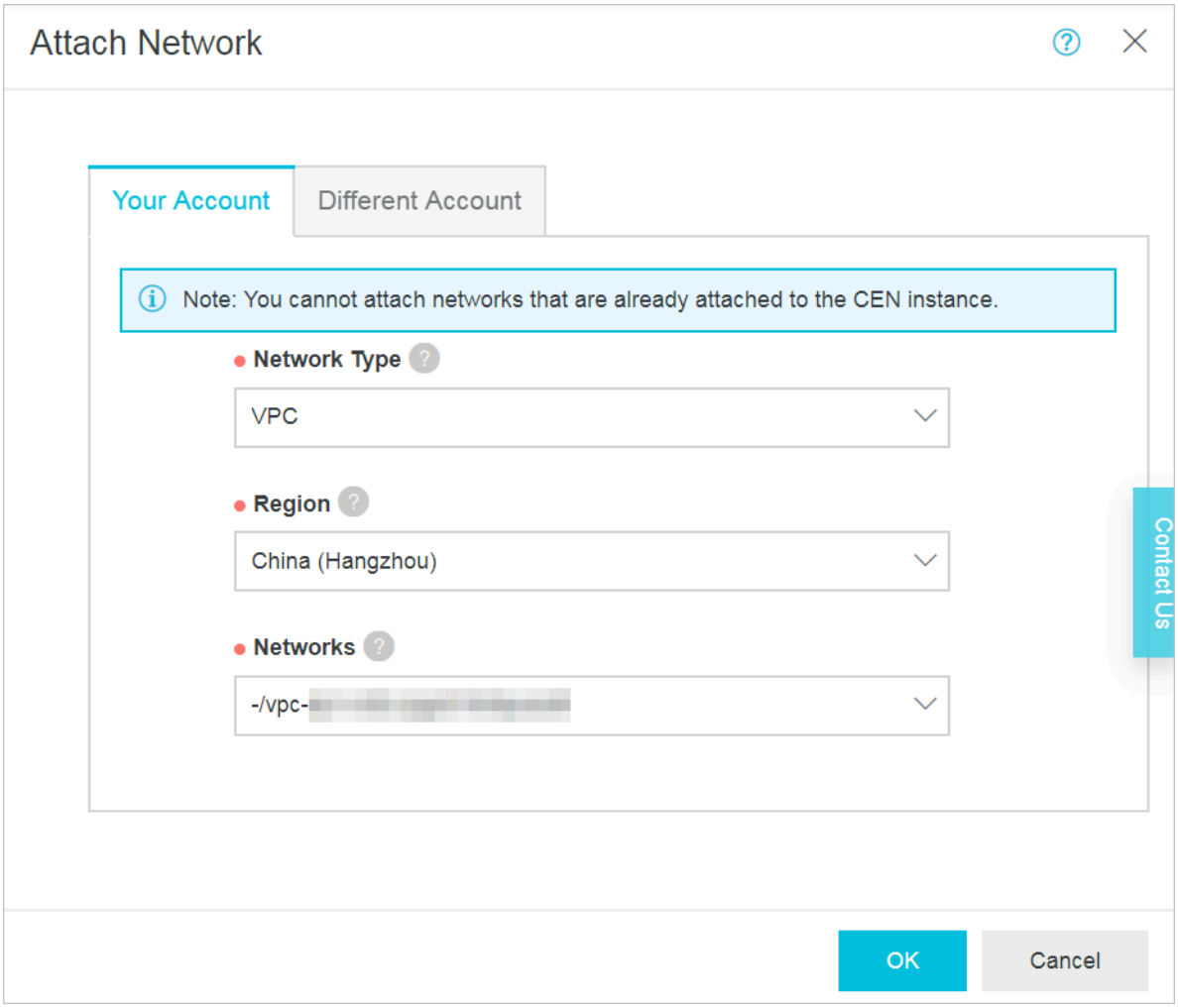
Procedure

To migrate a VPC in a peering connection to a CEN instance, follow these steps:

> **Note:**
> Make sure that you have made the necessary preparations before migration.

1. Log on to the CEN console.
2. On the Instances page, find the target CEN instance and click the instance ID.

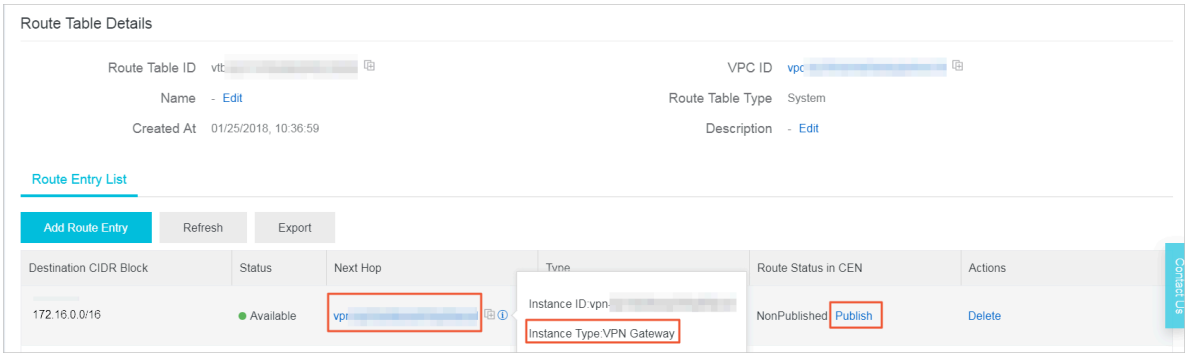
3. On the Networks tab, click Attach Network and add the VPC to be migrated. For more information, see #unique_8.



4. If you need the VPC to communicate with other resources that belong to different regions, you need to buy a bandwidth package and set an intranet communication bandwidth value.

   For more information, see #unique_9/unique_9_Connect_42_section_gtq_n5n_tdb.

5. If you have added routes destined for ECS instances, VPN Gateways, or High-Availability Virtual IP Addresses (HaVips) in the VPC, you need to publish these routes to the CEN instance.

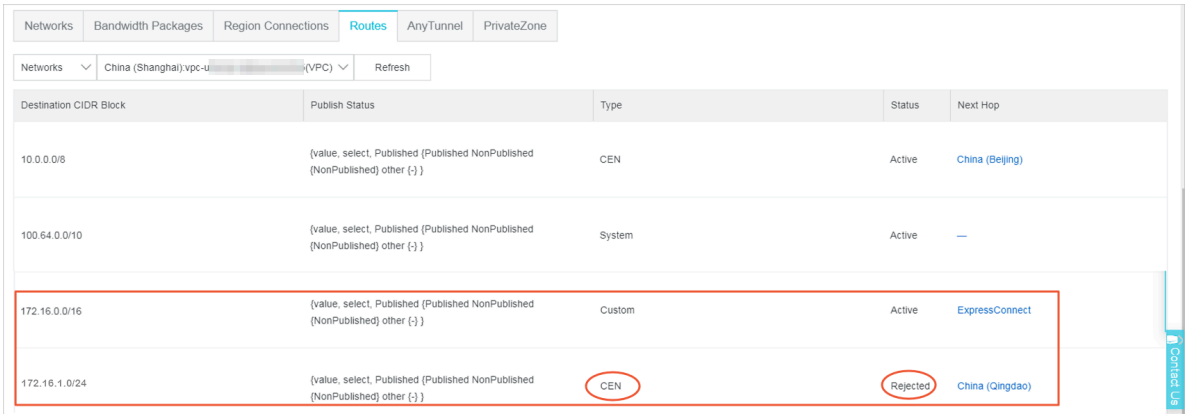


6. Log on to the CEN console, click the ID of the target CEN instance, and on the Routes tab, check the routes. Make sure that the routes do not conflict with each other after you add the VPC to the CEN instance.

   The static route configured for the peering connection takes precedence over the dynamic route of the CEN instance. Specifically, if a static route is configured for the peering connection, no CEN route that is more detailed than or the same as the static route is allowed to be learnt by the CEN instance. In this case, we

recommend that you divide a large route segment into smaller route segments and delete these routes after CEN learns the routes to ensure smooth migration.

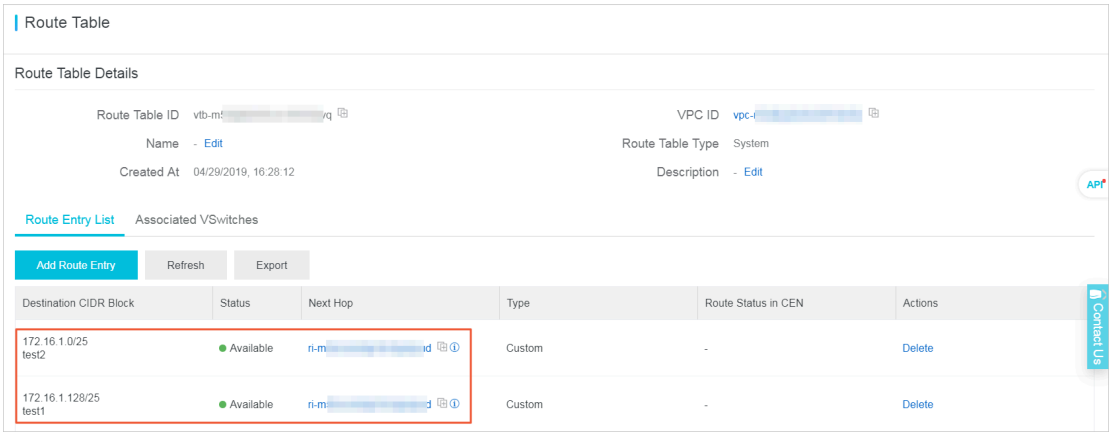
For example, the CEN route 172.16.1.0/24 in the following figure is more detailed than the route 172.16.0.0/16 configured for the peering connection, which constitutes a route conflict.



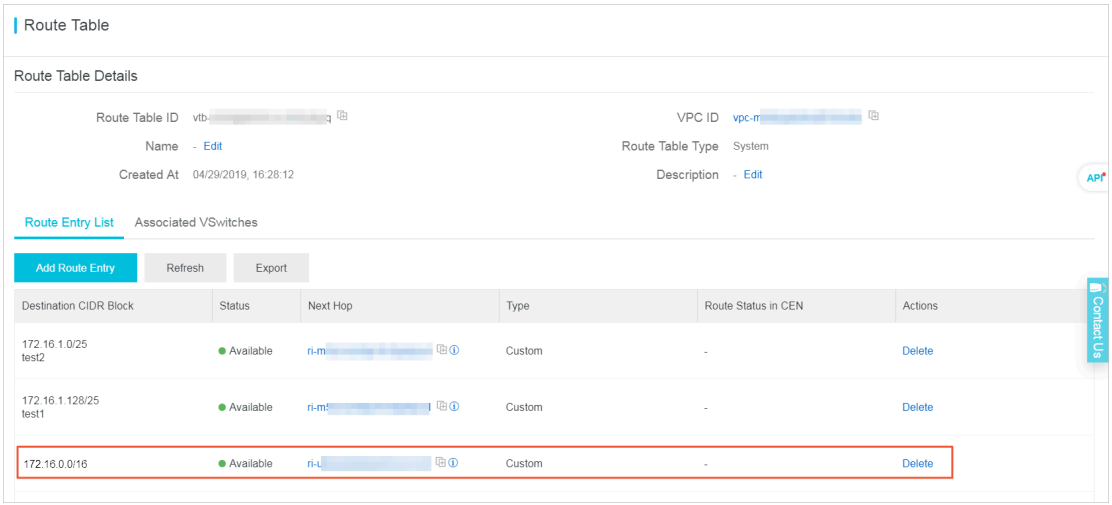
- You can directly delete the route of the peering connection through the VPC console. Then, the CEN route takes effect automatically. However, this method causes intermittent disconnections.

  The duration of disconnections is in proportion to the number of CEN routes . Therefore, we recommend that you use the following method to smoothly migrate the VPC for important services.
- You can divide the peering connection route 172.16.0.0/16 into two smaller route segments, 172.16.1.0/25 and 172.16.1.128/25, which are smaller than the CEN route 172.16.1.0/24.

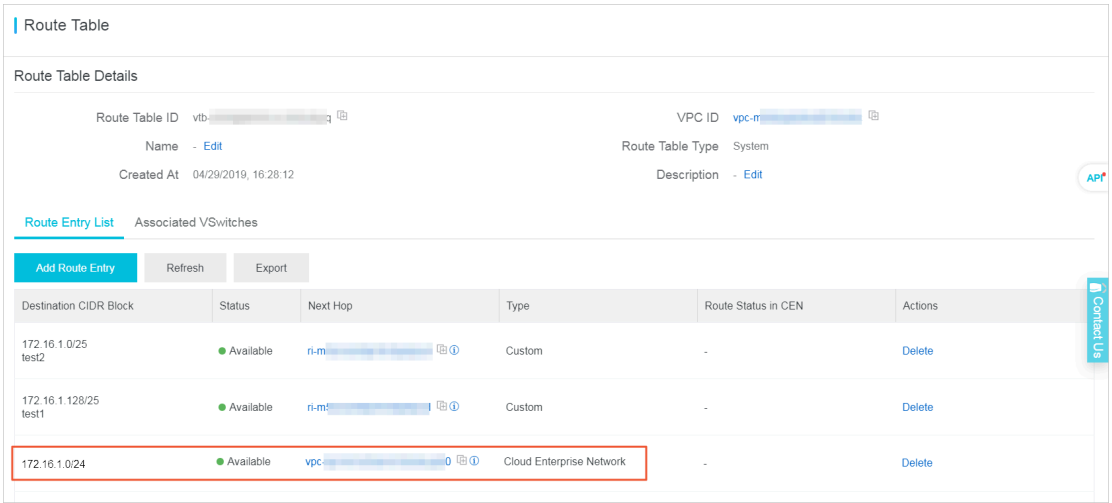
  a. Log on to the VPC console and find the route table to which the target peering connection route belongs.
  b. Click Add Route Entry. Add two route entries that are respectively destined for 172.16.1.0/25 and 172.16.1.128/25 with the Express Connect route interface as the next hop type.



c. In the VPC route table, find the target peering connection route 172.16.0.0/16 and click Delete to delete this route.



d. Click Refresh to check if the CEN route has taken effect.



e. After the CEN route takes effect, delete the added two route entries 172.16.1.0/25 and 172.16.1.128/25 to complete the smooth migration.

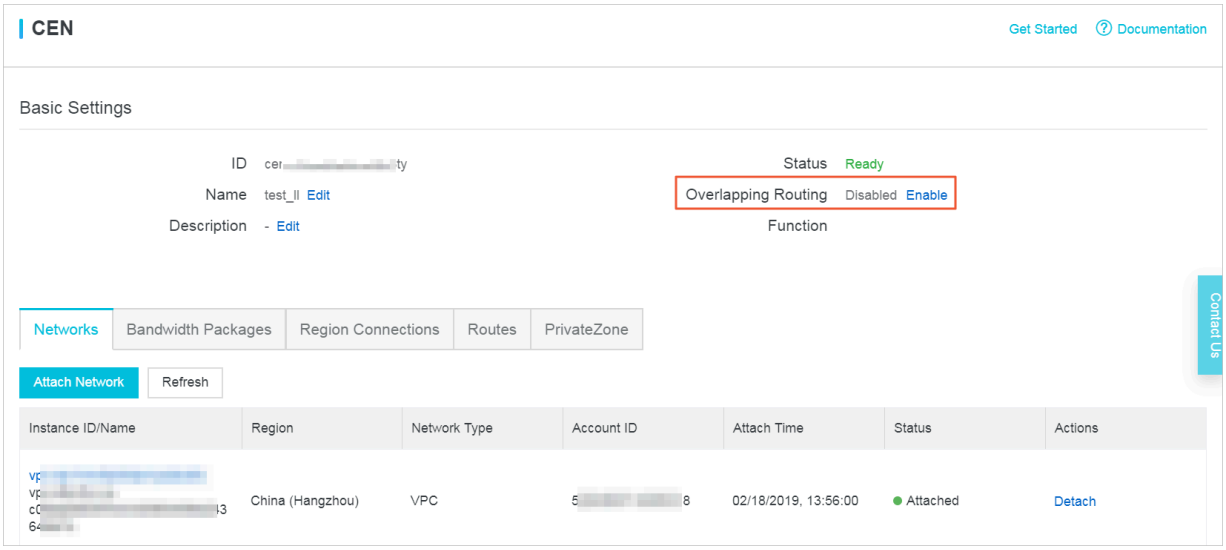
1.3 Migrate a VBR in a peering connection to a CEN instance

This topic describes how to migrate a Virtual Border Router (VBR) that uses a peering connection to a Cloud Enterprise Network (CEN) instance. By using CEN, you can build private network communication channels between VPCs or between VPCs and on-premises data centers. CEN uses automatic route distribution and learning, which can improve the network convergence and the quality and security of cross-network communication, and achieve the interconnection of all network resources.

Prerequisites

If you want to use an existing CEN instance, make sure that the overlapping routing function is enabled.

> **Note:**
> If the overlapping routing function is not enabled for the target CEN instance, enable the function first.



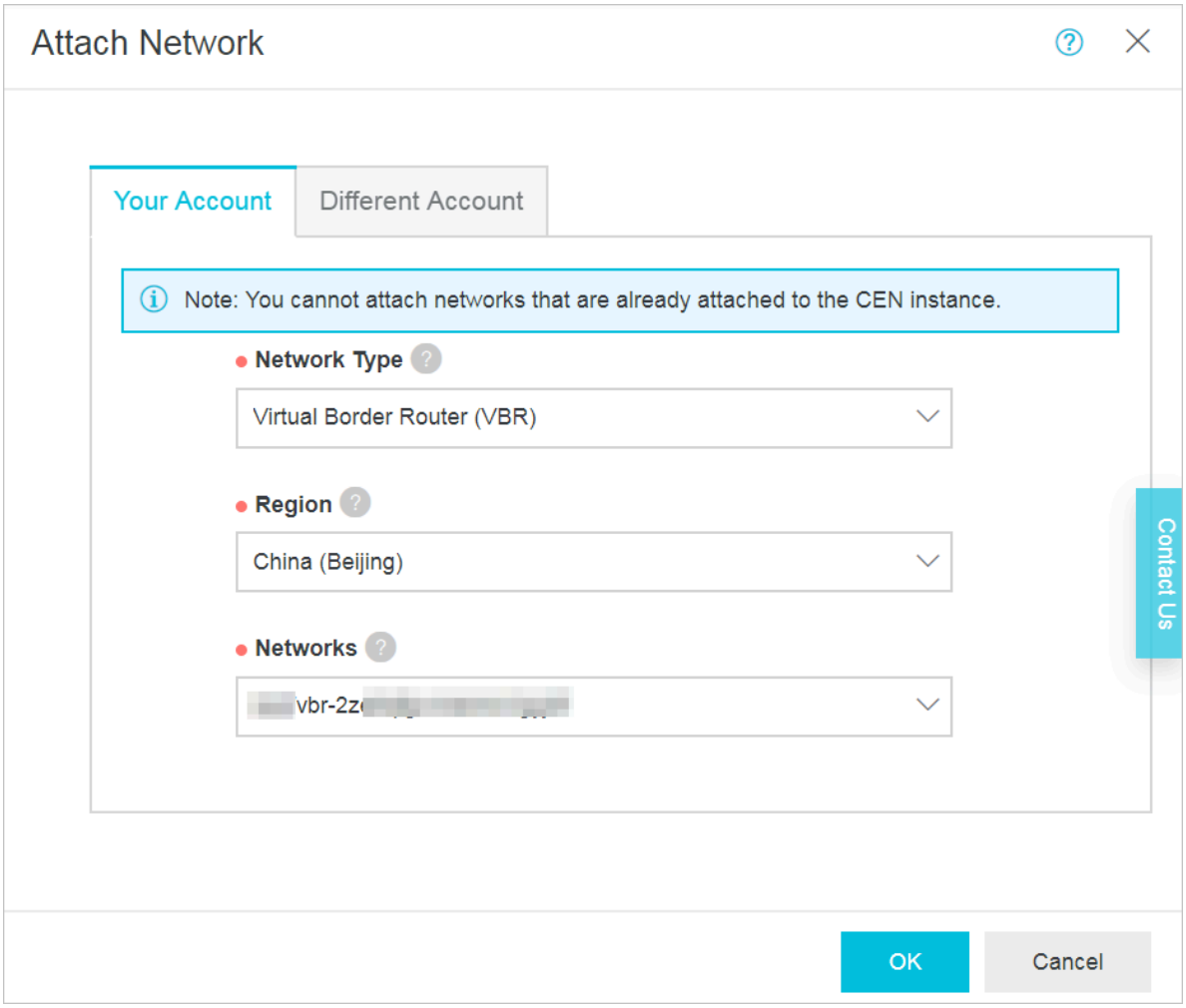
Procedure

To migrate a VBR in a peering connection to a CEN instance, follow these steps:

> **Note:**
> Make sure that you have made the necessary preparations before migration.

1. If you have enabled the health check function for the VBR, we recommend that you first disable the health check function in the Express Connect console.
2. Log on to the CEN console.

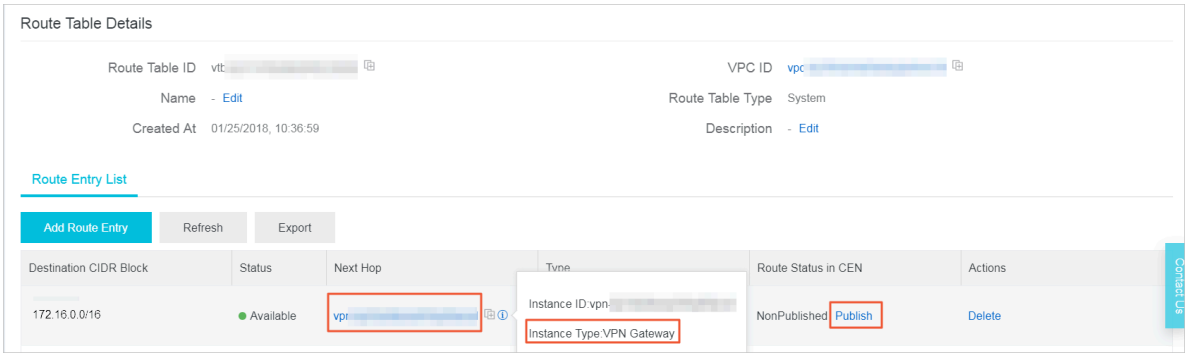
3. On the Instances page, find the target CEN instance and click the instance ID.
4. On the Networks tab, click Attach Network and add the VBR and VPC to be migrated. For more information, see #unique_8.



5. If you need the VPC to communicate with other resources that belong to different regions, you need to buy a bandwidth package and set an intranet communication bandwidth value.

   For more information, see #unique_9/unique_9_Connect_42_section_gtq_n5n_tdb.

6. If you have added routes destined for ECS instances, VPN Gateways, or High-Availability Virtual IP Addresses (HaVips) in the VPC, you need to publish these routes to the CEN instance.



7. If an on-premises data center needs to access cloud resources, such as OSS and PrivateZone, perform the configurations through the CEN console.

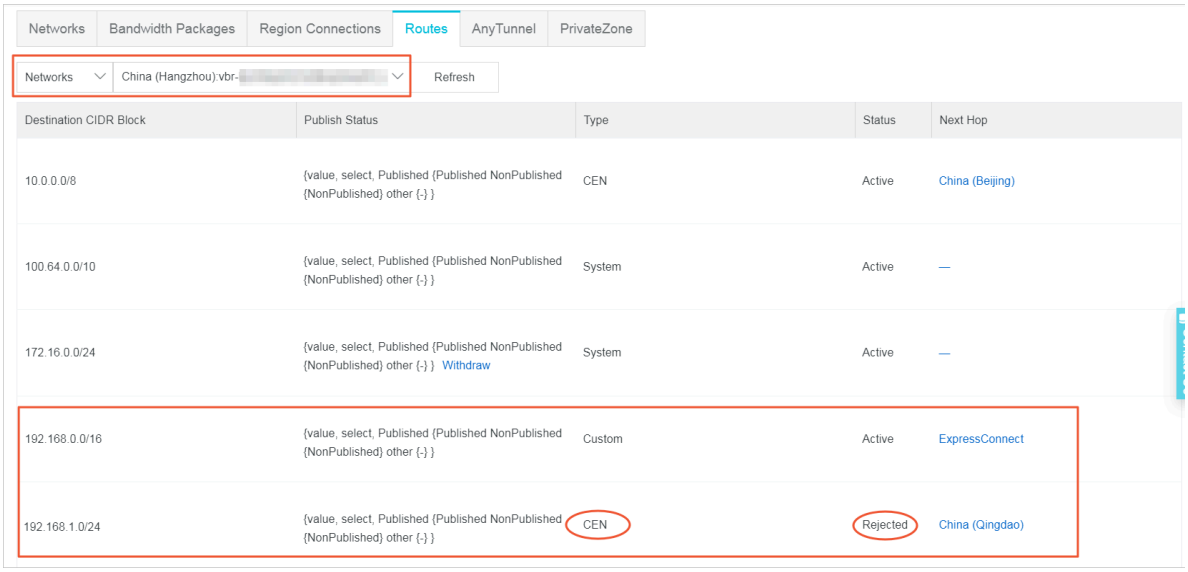
   For more information, see #unique_11.

8. Log on to the CEN console, click the ID of the target CEN instance, and on the Routes tab, check the routes. Make sure that the routes do not conflict with each other after you add the VBR and VPC to the CEN instance.

   The static route configured for the peering connection takes precedence over the dynamic route of the CEN instance. Specifically, if a static route is configured for the peering connection, no CEN route that is more detailed than or the same as the static route is allowed to be learnt by the CEN instance. In this case, we recommend that you divide a large route segment for the peering connection into

smaller route segments and delete these routes after CEN learns the routes to ensure smooth migration.

For example, the CEN route 192.168.1.0/24 in the following figure is more detailed than the route 192.168.0.0/16 configured for the peering connection, which constitutes a route conflict.

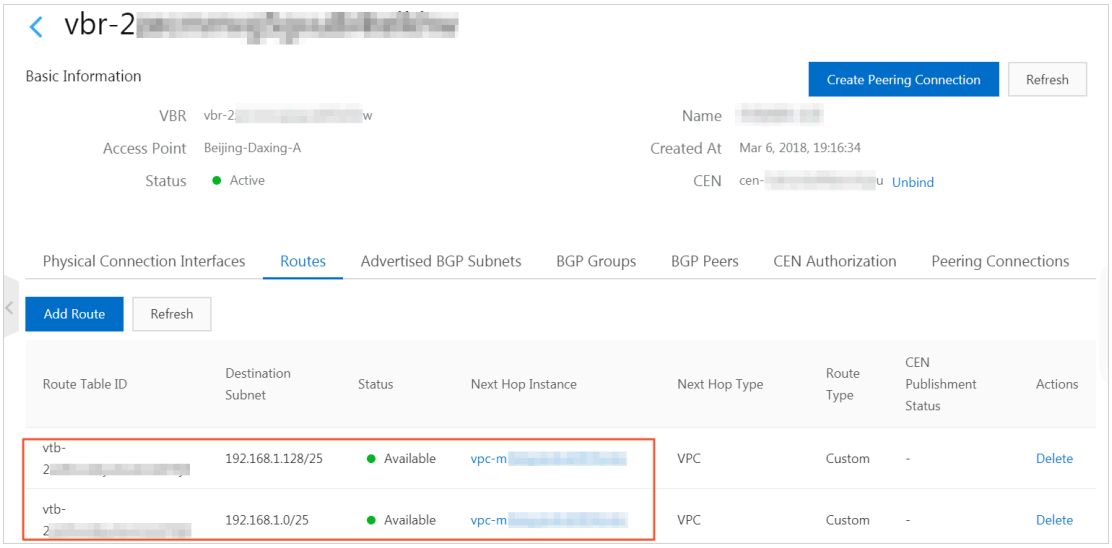


- You can directly delete the route of the peering connection. Then, the CEN route takes effect automatically. However, this method causes intermittent disconnections.

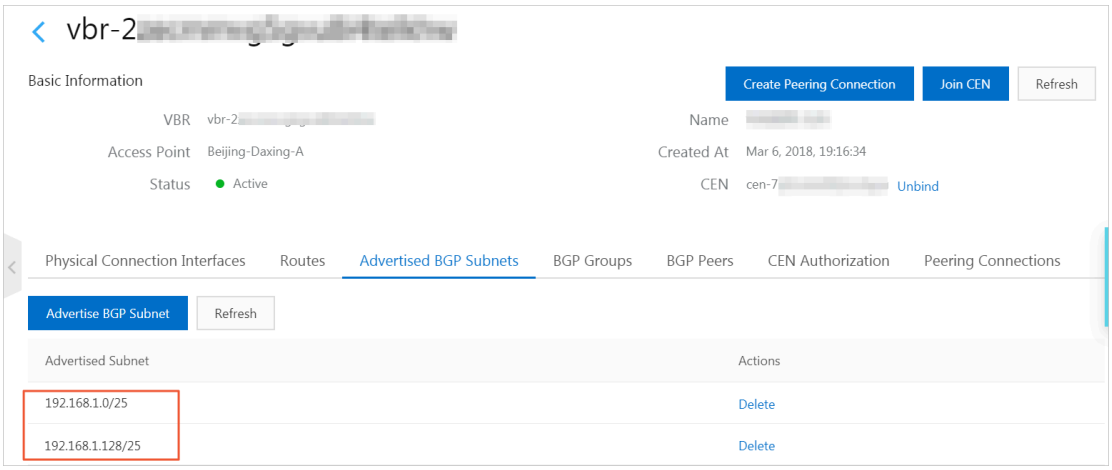
  The duration of disconnections is in proportion to the number of CEN routes . Therefore, we recommend that you use the following method to smoothly migrate the VPC for important services.
- You can divide the peering connection route 192.168.0.0/16 into two smaller route segments, 192.168.1.0/25 and 192.168.1.128/25, which are smaller than the CEN route 192.168.1.0/24.

  a. Log on to the Express Connect console, find the target VBR, click the VBR ID, and then click the Routes tab.

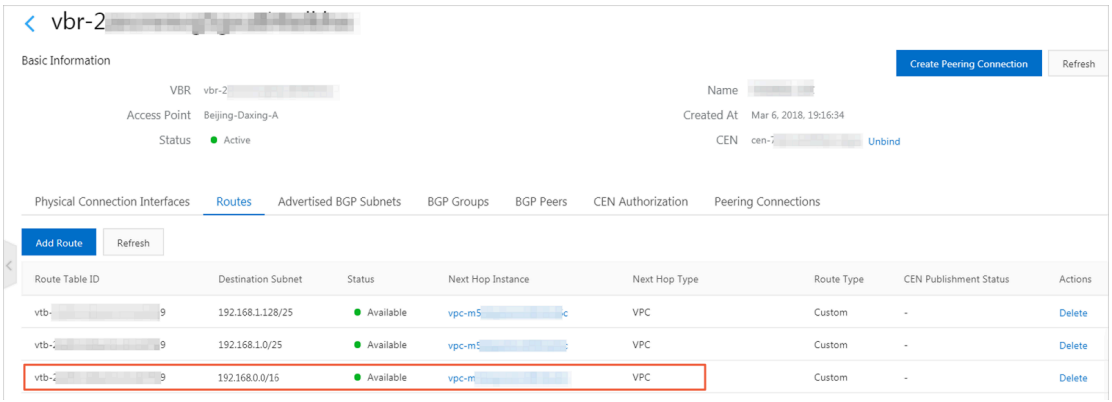
  b. Click Add Route. Add two routes that are respectively destined for 192.168.1.0/25 and 192.168.1.128/25 with the next hop type of VPCs.



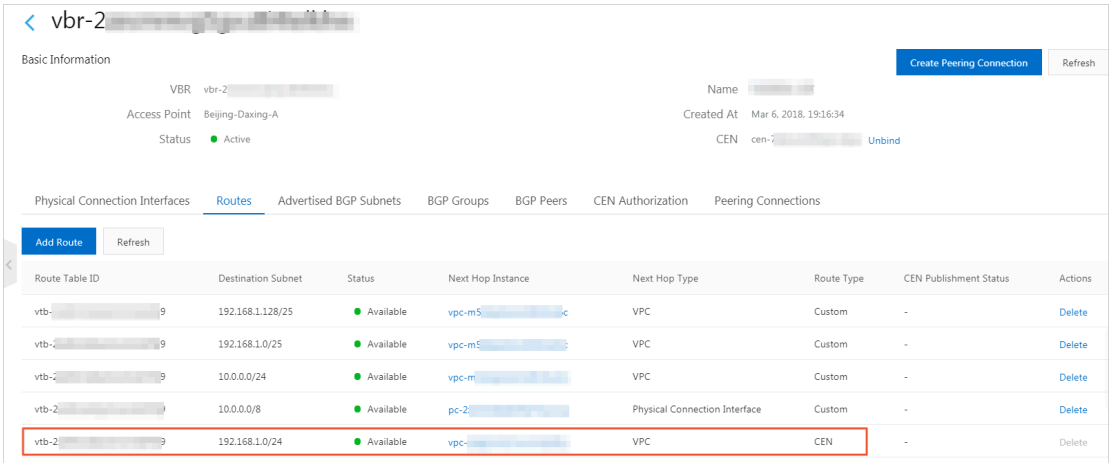
c. For BGP routing, you need to advertise the CIDR blocks related to 192.168.1.0/25 and 192.168.1.128/25.



d. Delete the peering connection route 192.168.0.0/16.



e. Click Refresh and check whether the CEN route has taken effect.



f. Delete the two routes 192.168.1.0/25 and 192.168.1.128/25 in the VBR route table, and delete the advertised BGP routes.

g. In the CEN console, configure health checks for the migrated VBR. For more information, see #unique_12/unique_12_Connect_42_section_hv3_qzn_tdb.

1.4 Roll back the migration

This topic describes how to roll back your migration by modifying the routes.

Rollback solutions depend on the migration methods you have adopted. The available rollback solutions are as follows:

- Migration with intermittent disconnections: Re-add the deleted static route of the peering connection. All the routes that are more detailed than or equals the re-added peering connection route are automatically deleted.
- Smooth migration: Re-add the deleted detailed routes directly.

> **Note:**
> If the migrated Virtual Border Router (VBR) is configured with BGP routes, you need to re-advertise the related CIDR blocks.

2 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 #unique_12.
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.

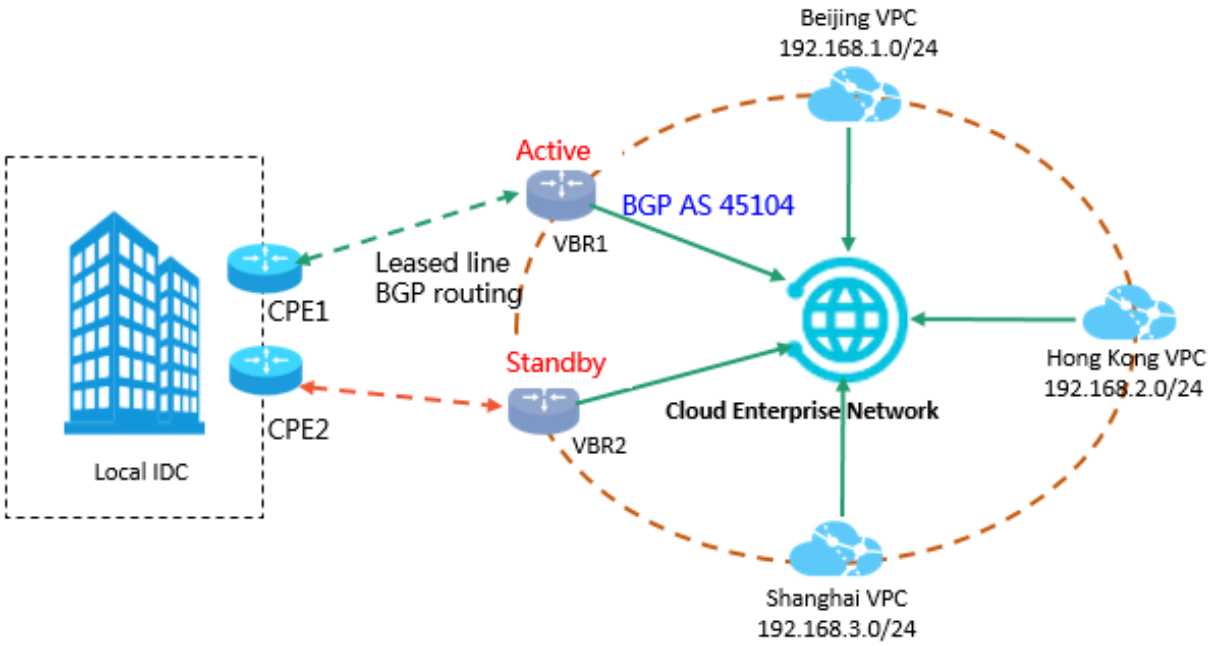
Network topology

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

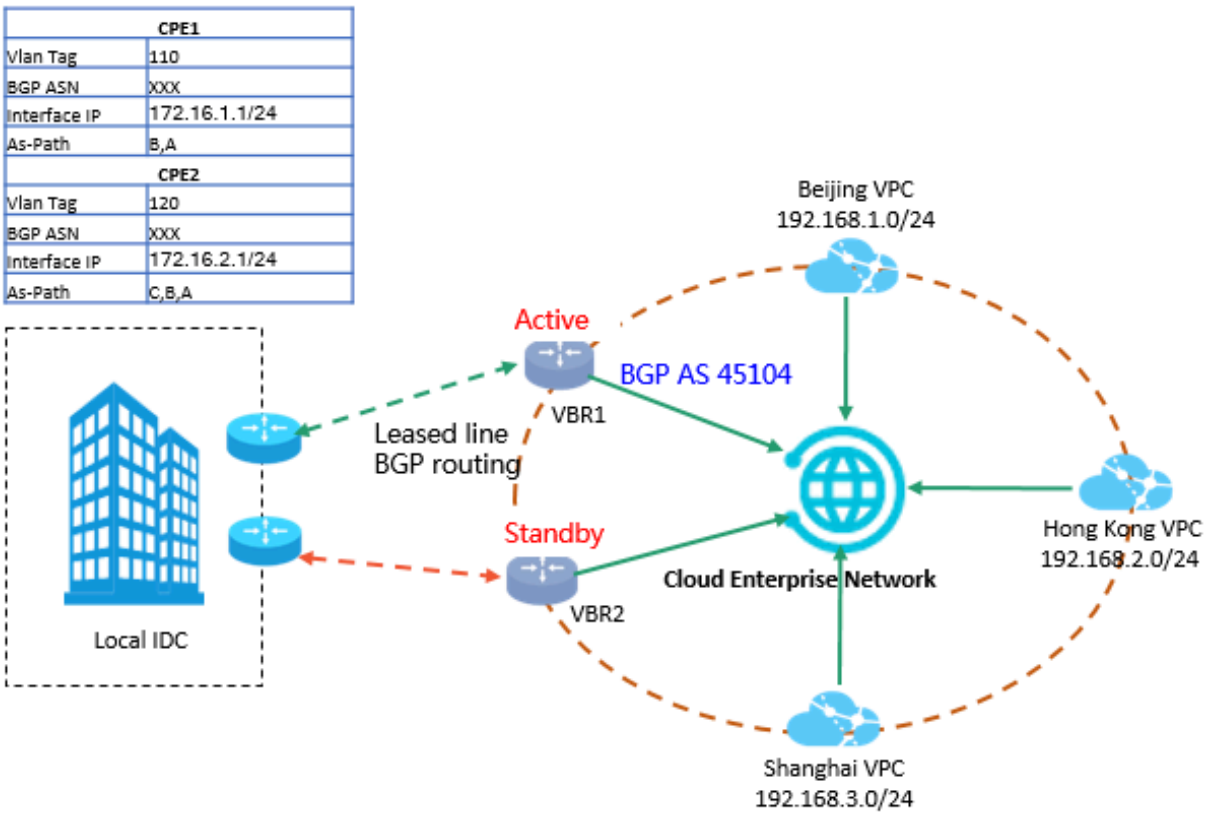
Network	CIDR block
Beijing VPC	192.168.1.0/24
Hong Kong VPC	192.168.2.0/24
Shanghai VPC	192.168.3.0/24



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 #unique_15/unique_15_Connect_42_section_fxm_rbb_ydb).

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.



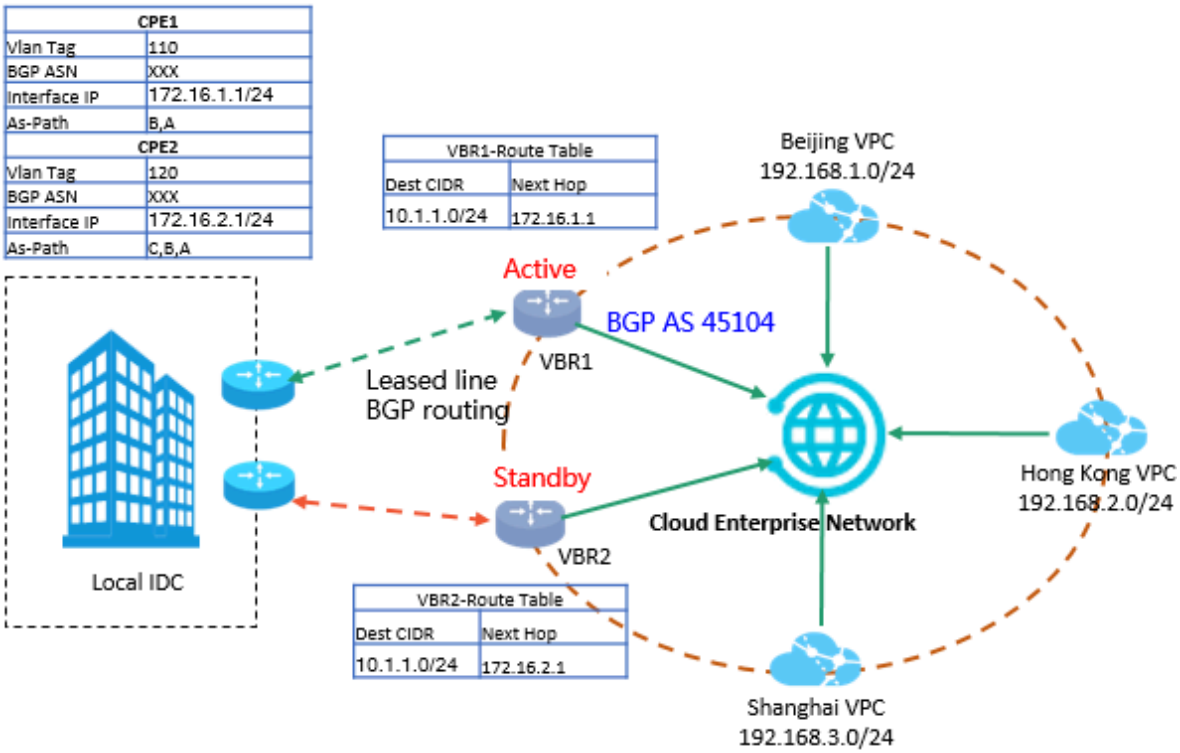
As shown in the preceding figure, the green line (CPE1) is the active link and the red line (CPE2) is the standby link. The BGP configurations of the two CPEs are as follows.

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

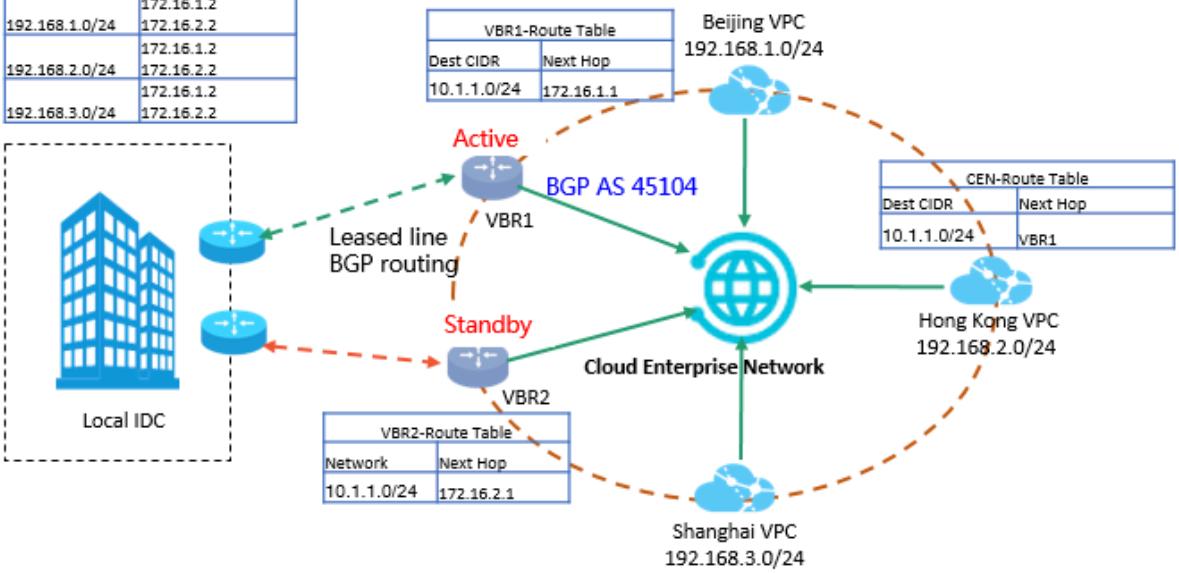


As shown in the following figure, the route tables of VBR1 and VBR2 contain routes and next hops learned from the BGP peers of VBR1 and VBR2. The VBRs, which are attached to the CEN, send the BGP routes learned from the local data center to the CEN, including AS-Path configurations.

- All routes in the CEN

CPE1	
Vlan Tag	110
BGP ASN	XXX
Interface IP	172.16.1.1/24
As-Path	B,A
CPE2	
Vlan Tag	120
BGP ASN	XXX
Interface IP	172.16.2.1/24
As-Path	C,B,A

IDC Route Table	
Dest CIDR	Next Hop
192.168.1.0/24	172.16.1.2 172.16.2.2
192.168.2.0/24	172.16.1.2 172.16.2.2
192.168.3.0/24	172.16.1.2 172.16.2.2



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).

3 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 #unique_12.
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 #unique_17/unique_17_Connect_42_section_kvd_hqn_l2b.

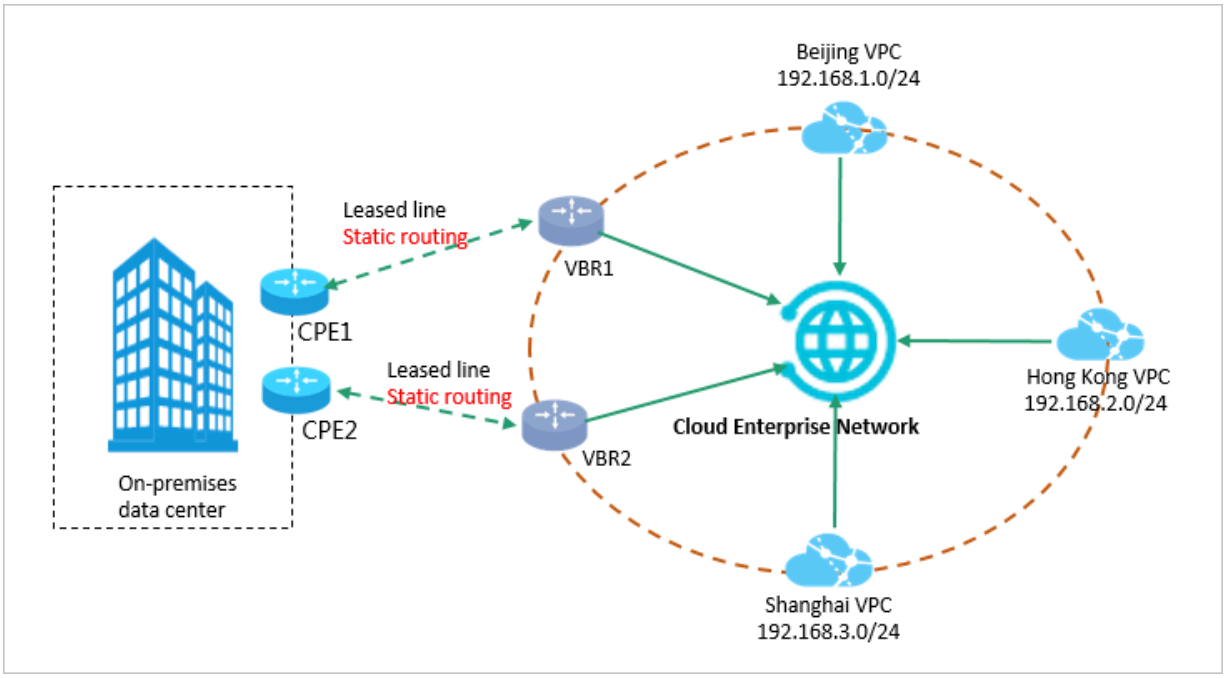
Network topology

The network topology used in this topic is as follows:

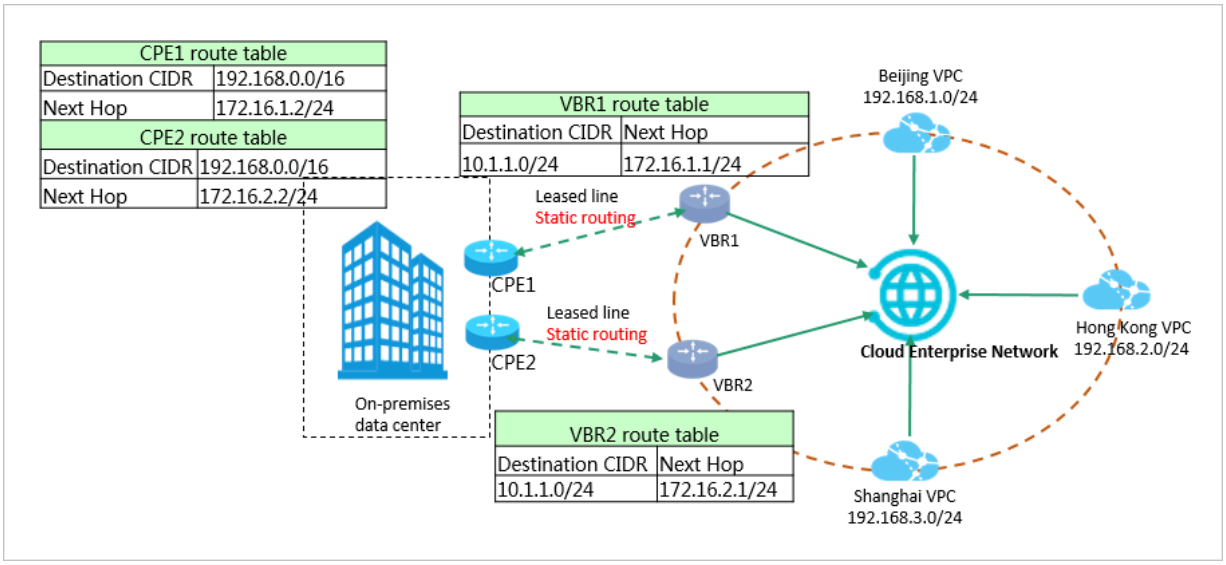
- The on-premises data center is already connected to the VBRs through two leased lines. Configure static routes between the on-premises data center and the VBRs.
- Three VPCs are already created in the China (Beijing), China (Shanghai), and China (Hong Kong) regions.

- 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.

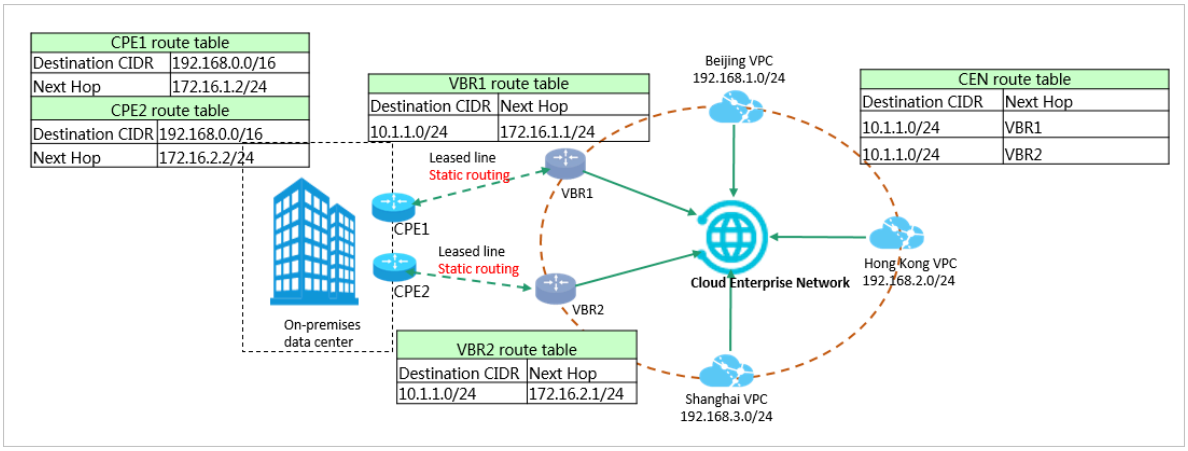
Configuration	CPE1	CPE2
Destination CIDR block	192.168.0.0/16	192.168.0.0/16
Next hop	172.16.1.2/24 (VBR1)	172.16.2.2/24 (VBR2)

- VBR route configuration

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

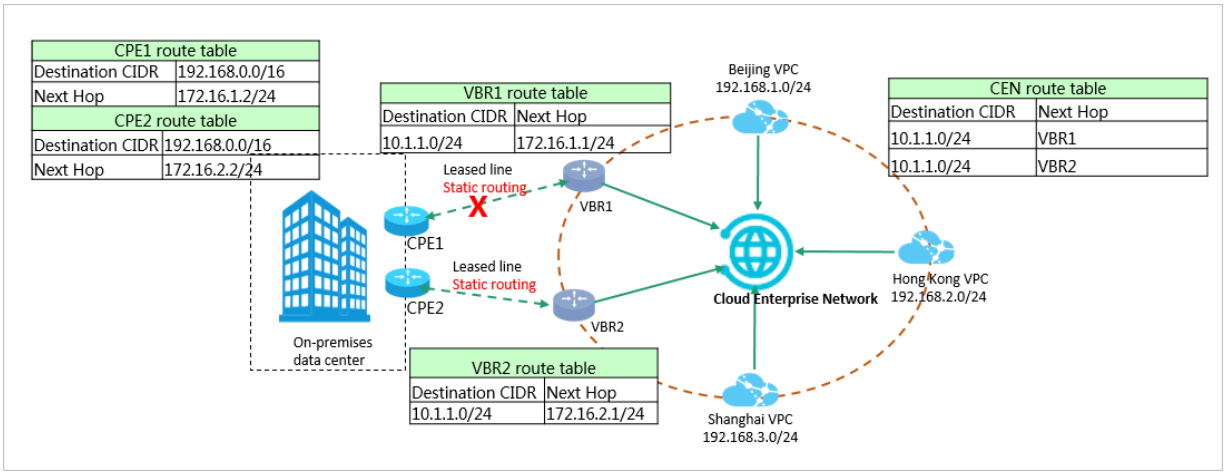
Configuration	VBR1	VBR2
Destination CIDR block	10.1.1.0/24	10.1.1.0/24
Next hop	172.16.1.1/24	172.16.2.1/24

- 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.

4 Connect an on-premises data center to Alibaba Cloud through a VPN Gateway

This topic describes how to use VPN Gateway and Cloud Enterprise Network (CEN) to connect an on-premises data center to Alibaba Cloud and enable the on-premises data center to communicate with VPCs in different regions.

Overview

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

1. Configure a VPN Gateway

   Create an IPsec-VPN connection to connect the on-premises data center to Alibaba Cloud. For more information, see #unique_19.
2. Attach networks

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

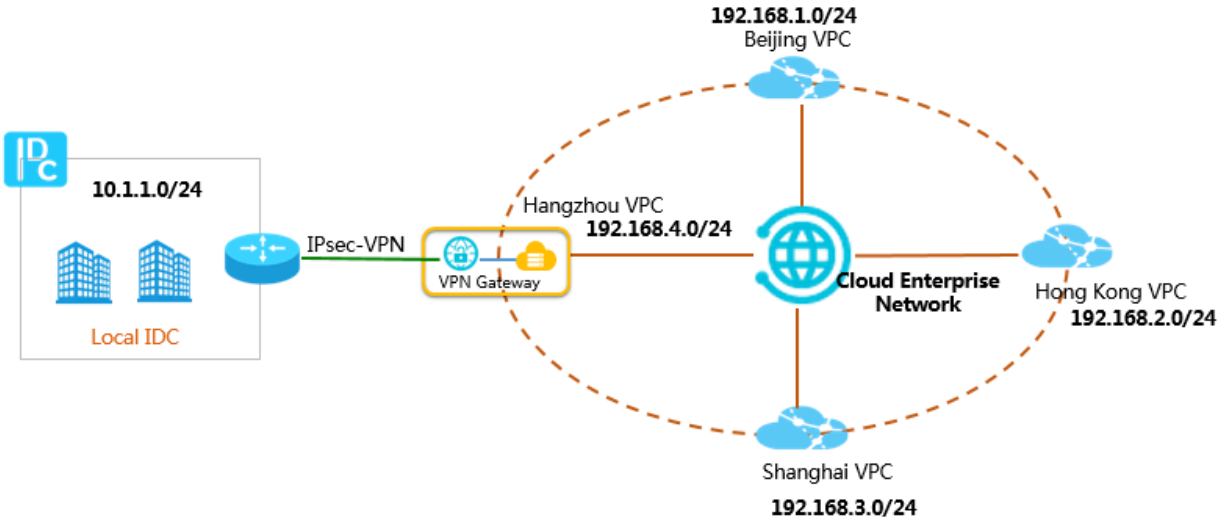
   You can publish the route entry pointing to the VPN Gateway in the VPC to CEN, so that other networks attached to the CEN instance can learn the route.

Network topology

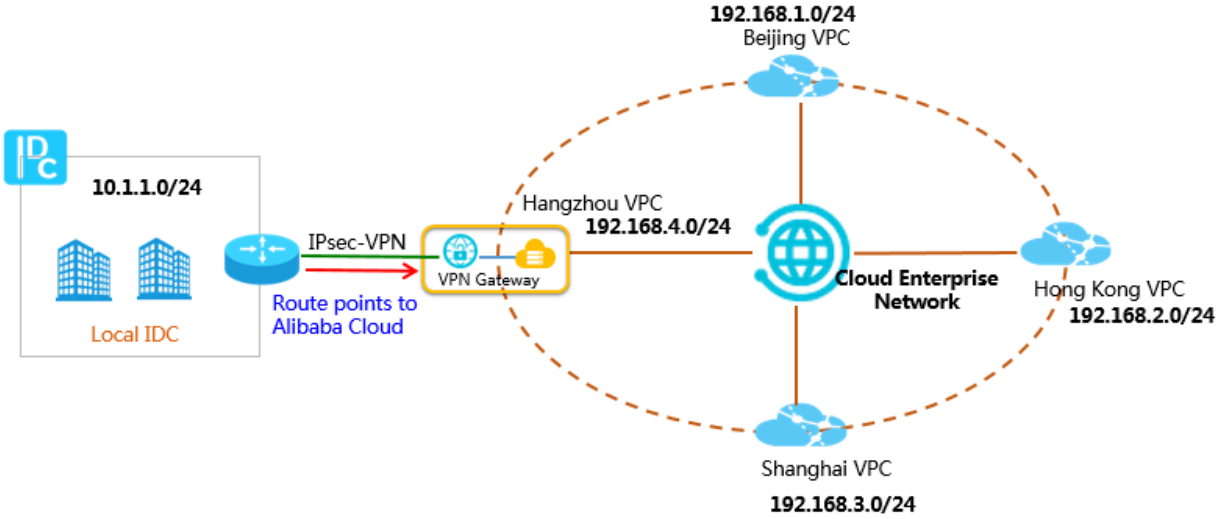
The network architecture used in this topic is as follows:

- The on-premises data center is connected to Alibaba Cloud through the VPN Gateway.
- Three VPCs are created in the China (Hangzhou), China (Beijing), China (Shanghai), and Hong Kong regions.
- The CIDR blocks of networks in this topic are as follows. Make sure that the CIDR blocks do not conflict with each other.

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
Hangzhou VPC	192.168.4.0/24



On-premises data center route configuration



An IPsec-VPN connection is established between the on-premises data center and the VPN Gateway, and custom or contributing route entries pointing to Alibaba Cloud are configured.

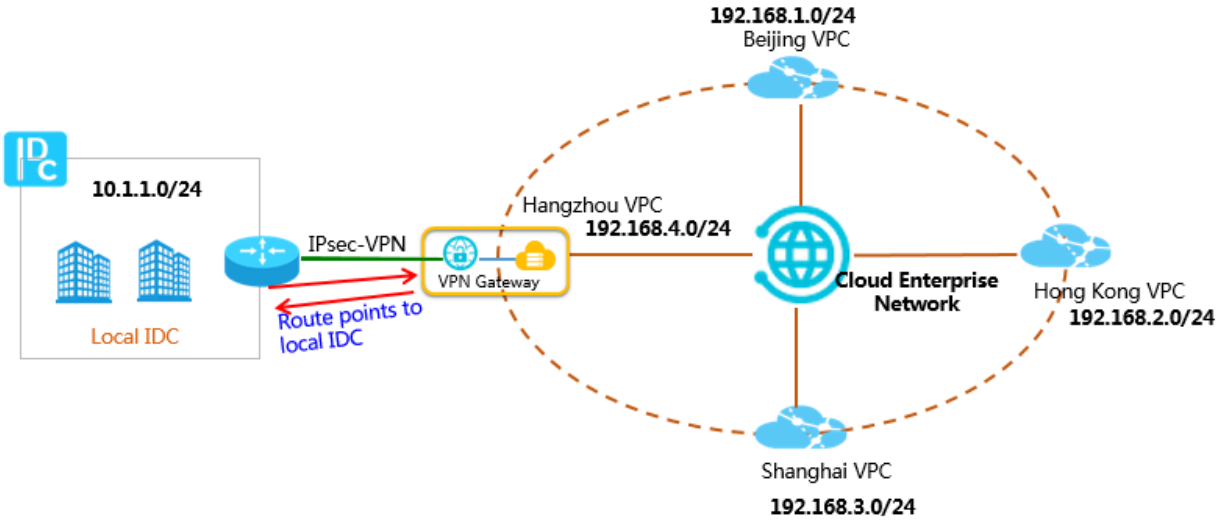
Table 4-1: Contributing route entries in the on-premises data center

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
192.168.4.0/24	VPN Gateway

Table 4-2: Default route entries in the on-premises data center

Destination CIDR block	Next hop
0.0.0.0/0	VPN Gateway

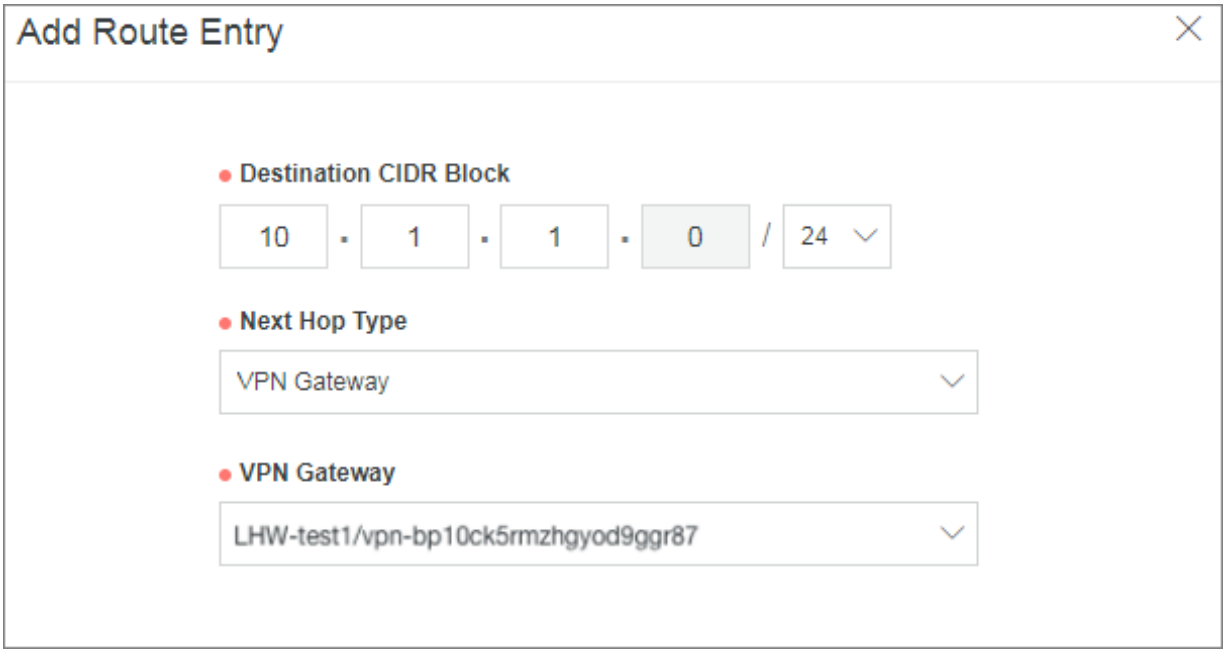
VPC route configuration



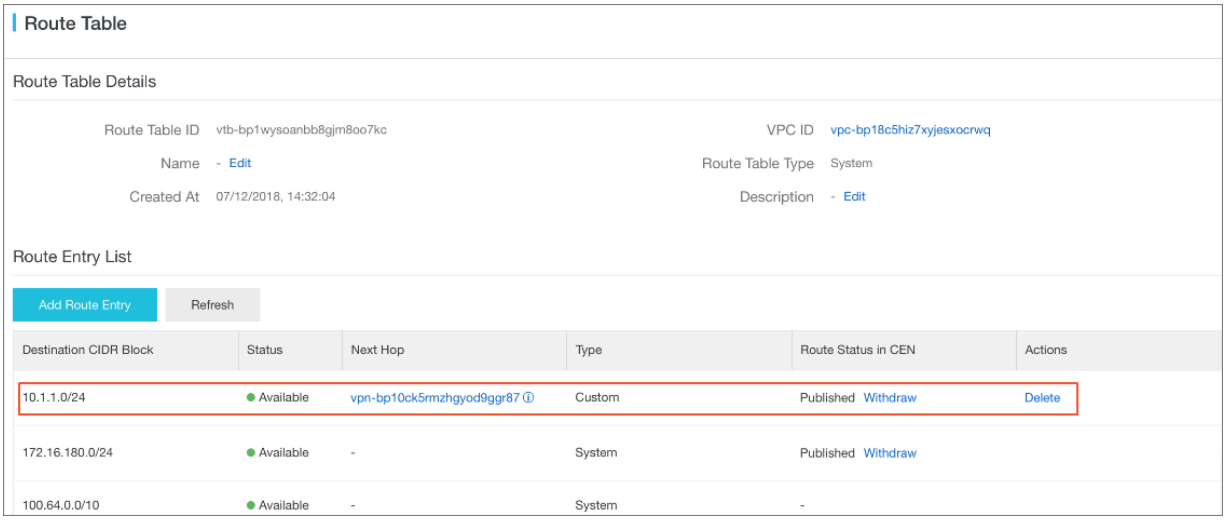
To enable the communication between the on-premises data center and the VPCs, you need to configure a route entry pointing to the on-premises data center (VPN Gateway) in the VPC connected to the VPN Gateway and publish the route to CEN.

A route entry pointing to Alibaba Cloud is created in the on-premises data center, so traffic from the on-premises data center can be forwarded to Alibaba Cloud. To forward traffic from the Hangzhou VPC to the on-premises data center, configure a route entry pointing to the VPN Gateway in the Hangzhou VPC.

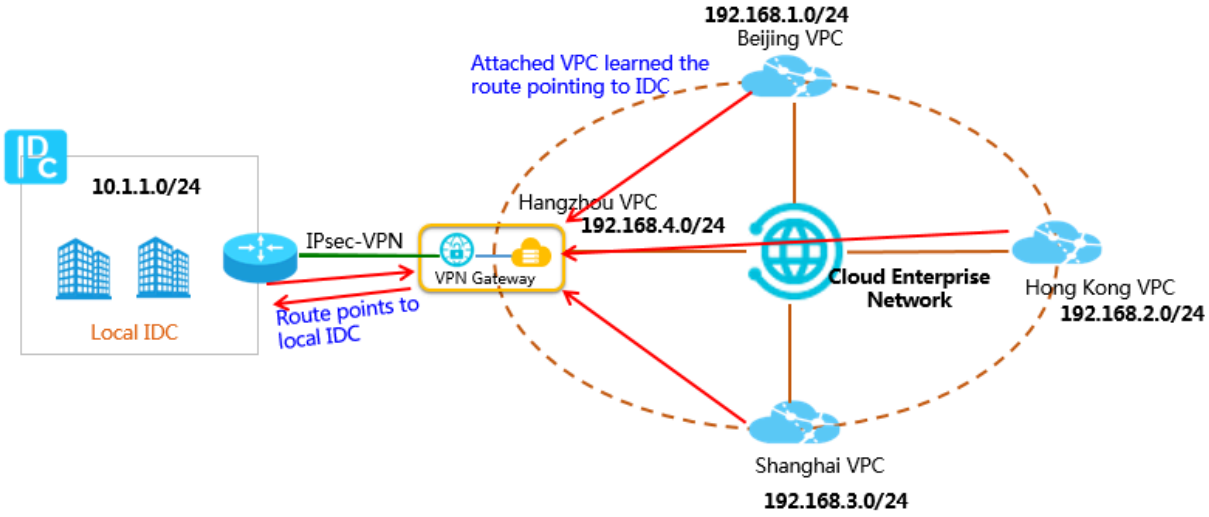
As shown in the following figure, you need to configure a custom route entry pointing to the VPN Gateway (on-premises data center) in the Hangzhou VPC:



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

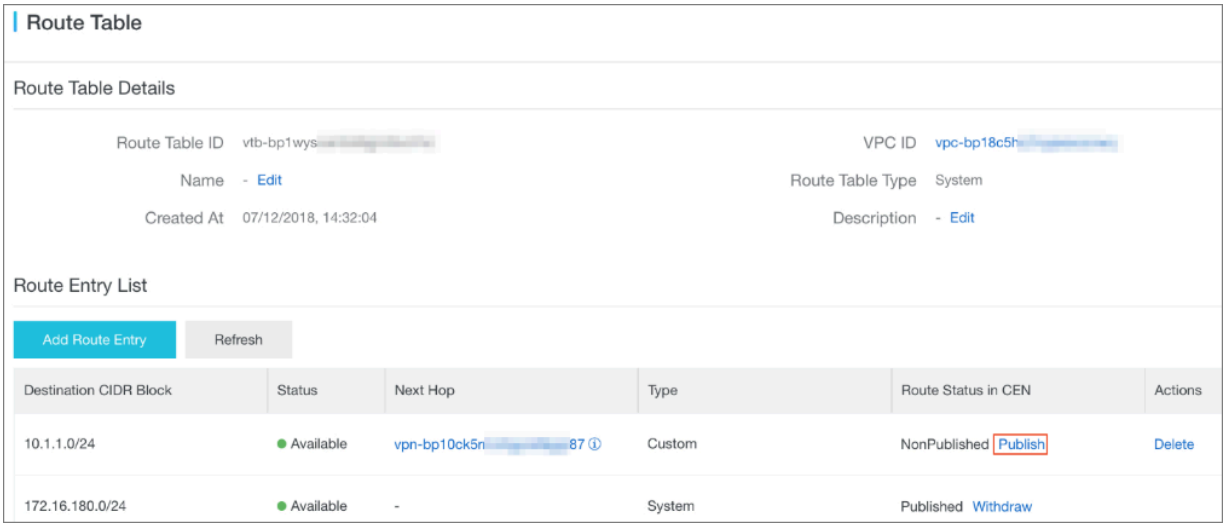


Publish the route entry to CEN

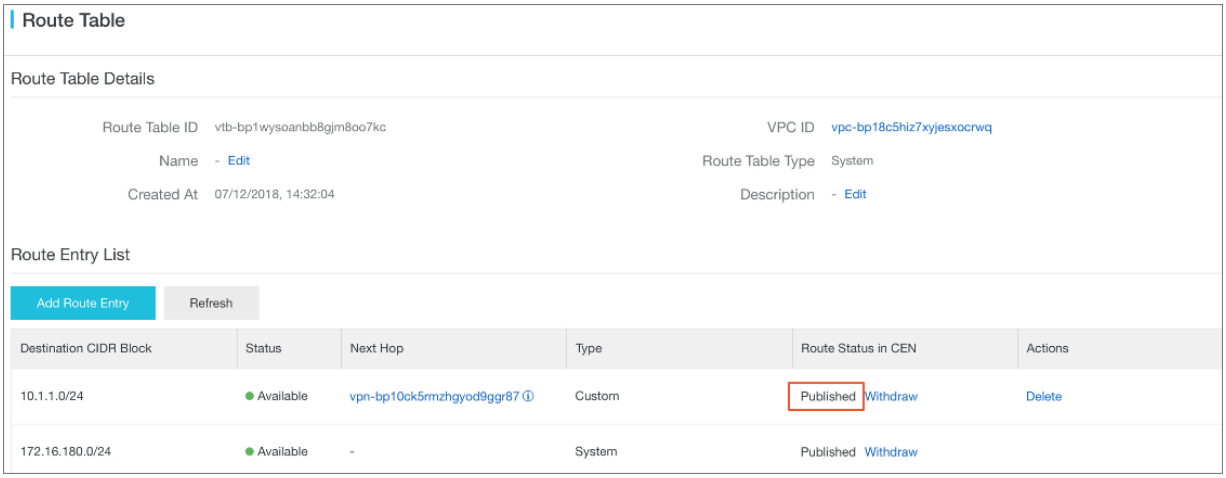


To mark other VPCs attached to the CEN instance learn the route pointing to the on-premises data center, you need to publish the route entry pointing to the VPN Gateway to the CEN instance so that other attached VPCs can learn the route.

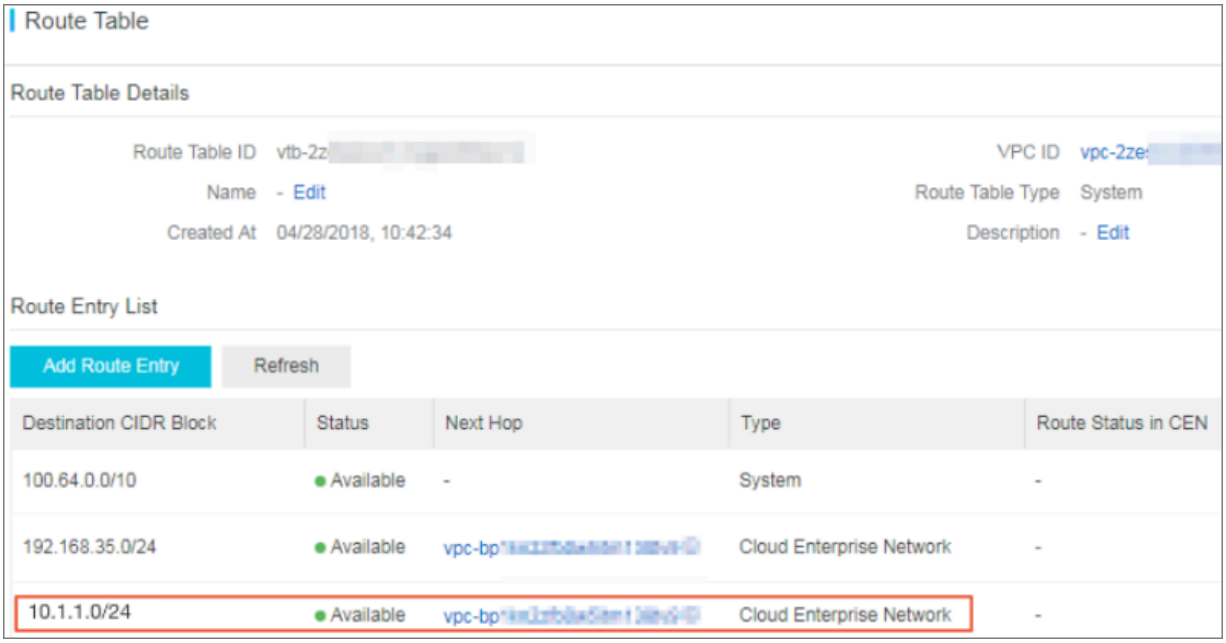
The following figure shows the route table before the route entry is published.



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 instance .



After the previous operations, other VPCs attached to the CEN instance have learned the route entry pointing to the on-premises data center. Therefore, the on-premises data center can communicate with any VPC attached to the CEN instance.

CEN route publishing

The preceding 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
A route entry pointing to a VPN Gateway	VPC	No
A route entry pointing to a High-Availablity Virtual IP Address (HaVip)	VPC	No
A VPC system route entry	VPC	Yes
A route entry pointing to an on-premises data center	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 instance and then is deleted from the VPC to which it belongs, the route entry is also deleted from the CEN instance.

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 #unique_20 API.

5 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.

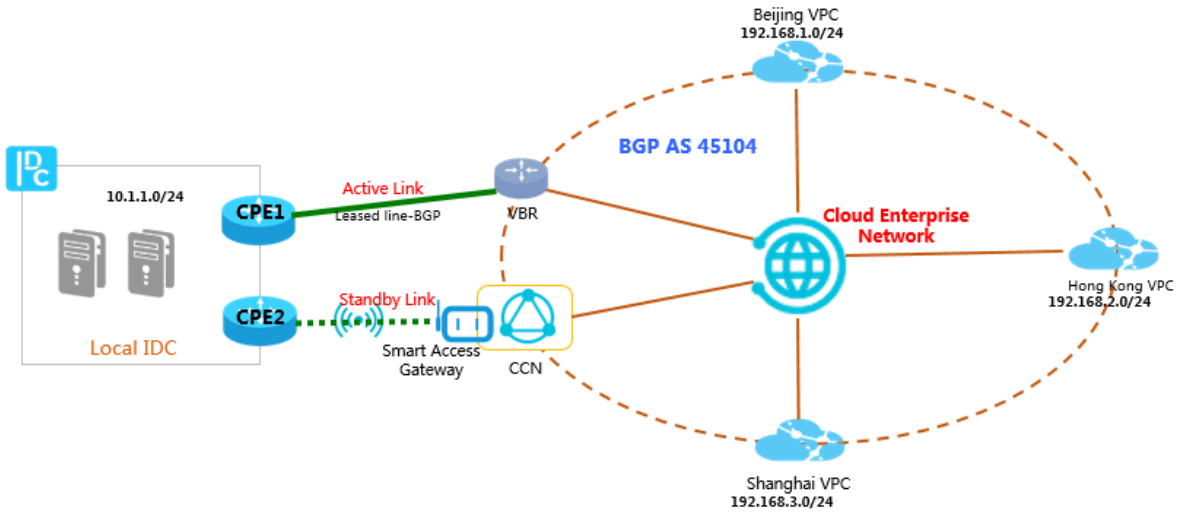
Network topology

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

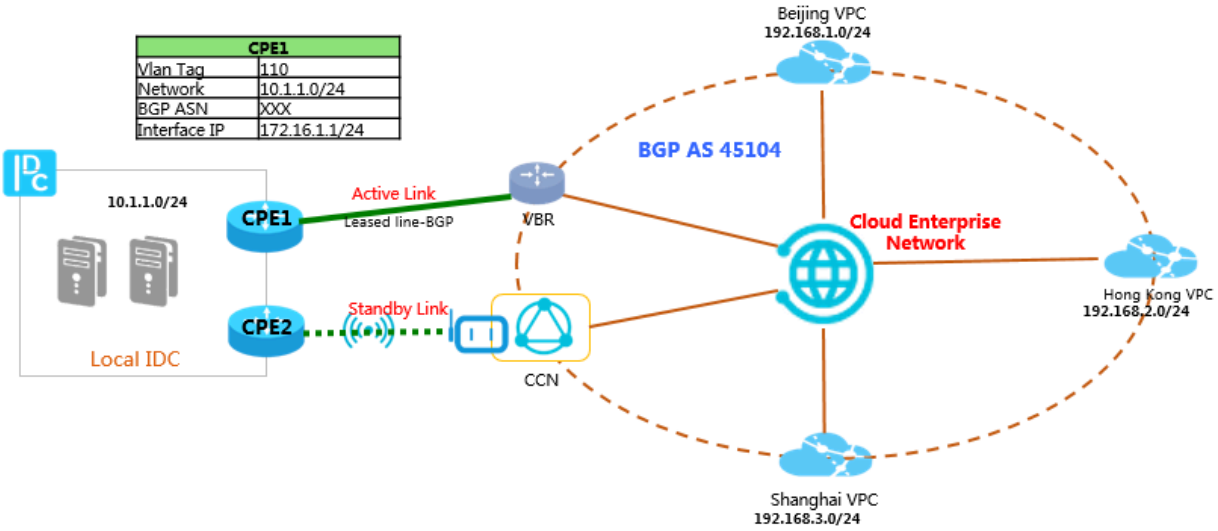
When a leased line and a Smart Access Gateway destined to the same CIDR block are connected to a CEN, the route priority within the CEN is: the leased line takes precedence over Smart Access Gateway.

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.

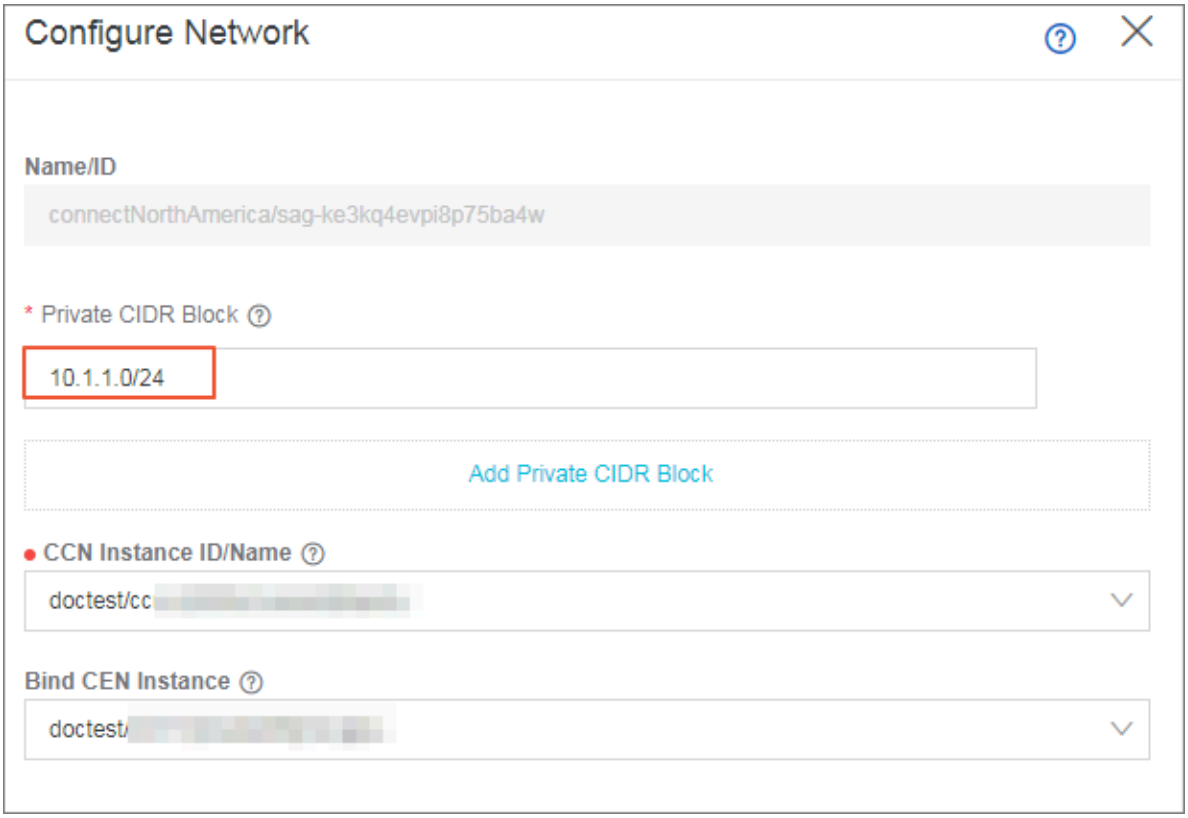
Configuration	Value
Vlan Tag	110
Network	10.1.1.0/24
BGP ASN	xxx
Interface IP	172.16.1.1/24



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.

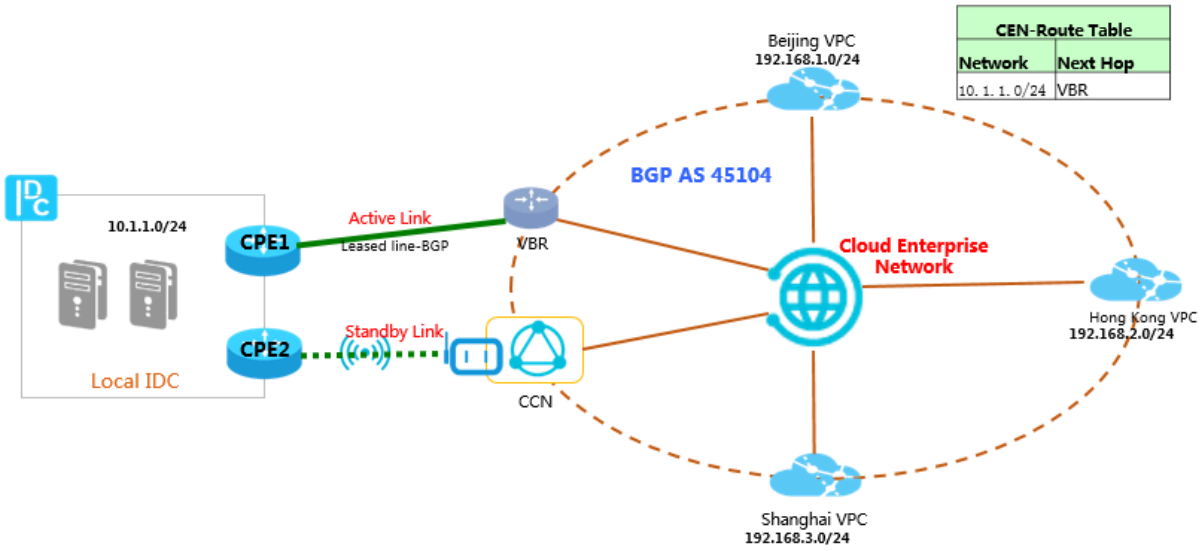
   The Smart Access Gateway has been attached to the CEN. You need to configure the CIDR block 10.1.1.0/24 of the local IDC in the Smart Access Gateway.



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.

6 Build an enterprise-level hybrid cloud by using different access methods

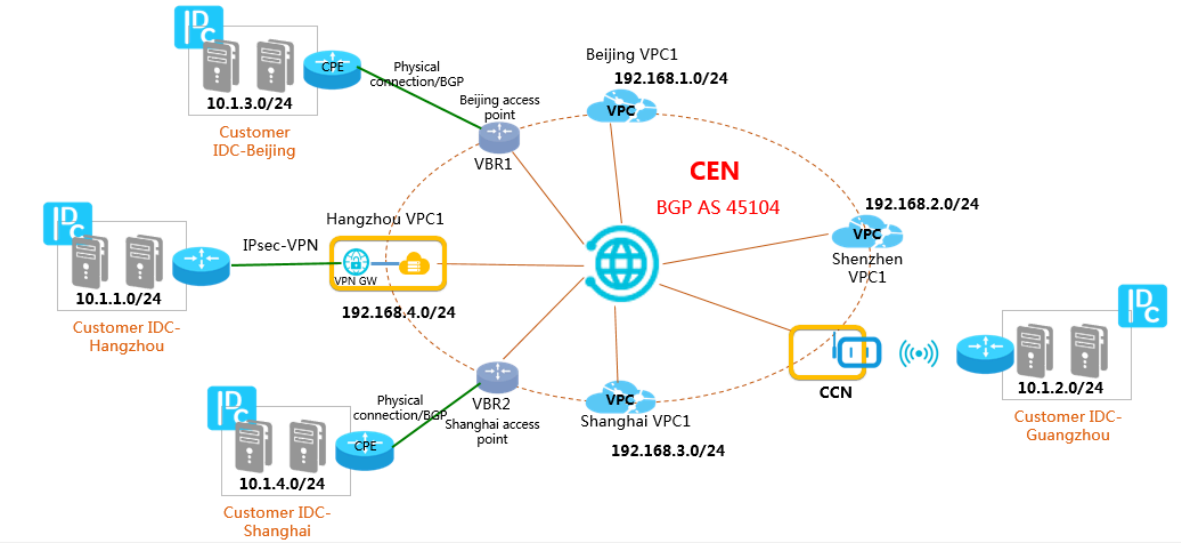
Cloud Enterprise Network (CEN) provides a high-quality network transmission environment. By simplifying the networking process, CEN helps you rapidly build a hybrid cloud network with enterprise-level scale and communication capability. This topic describes how to rapidly build a hybrid cloud network by using CEN together with Express Connect physical connections, VPN Gateway, and Smart Access Gateway.

Network topology

This topic takes the following network topology as an example:

- A company has deployed on-premises data centers in Beijing, Shanghai, Hangzhou , and Guangzhou.
- The company has also deployed services on the cloud. It has created separate VPCs in the China (Beijing), China (Shanghai), China (Hangzhou), and China (Shenzhen) regions.
- Beijing and Shanghai on-premises data centers are connected to access points of Alibaba Cloud through physical connections and their corresponding Virtual Border Routers (VBRs) are attached to a CEN instance.
- Hangzhou data center is connected to the Hangzhou VPC through VPN Gateway.
- Guangzhou on-premises data center accesses Alibaba Cloud through Smart Access Gateway. The Cloud Connect Network (CCN) to which the Smart Access Gateway belongs is attached to the CEN instance.

- The VPCs in the China (Beijing), China (Shanghai), China (Shenzhen), and China (Hangzhou) regions are attached to the CEN instance.



IP address planning

When you build a hybrid cloud, you must ensure that no CIDR blocks conflict with each other. The CIDR blocks used in this example are as follows:

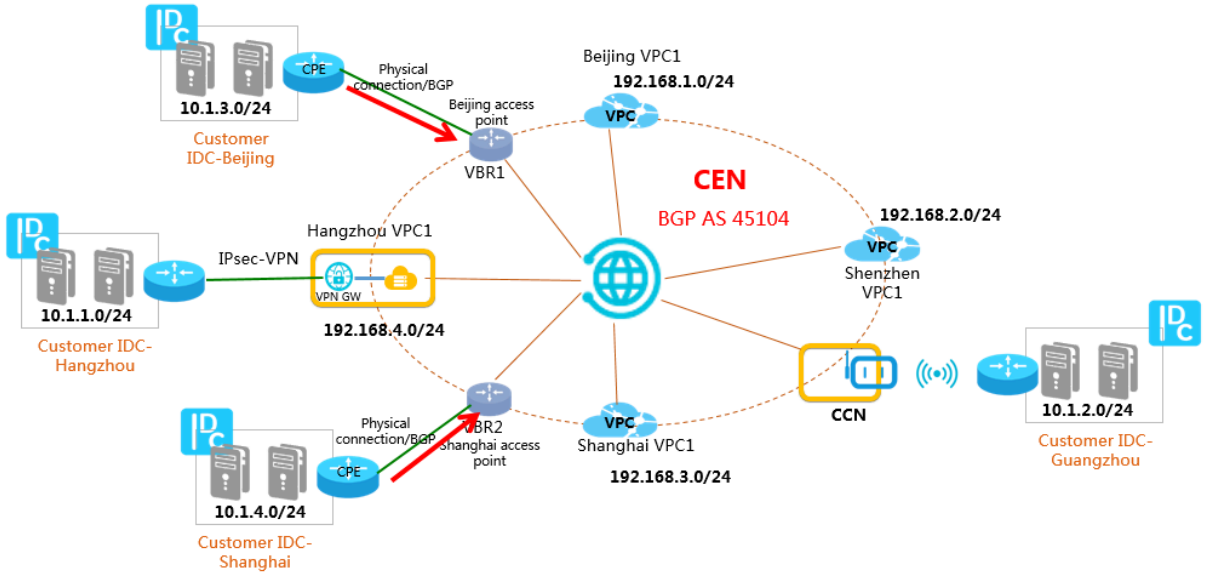
Network	CIDR block
Hangzhou data center	10.1.1.0/24
Guangzhou data center	10.1.2.0/24
Beijing data center	10.1.3.0/24
Shanghai data center	10.1.4.0/24
Beijing VPC	192.168.1.0/24
Shenzhen VPC	192.168.2.0/24
Shanghai VPC	192.168.3.0/24
Hangzhou VPC	192.168.4.0/24

Access methods

In this topic, on-premises data centers are connected to Alibaba Cloud in the following ways:

- Beijing and Shanghai data centers access Alibaba Cloud through physical connections.
- Hangzhou data center accesses Alibaba Cloud through VPN Gateway.
- Guangzhou data center accesses Alibaba Cloud through Smart Access Gateway.

Beijing and Shanghai data centers access Alibaba Cloud through physical connections



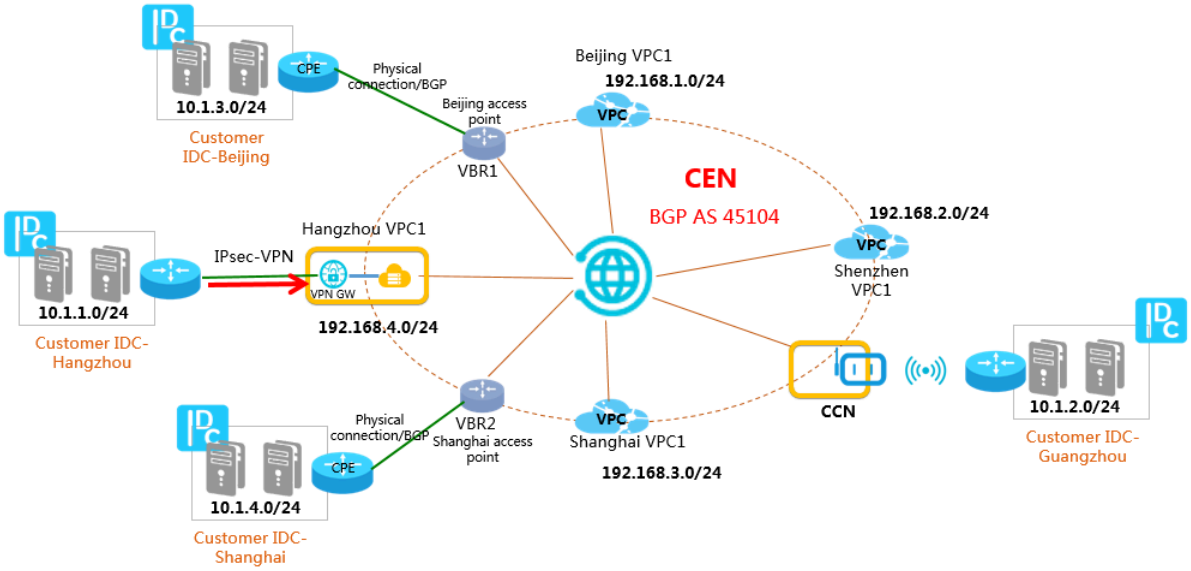
Configuration description:

1. Beijing and Shanghai data centers are connected to VBRs through physical connections, and each data center and the corresponding VBR are each other's BGP peer. For more information, see #unique_23.
2. The CPEs of Beijing and Shanghai data centers advertise the CIDR blocks of the data centers to 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 data center and the corresponding VBR become each other's BGP peer, the data center and the VBR can learn each other's routes.

Hangzhou data center accesses Alibaba Cloud through VPN Gateway



Configuration description:

1. Hangzhou data center accesses the Hangzhou VPC through VPN Gateway. For more information, see #unique_19.
2. An IPsec-VPN connection is established between the on-premises data center and the VPN Gateway, and contributing routes or default routes pointing to Alibaba Cloud are configured.

   Contributing routes:

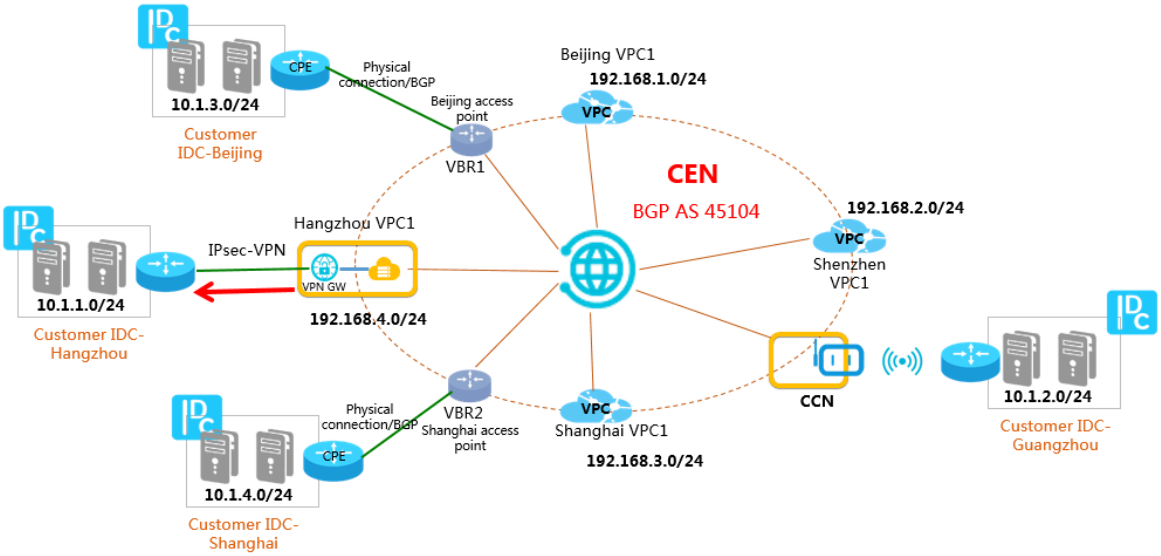
Destination CIDR block	Next hop
10.1.2.0/24	VPN Gateway
10.1.3.0/24	VPN Gateway
10.1.4.0/24	VPN Gateway
192.168.1.0/24	VPN Gateway
192.168.2.0/24	VPN Gateway
192.168.3.0/24	VPN Gateway
192.168.4.0/24	VPN Gateway

   Default route:

Destination CIDR block	Next hop
0.0.0.0/0	VPN Gateway

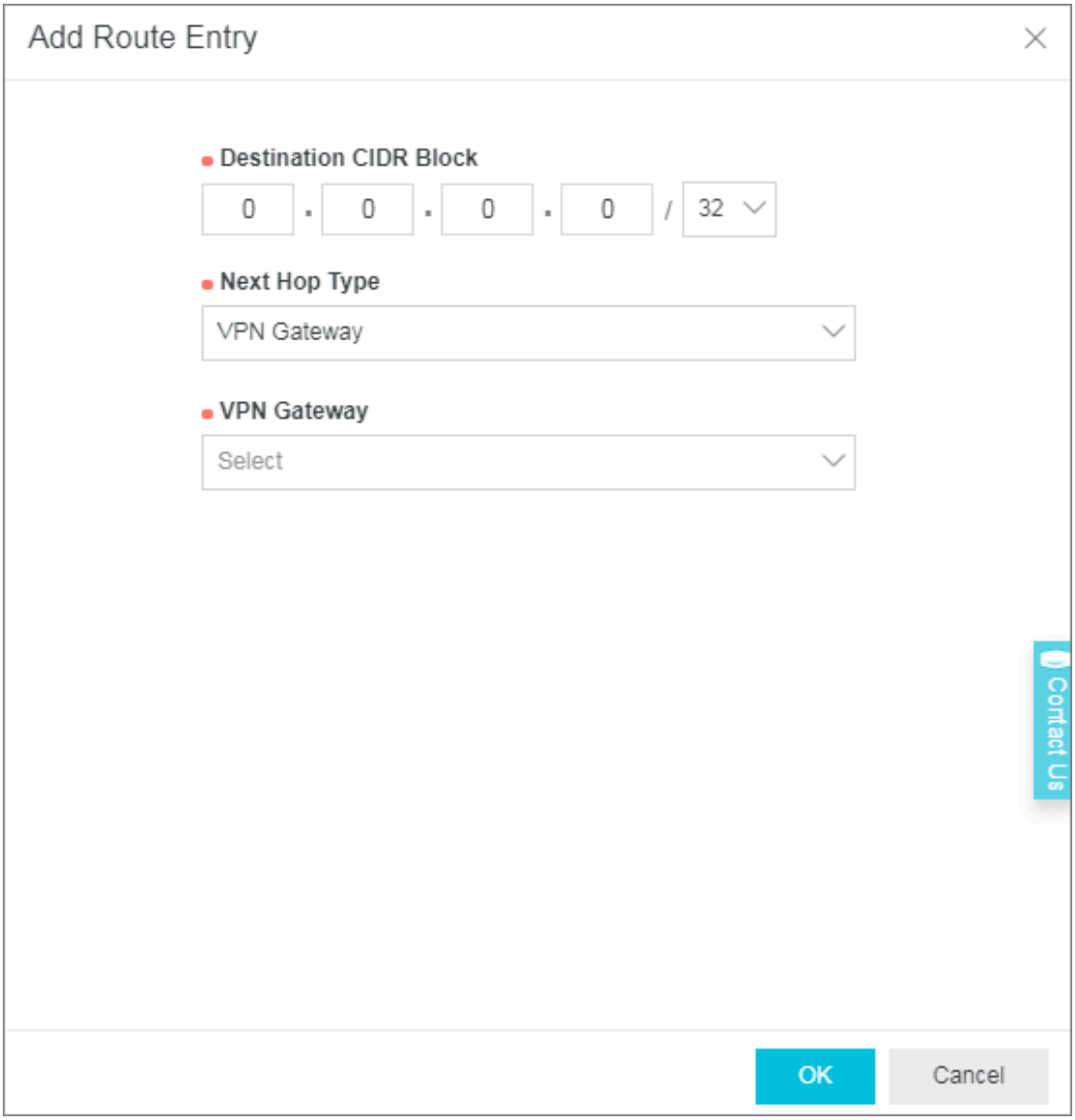
3. To enable the communication between the on-premises data center and the networks attached to CEN, you must configure a route entry pointing to the data

center (VPN Gateway) in the VPC connected to the VPN Gateway and publish the route to CEN.

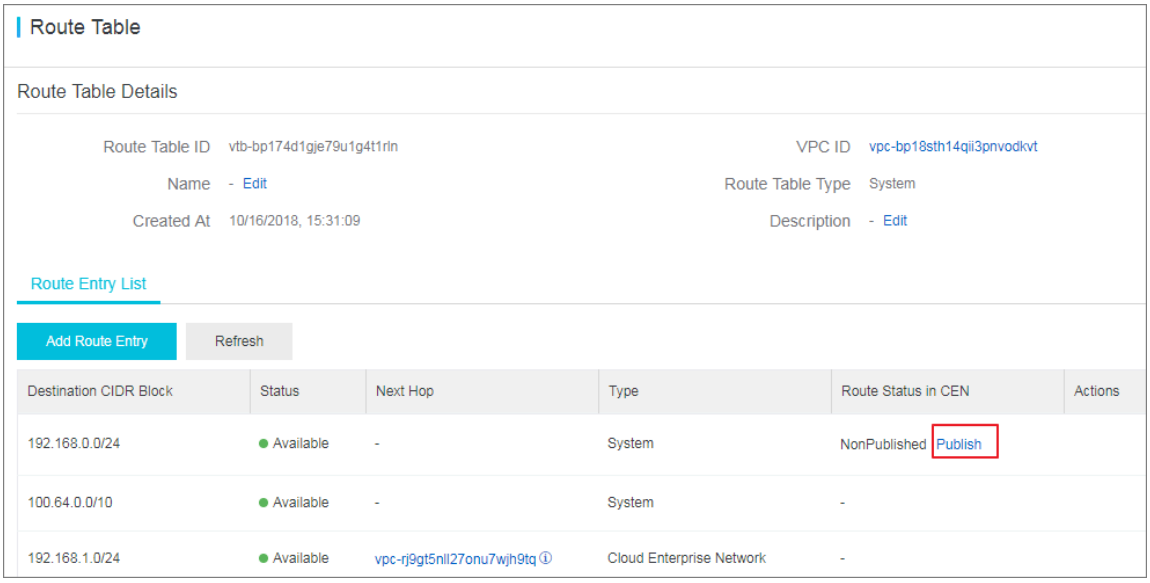


To configure the route, follow these steps:

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

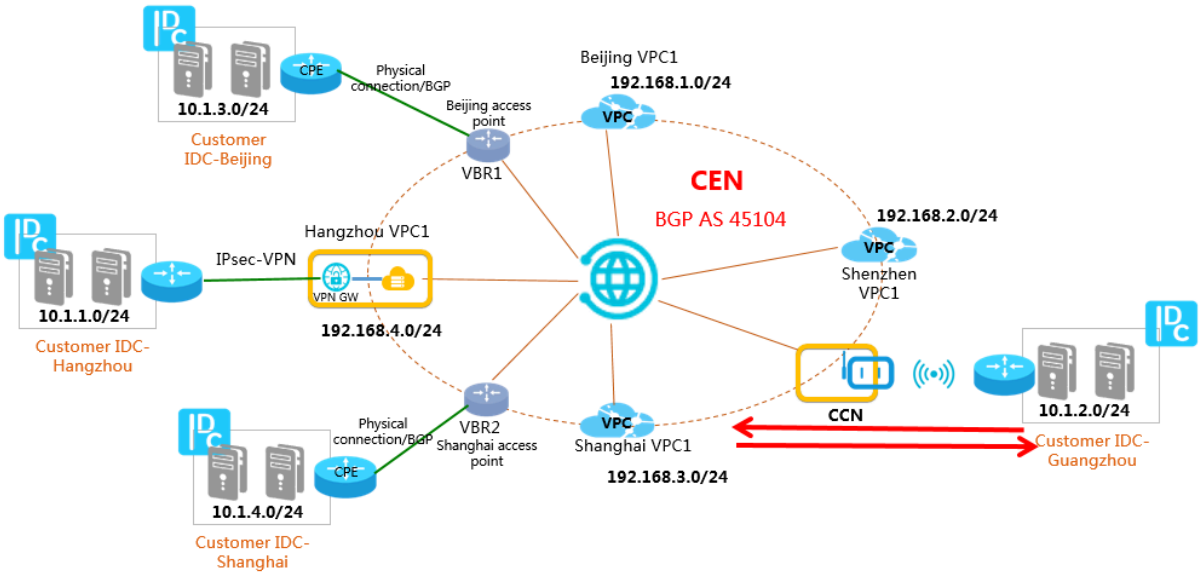


b. Publish the route to CEN from the VPC.



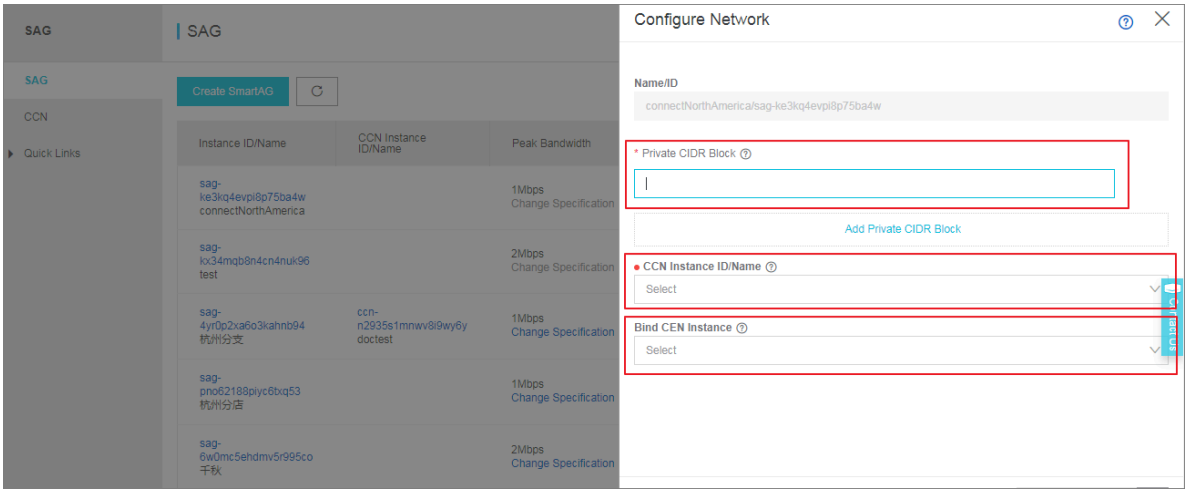
Through the preceding steps, all networks in the CEN instance can learn the route pointing to the data center and the data center can communicate with any network in the CEN instance. For more information, see #unique_24.

Guangzhou data center accesses Alibaba Cloud through Smart Access Gateway



Configuration description:

1. In the Smart Access Gateway console, configure the CIDR block of Guangzhou data center connected to Smart Access Gateway as a private CIDR block.
2. Attach the CCN associated with the Smart Access Gateway to the CEN instance. Then Guangzhou data center can communicate with any network in the CEN instance.

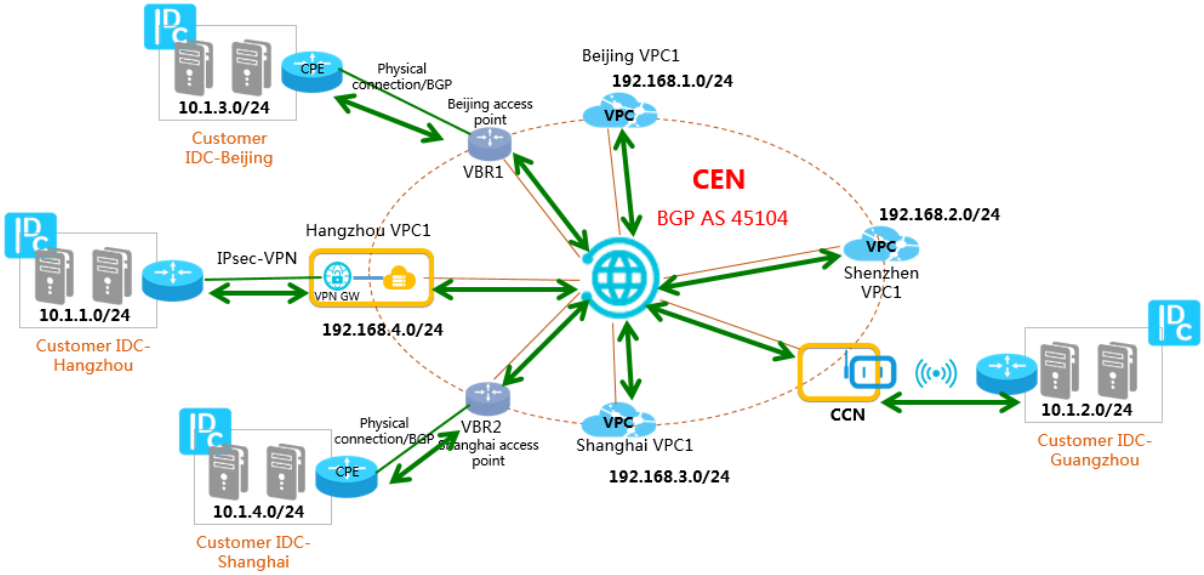


Interconnection of on-premises data centers and networks

Through the preceding ways:

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

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 6-1: 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 6-2: 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 6-3: Shenzhen VPC

Destination CIDR block	Next hop	Route type
10.1.1.0/24	Hangzhou VPC	CEN route
10.1.2.0/24	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

7 Route map solutions

7.1 Stop the communication between a VPC and other networks attached to a CEN instance

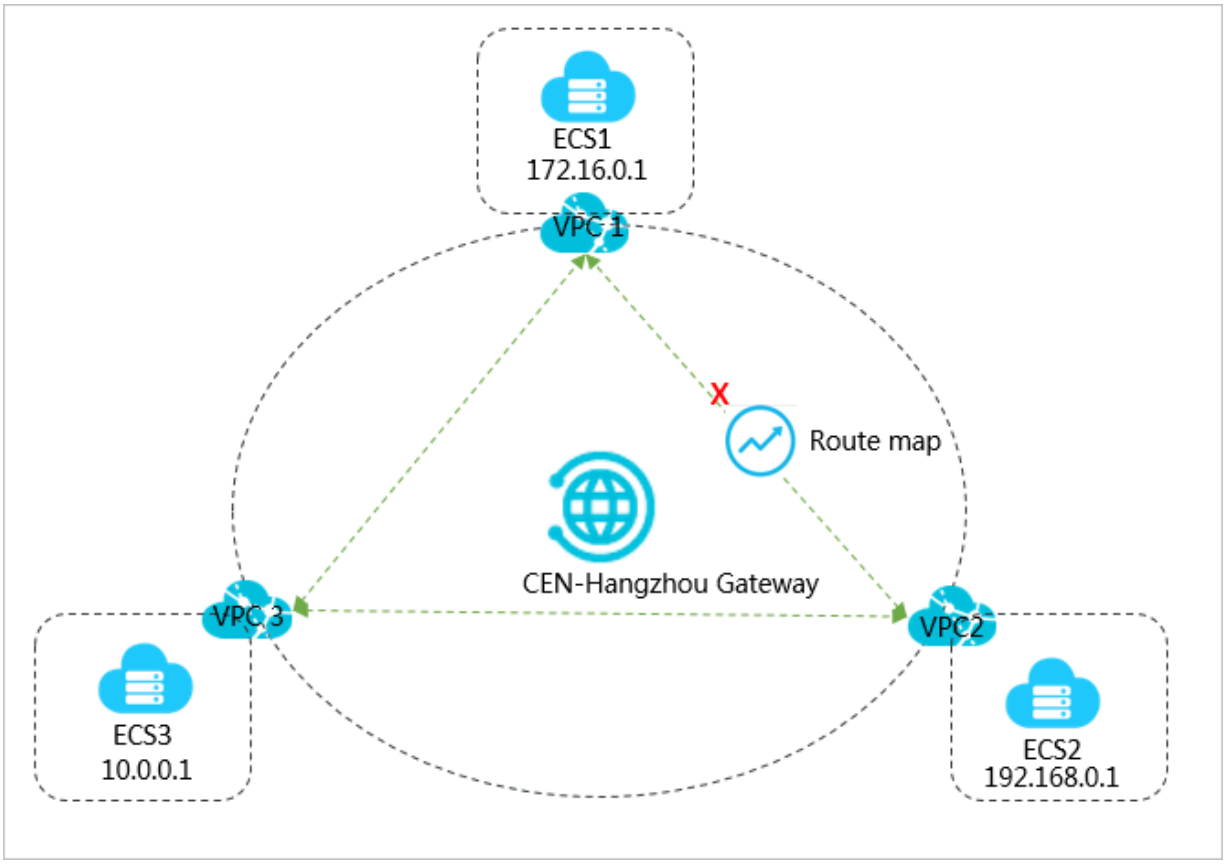
This topic describes how to use route maps to stop the communication between a VPC and other networks (VPCs, VBRs, or CCNs) that are attached to the same Cloud Enterprise Network (CEN) instance.

Prerequisites

A CEN instance is created and the required networks are attached to the CEN instance. For more information, see #unique_27 and #unique_28.

Context

VPCs can communicate with VPCs, Virtual Border Routers (VBRs), and Cloud Connect Networks (CCNs) that are attached to the same CEN instance by default. However, you may need to block the communication between two VPCs, or between a VPC and a VBR or CCN. In this topic, two VPCs are used as an example to show you how to stop the communication between two VPCs by using route maps.



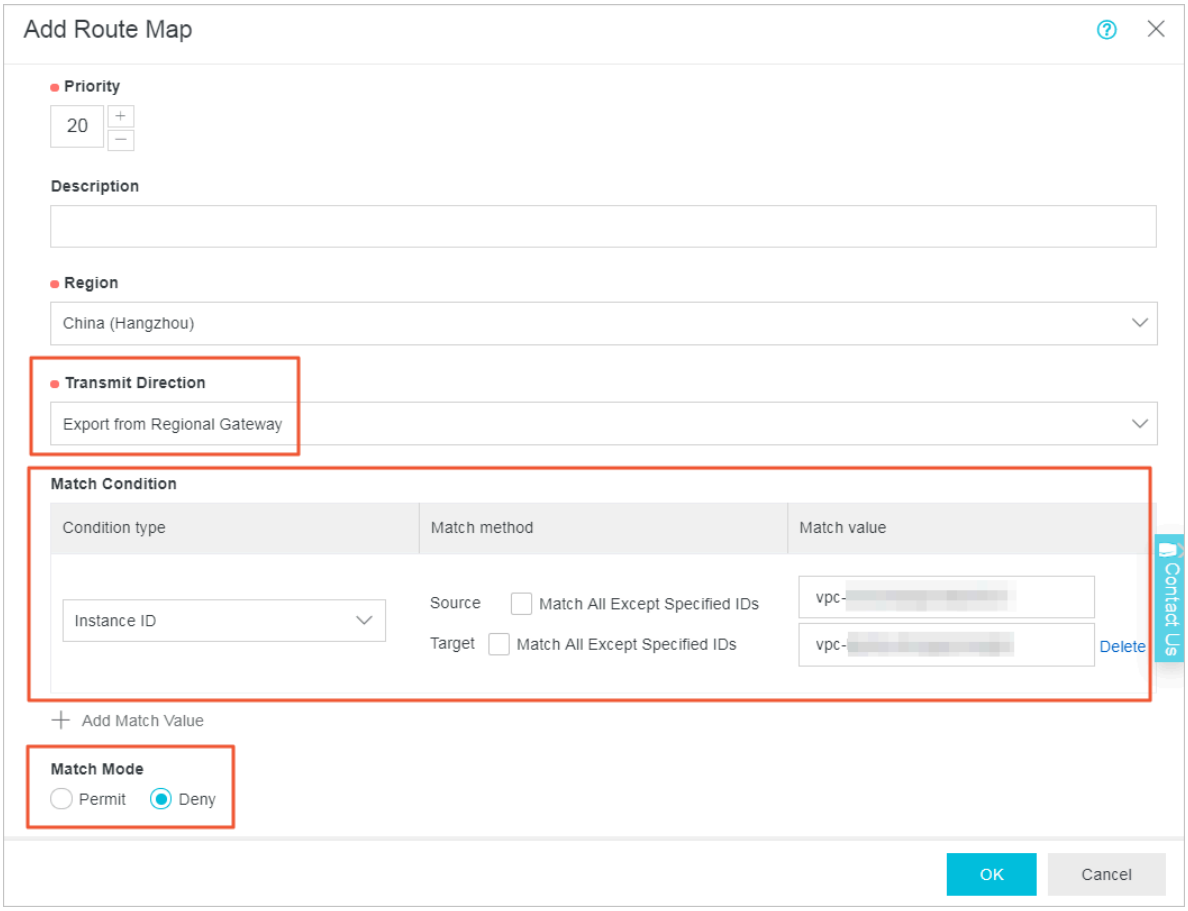
As shown in the preceding figure, VPC1, VPC2, and VPC3 are attached to CEN. By default, VPC1, VPC2, and VPC3 are all connected and can communicate with each other. By using route maps, you can block the communication between VPC1 and VPC2 while VPC1 and VPC2 can still communicate with VPC3.

Step 1: Set a route map to deny access from VPC1 to VPC2

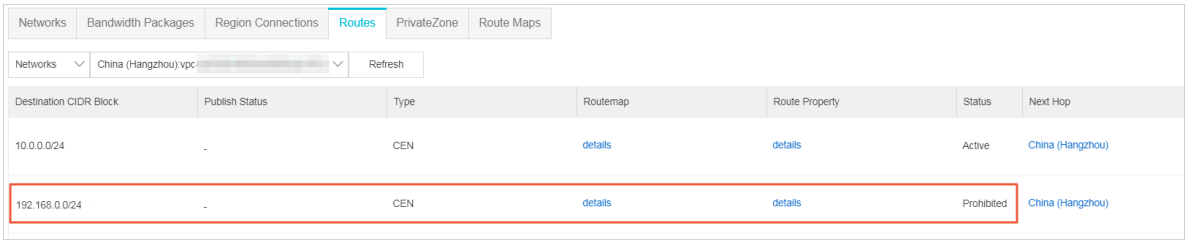
To set a route map to deny access from VPC1 to VPC2, follow these steps:

1. Log on to the CEN console.
2. In the left-side navigation pane, click Instances.
3. On the Instances page, find the target CEN instance and click Manage in the Actions column.
4. On the CEN page, click the Route Maps tab and then click Add Route Map.

5. In the Add Route Map dialog box, configure the route map according to the following information and then click OK.
   - Priority: Enter the priority of the route map. A smaller number represents a higher priority. In this example, enter 20.
   - Region: Select the region to which the route map is applied. In this example, select China (Hangzhou).
   - Transmit Direction: Select the direction of the route map. In this example, select Export from Regional Gateway.
   - Match Condition: Set the matching conditions of the route map. In this example, add a matching condition and set the source instance ID to the ID of VPC2 and the target instance ID to the ID of VPC1.
   - Match Mode: Select the matching mode of the route map. In this example, select Deny.



After you add the route map, you can view the route that denies access from VPC1 to VPC2 on the Routes tab.

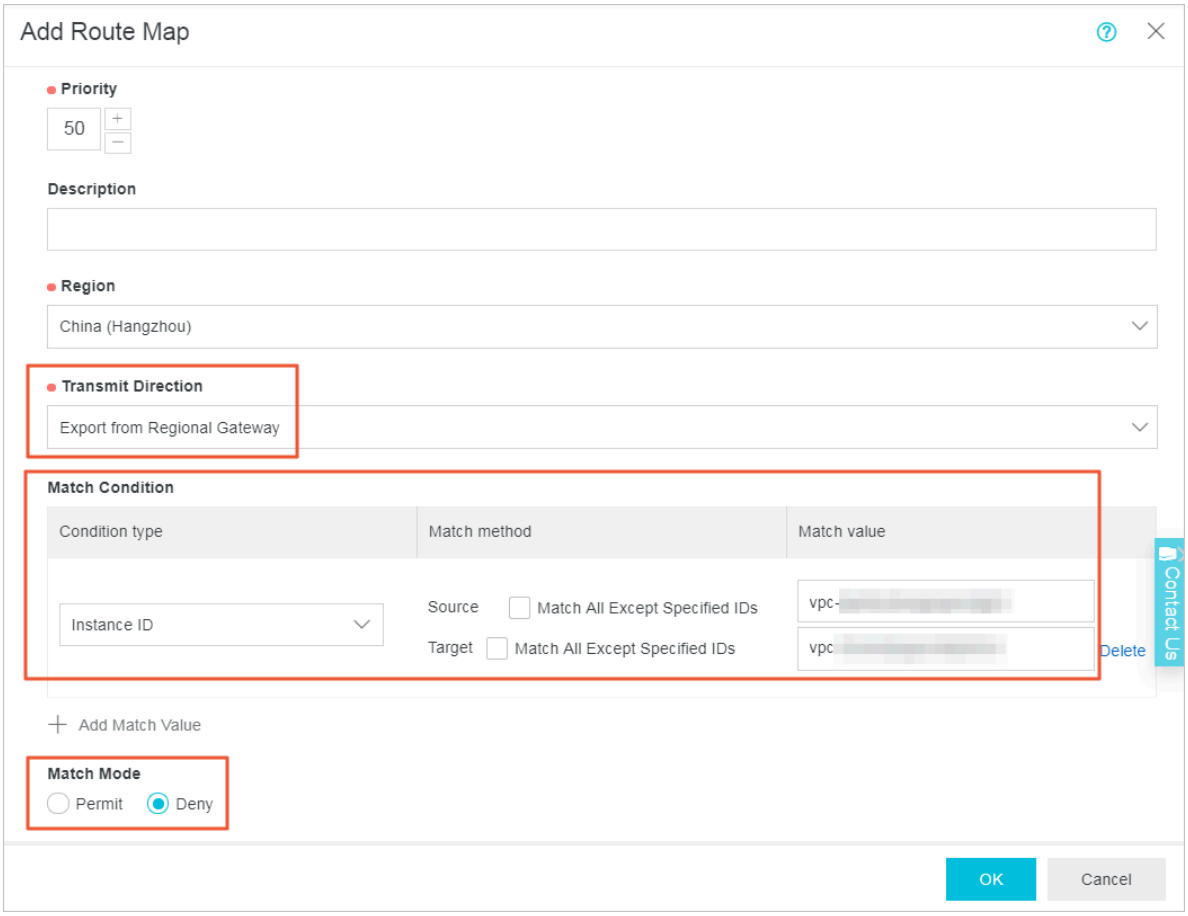


Step 2: Set a route map to deny access from VPC2 to VPC1

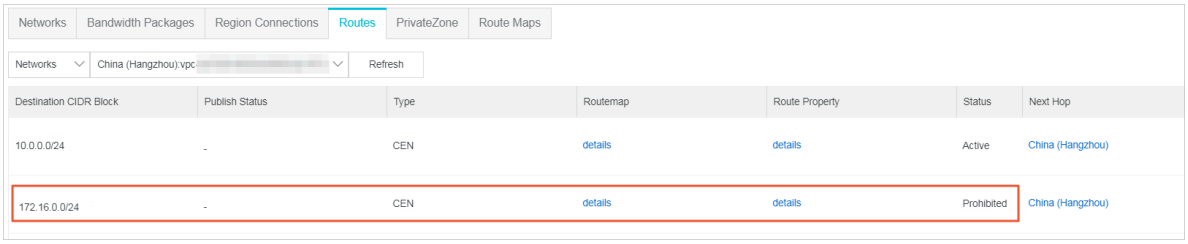
To set a route map to deny access from VPC2 to VPC1, follow these steps:

1. In the left-side navigation pane, click Instances.
2. On the Instances page, find the target CEN instance and click Manage in the Actions column.
3. On the CEN page, click the Route Maps tab and then click Add Route Map.

4. In the Add Route Map dialog box, configure the route map according to the following information and then click OK.
   - Priority: Enter the priority of the route map. A smaller number represents a higher priority. In this example, enter 50.
   - Region: Select the region to which the route map is applied. In this example, select China (Hangzhou).
   - Transmit Direction: Select the direction of the route map. In this example, select Export from Regional Gateway.
   - Match Condition: Set the matching conditions of the route map. In this example, add a matching condition and set the source instance ID to the ID of VPC1 and the target instance ID to the ID of VPC2.
   - Match Mode: Select the matching mode of the route map. In this example, select Deny.



After you add the route map, you can view the route that denies access from VPC2 to VPC1 on the Routes tab.



Step 3: Test the network connectivity

To test the network connectivity between VPC1 and VPC2, follow these steps:

1. Log on to the ECS instance ECS1 in VPC1.
2. Use the `ping` command to `ping` the IP address of the ECS instance ECS2 in VPC2.

   The output shows that ECS1 cannot access ECS2, which means VPC1 cannot access VPC2.

```
[root@                    ~]# ping 192.168.0.1
PING 192.168.0.1 (192.168.0.1) 56(84) bytes of data.



^C
--- 192.168.0.1 ping statistics ---
17 packets transmitted, 0 received, 100% packet loss, time 15999ms
```

3. Log on to ECS2 in VPC2.
4. Use the `ping` command to `ping` the IP address of ECS1 in VPC1.

   The output shows that ECS2 cannot access ECS1, which means VPC2 cannot access VPC1.

```
[root@                    ~]# ping 172.16.0.1
PING 172.16.0.1 (172.16.0.1) 56(84) bytes of data.



^C
--- 172.16.0.1 ping statistics ---
6 packets transmitted, 0 received, 100% packet loss, time 5000ms
```

To test the network connectivity between VPC1 and VPC3, follow these steps:

1. Log on to ECS1 in VPC1.

2. Use the `ping` command to `ping` the IP address of ECS3 in VPC3.

   The output shows that ECS1 can access ECS3, which means VPC1 can access VPC3.

```
C:\Users\Administrator>ping 10.0.0.1

Pinging 10.0.0.1 with 32 bytes of data:
Reply from 10.0.0.1: bytes=32 time<1ms TTL=128
Reply from 10.0.0.1: bytes=32 time<1ms TTL=128
Reply from 10.0.0.1: bytes=32 time<1ms TTL=128
Reply from 10.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 10.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

3. Log on to ECS3 in VPC3.
4. Use the `ping` command to `ping` the IP address of ECS1 in VPC1.

   The output shows that ECS3 can access ECS1, which means VPC3 can access VPC1.

```
C:\Users\Administrator>ping 172.16.0.1

Pinging 172.16.0.1 with 32 bytes of data:
Reply from 172.16.0.1: bytes=32 time<1ms TTL=128
Reply from 172.16.0.1: bytes=32 time<1ms TTL=128
Reply from 172.16.0.1: bytes=32 time<1ms TTL=128
Reply from 172.16.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 172.16.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

To test the network connectivity between VPC2 and VPC3, follow these steps:

1. Log on to ECS2 in VPC2.

2. Use the `ping` command to `ping` the IP address of ECS3 in VPC3.

   The output shows that ECS2 can access ECS3, which means VPC2 can access VPC3.

```
C:\Users\Administrator>ping 10.0.0.1

Pinging 10.0.0.1 with 32 bytes of data:
Reply from 10.0.0.1: bytes=32 time<1ms TTL=128
Reply from 10.0.0.1: bytes=32 time<1ms TTL=128
Reply from 10.0.0.1: bytes=32 time<1ms TTL=128
Reply from 10.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 10.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

3. Log on to ECS3 in VPC3.
4. Use the `ping` command to `ping` the IP address of ECS2 in VPC2.

   The output shows that ECS3 can access ECS2, which means VPC3 can access VPC2.

```
C:\Users\Administrator>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:
Reply from 192.168.0.1: bytes=32 time<1ms TTL=128
Reply from 192.168.0.1: bytes=32 time<1ms TTL=128
Reply from 192.168.0.1: bytes=32 time<1ms TTL=128
Reply from 192.168.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

7.2 Stop the communication between a VPC and a CIDR block in CEN

The topic describes how to use route maps to stop the communication between a VPC and a CIDR block in Cloud Enterprise Network (CEN).

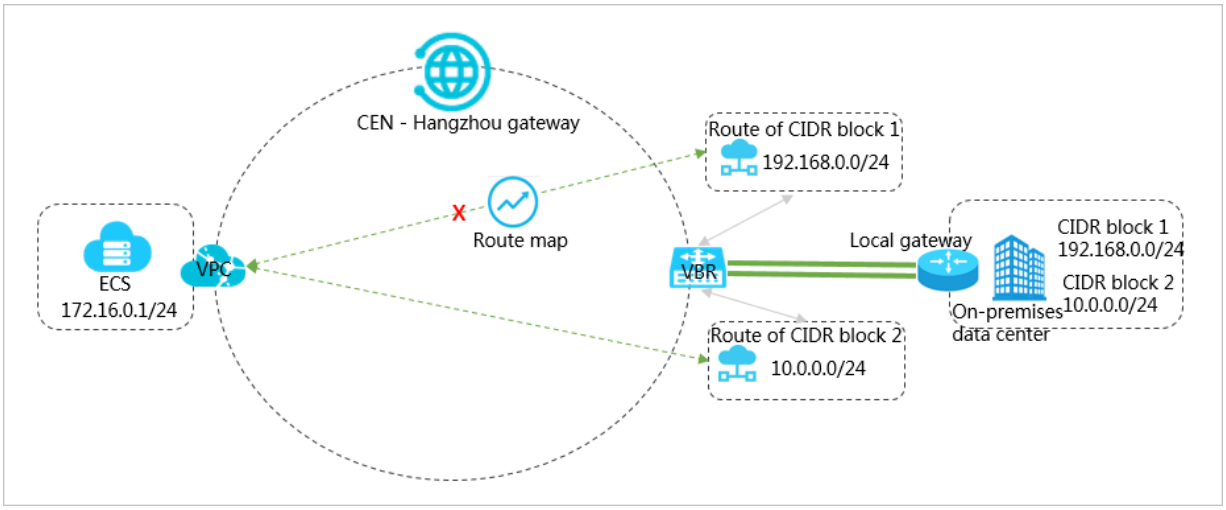
Prerequisites

Before you add a route map, make sure that the following conditions are met:

- The on-premises data center is connected to Alibaba cloud through a leased line. For more information, see #unique_30 and #unique_31.
- A CEN instance is created and the required networks are attached to the CEN instance. For more information, see #unique_27 and #unique_28.

Context

VPCs can communicate with the CIDR blocks of VPCs, Virtual Border Routers (VBRs), and Cloud Connect Networks (CCNs) that are attached to the same CEN instance by default. However, you may need to stop a VPC from communicating with a certain CIDR block of a VPC, VBR or CCN.



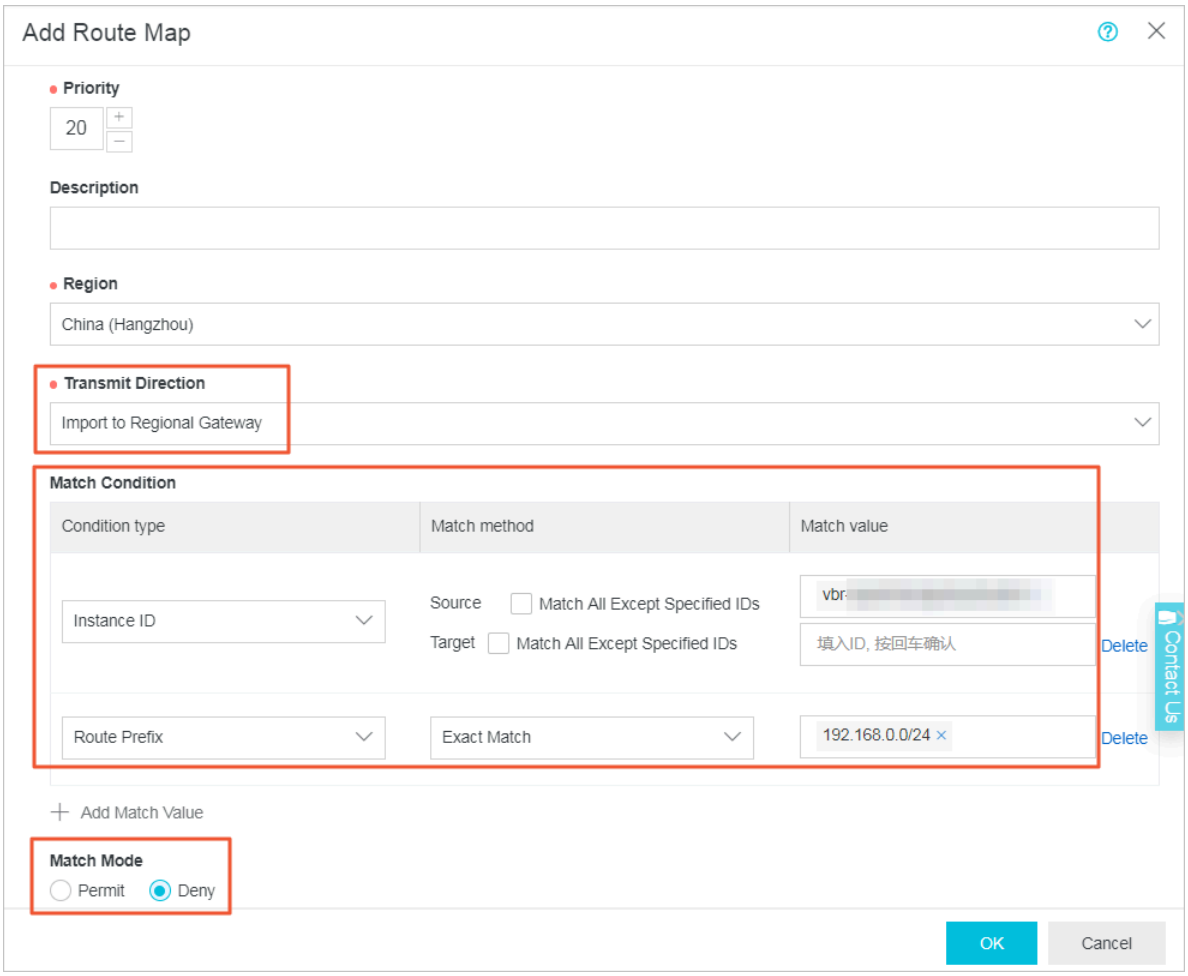
As shown in the preceding figure, a VPC and a VBR are attached to CEN. The VBR learns the routes pointing to CIDR block 1 and CIDR block 2 of the on-premises data center through BGP. By default, the VPC can communicate with CIDR block 1 and CIDR block 2 of the on-premises data center, too. If you want to stop the VPC from communicating with CIDR block 1, you can use route maps. By using route maps, you can stop the VPC from communicating with CIDR block 1 while the VPC can still communicate with CIDR block 2.

Step 1: Set a route map to deny the route of CIDR block 1

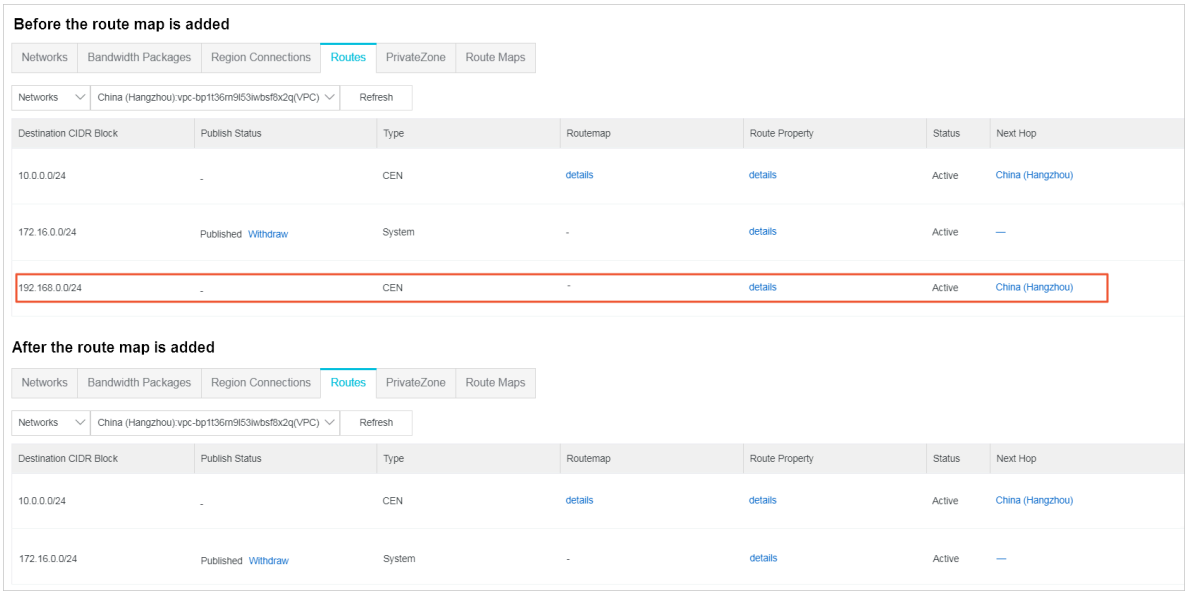
To set a route map to deny the route of CIDR block 1, follow these steps:

1. Log on to the CEN console.
2. In the left-side navigation pane, click Instances.
3. On the Instances page, find the target CEN instance and click Manage in the Actions column.
4. On the CEN page, click the Route Maps tab and then click Add Route Map.

5. On the Add Route Map page, configure the route map according to the following information and then click OK.
   - Priority: Enter the priority of the route map. A smaller number represents a higher priority. In this example, enter 20.
   - Region: Select the region to which the route map is applied. In this example, select China (Hangzhou).
   - Transmit Direction: Select the direction of the route map. In this example, select Import to Regional Gateway.
   - Match Condition: Set the matching conditions of the route map. In this example, add two matching conditions:
     - Source Instance ID: Enter the instance ID of the VBR.
     - Route Prefix: Enter 192.168.0.0/24. Select Exact Match for Condition Type.
   - Match Mode: Select the matching mode of the route map. In this example, select Deny.



After you add the route map, you can see that the route pointing to CIDR block 1, 192.168.0.0/24, is deleted from the VPC on the Routes tab.



Step 2: Test the network connectivity

To test the network connectivity between the VPC and CIDR block 1 of the on-premises data center, follow these steps:

1. Log on to an ECS instance in the VPC.
2. Use the `ping` command to `ping` the IP address of CIDR block 1.

   The output shows that the ECS instance in the VPC cannot access the IP address of CIDR block 1.

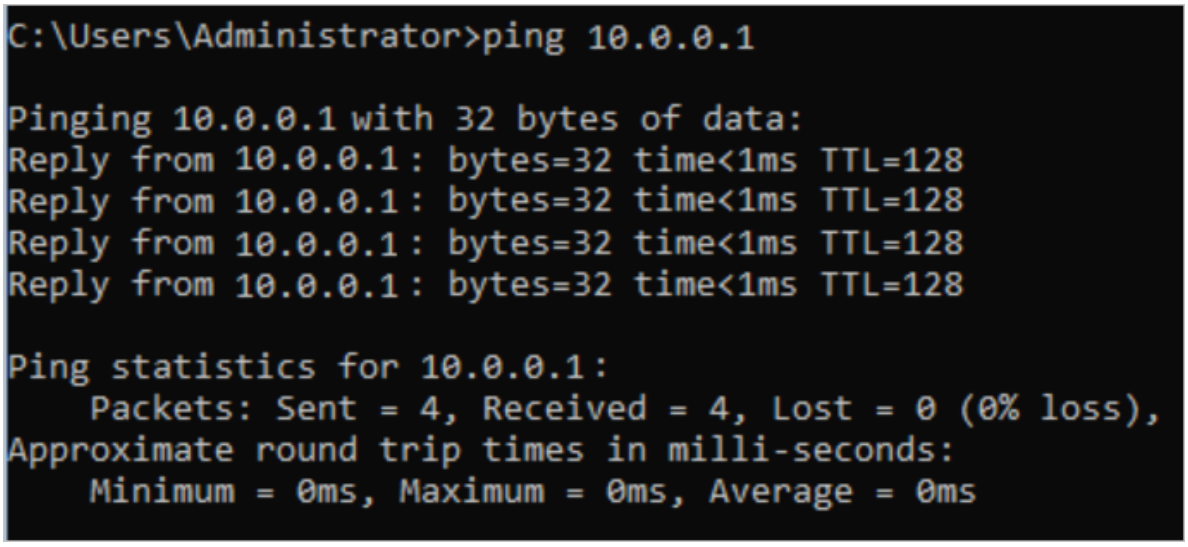
```
[root@                    ~]# ping 192.168.0.1
PING 192.168.0.1 (192.168.0.1) 56(84) bytes of data.



^C
--- 192.168.0.1 ping statistics ---
17 packets transmitted, 0 received, 100% packet loss, time 15999ms
```

To test the network connectivity between the VPC and CIDR block 2 of the on-premises data center, follow these steps:

1. Log on to the ECS instance in the VPC.

2. Use the `ping` command to `ping` the IP address of CIDR block 2.

   The output shows that the ECS instance in the VPC can access the IP address of CIDR block 2.



7.3 Connect two on-premises data centers through CEN

This topic describes how to connect two on-premises data centers by using route maps of Cloud Enterprise Network (CEN).

Prerequisites

Before you configure a route map, make sure that the following conditions are met:

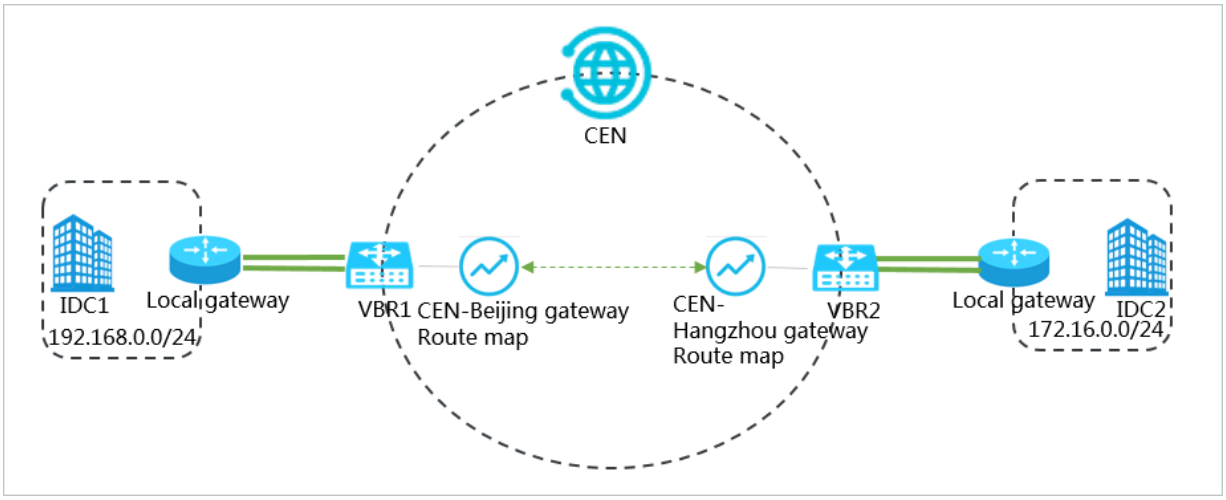
- The on-premises data centers are connected to Alibaba Cloud through a leased line. For more information, see #unique_30 and #unique_31.
- A CEN instance is created and the required networks are attached to the CEN instance. For more information, see #unique_27 and #unique_28.
- A bandwidth package is purchased and cross-region connection bandwidth is set. For more information, see #unique_33 and #unique_34.

Context

By default, CEN adds a route map with the priority of 5000 and the matching mode of DENY to the regional gateway. This route map stops Virtual Border Routers (VBRs) and Cloud Connect Networks (CCNs) from communicating with other VBRs and CCNs attached to the CEN instance. However, you may need to connect two VBRs or two CCNs attached to the CEN instance.

Notice:

Deletion of default route maps may cause a routing loop. Therefore, we recommend that you exercise caution when you delete default route maps.



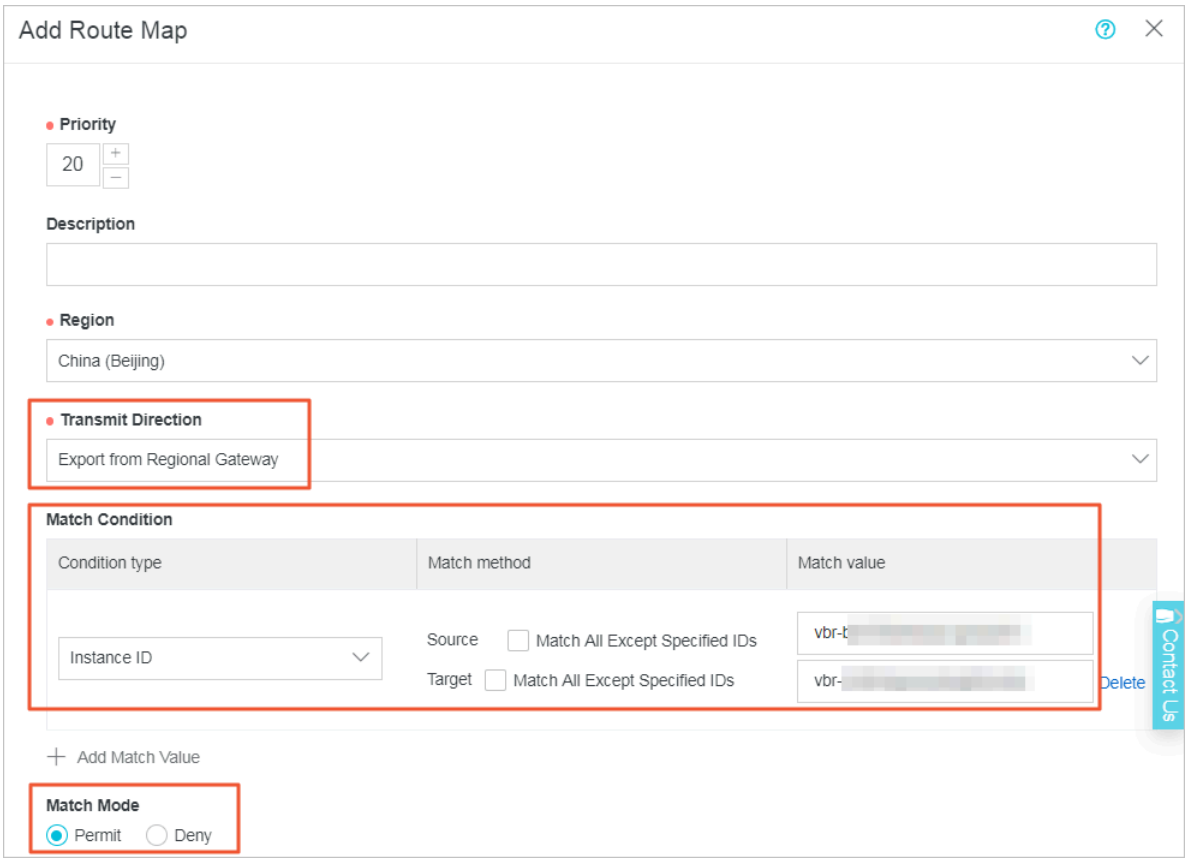
As shown in the preceding figure, the on-premises data center IDC1 is located in Beijing and connected to Alibaba Cloud through VBR1. The on-premises data center IDC2 is located in Hangzhou and connected to Alibaba Cloud through VBR2 . VBR1 and VBR2 are attached to a CEN instance. By default, IDC1 and IDC2 are not connected. If you want to connect IDC1 with IDC2, you can use route maps.

Step 1: Set a route map that allows IDC1 to access IDC2

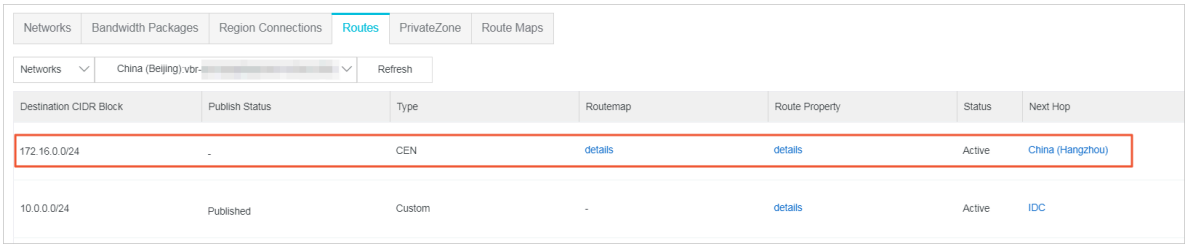
To set a route map that allows IDC1 to access IDC2, follow these steps:

1. Log on to the CEN console.
2. In the left-side navigation pane, click Instances.
3. On the Instances page, find the target CEN instance and click Manage in the Actions column.
4. On the CEN page, click the Route Maps tab and then click Add Route Map.

5. In the Add Route Map dialog box, configure the route map according to the following information and then click OK.
   - Priority: Enter the priority of the route map. A smaller number represents a higher priority. In this example, enter 20.
   - Region: Select the region to which the route map is applied. In this example, select China (Beijing).
   - Transmit Direction: Select the direction of the route map. In this example, select Export from Regional Gateway.
   - Match Condition: Set the matching conditions of the route map. In this example, add two matching conditions:
     - Source Instance ID: Enter the instance ID of VBR2.
     - Target Instance ID: Enter the instance ID of VBR1.
   - Match Mode: Select the matching mode of the route map. In this example, select Permit.



After you add the route map, you can view the route that allows IDC1 to access IDC2 on the Routes tab.

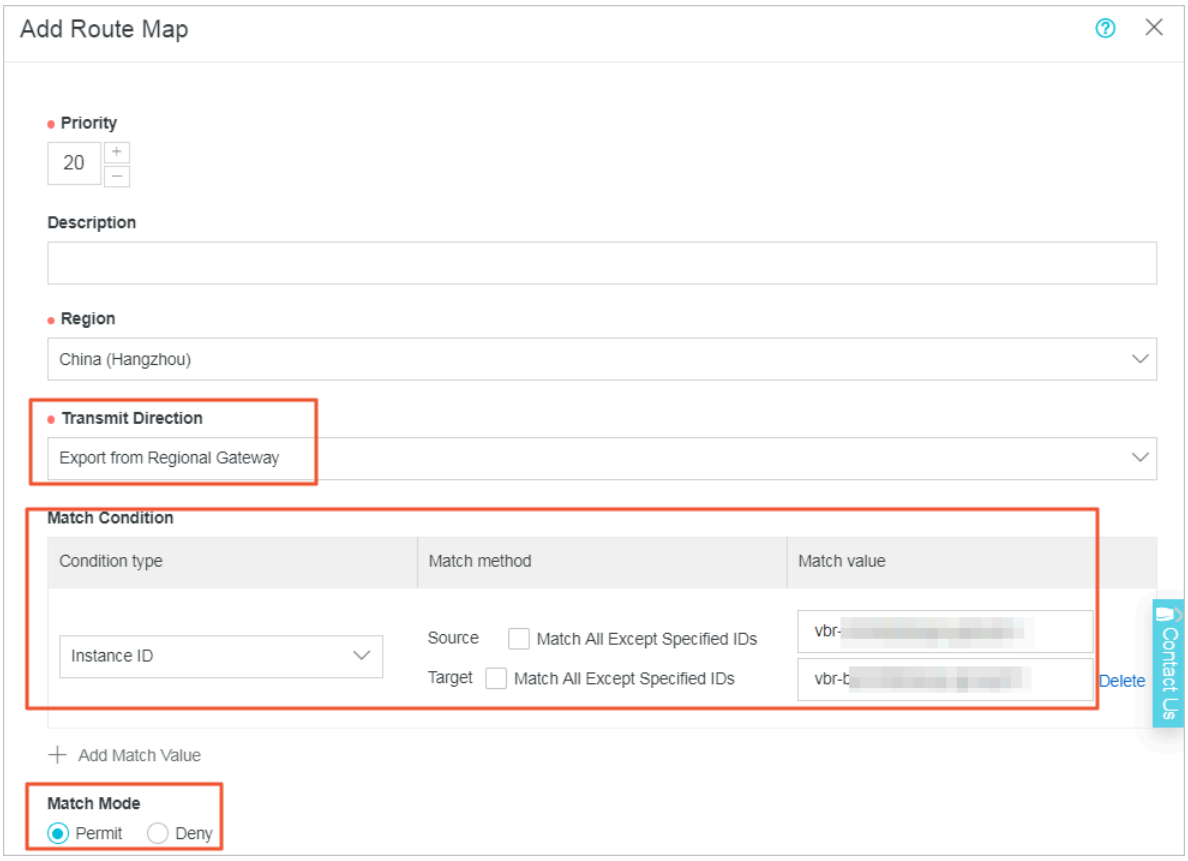


Step 2: Set a route map that allows IDC2 to access IDC1

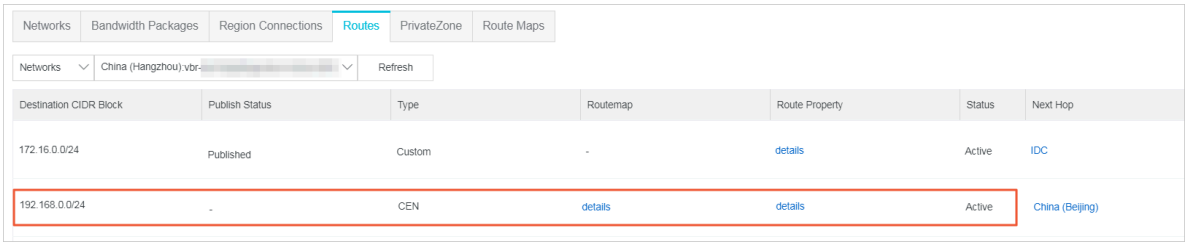
To set a route map that allows IDC2 to access IDC1, follow these steps:

1. In the left-side navigation pane, click Instances.
2. On the Instances page, find the target CEN instance and click Manage in the Actions column.
3. On the CEN page, click the Route Maps tab, and then click Add Route Map.

4. In the Add Route Map dialog box, configure the route map according to the following information and then click OK.
   - Priority: Enter the priority of the route map. A smaller number represents a higher priority. In this example, enter 20.
   - Region: Select the region to which the route map is applied. In this example, select China (Hangzhou).
   - Transmit Direction: Select the direction of the route map. In this example, select Export from Regional Gateway.
   - Match Condition: Set the matching conditions of the route map. In this example, add two matching conditions:
     - Source Instance ID: Enter the instance ID of VBR1.
     - Target Instance ID: Enter the instance ID of VBR2.
   - Match Mode: Select the matching mode of the route map. In this example, select Permit.



After you add the route map, you can view the route that allows IDC2 to access IDC1 on the Routes tab.

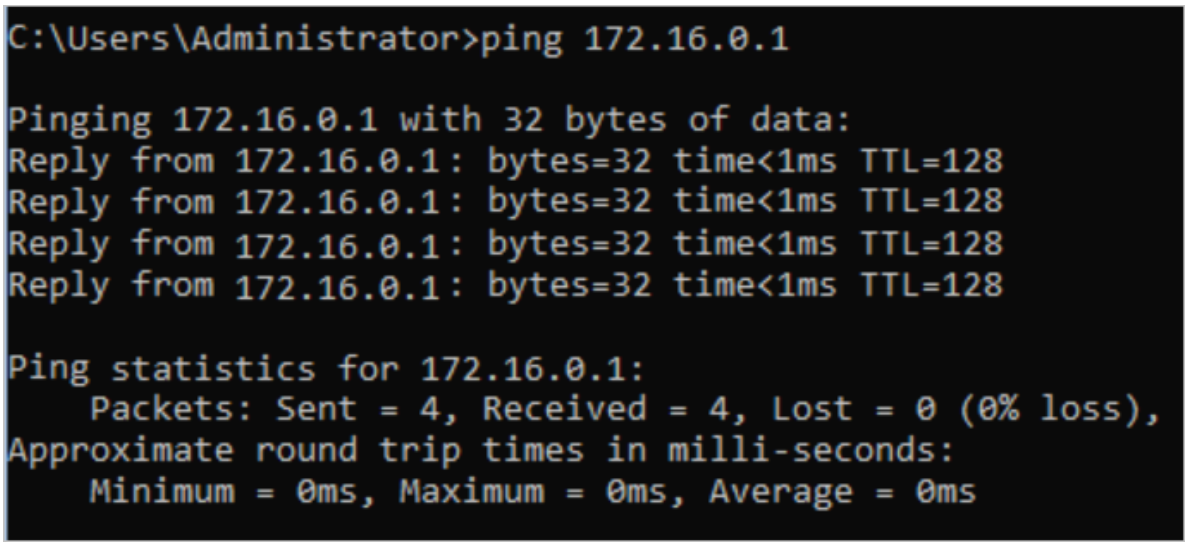


Step 3: Test the network connectivity

To test the network connectivity between IDC1 and IDC2, follow these steps.

1. Open the command prompt of the PC at the on-premises data center IDC1.
2. Use the `ping` command to `ping` the IP address of the PC at the on-premises data center IDC2..

   The output shows that the PC of IDC1 can access the PC of IDC2.



3. Open the command prompt of the PC of IDC2.

4. Use the `ping` command to `ping` the IP address of the PC of IDC1.

   The output shows that the PC of IDC2 can access the PC of IDC1.

```
C:\Users\Administrator>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:
Reply from 192.168.0.1 : bytes=32 time<1ms TTL=128
Reply from 192.168.0.1 : bytes=32 time<1ms TTL=128
Reply from 192.168.0.1 : bytes=32 time<1ms TTL=128
Reply from 192.168.0.1 : bytes=32 time<1ms TTL=128

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

7.4 Connect a branch to an on-premises data center by using route maps of CEN

This topic describes how to use the route maps of Cloud Enterprise Network (CEN) to connect a branch of a company and an on-premises data center.

Prerequisites

Before you configure a route map, make sure that the following conditions are met:

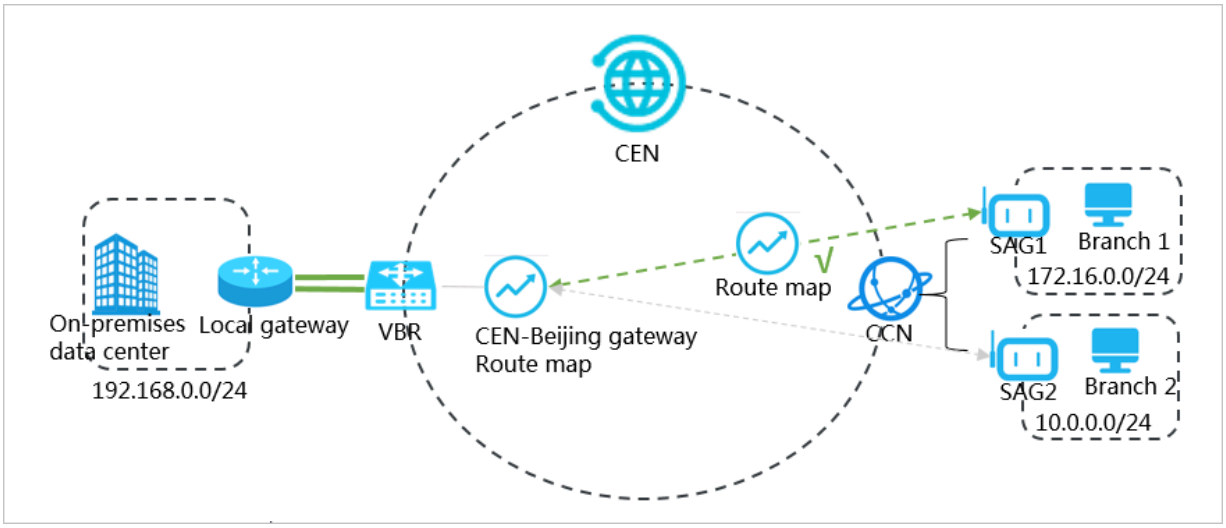
- A Cloud Connect Network (CCN) is created and the Smart Access Gateway (SAG) instances connected to the branches are attached to the CCN. For more information, see #unique_36 and #unique_37.
- A CEN instance is created and the networks that need to communicate with each other are attached to the CEN instance. For more information, see #unique_27 and #unique_28.
- A bandwidth package is purchased and cross-region connection bandwidth is set. For more information, see #unique_33 and #unique_34.

Context

By default, CEN adds a route map with the priority of 5000 and the matching mode of DENY to the regional gateway. This route map stops Virtual Border Routers (VBRs) and CCNs from communicating with other VBRs and CCNs attached to the CEN instance. However, you may need to connect two VBRs or two CCNs attached to the CEN instance.

Notice:

Deletion of default route maps may cause a routing loop. Therefore, we recommend that you exercise caution when you delete default route maps.



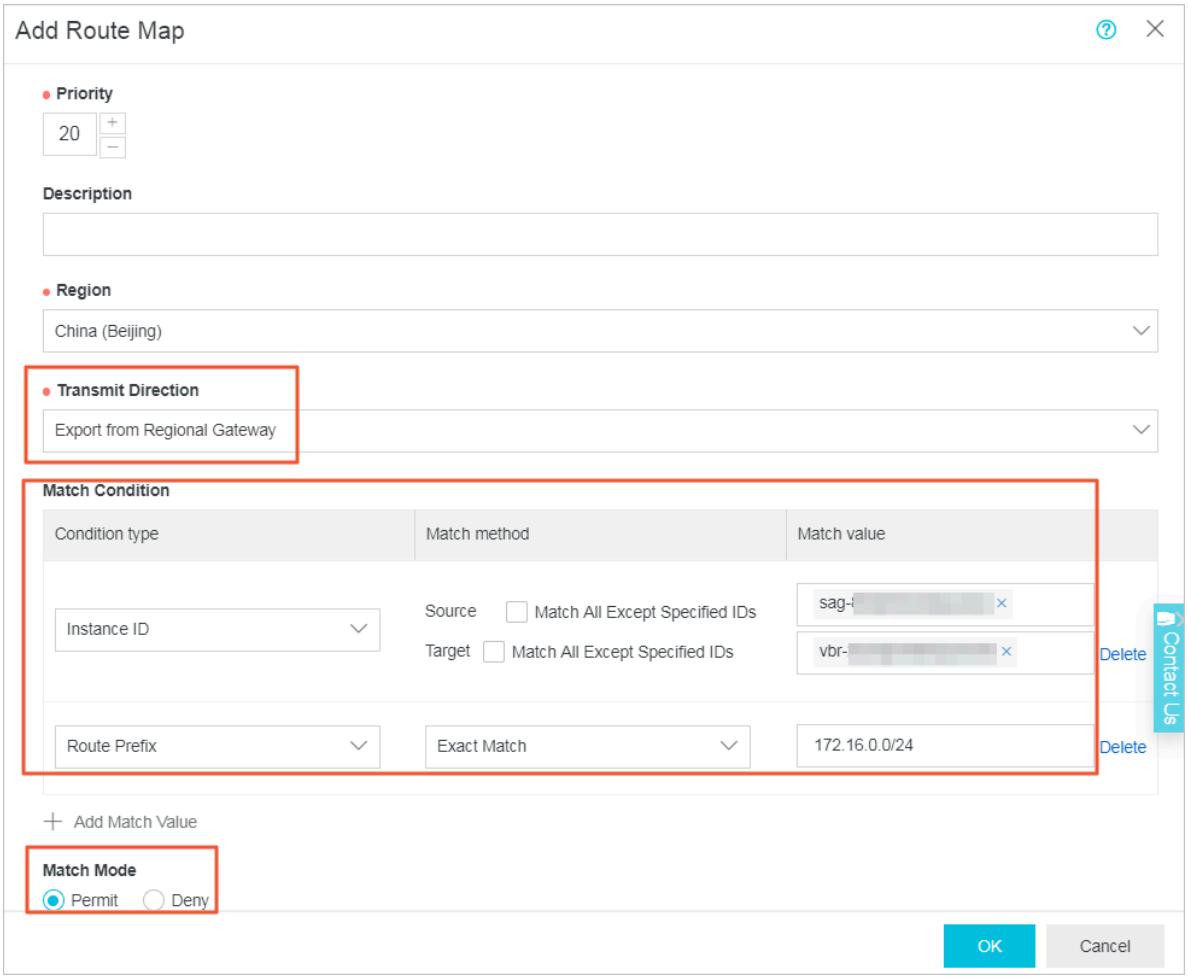
As shown in the preceding figure, the on-premises data center is located in Beijing and connected to Alibaba Cloud through a VBR. Branch 1 is located in Shanghai. Branch 2 is located in Hangzhou. The corresponding SAG instances SAG1 and SAG2 are attached to a CCN. The CCN and the VBR are attached to a CEN instance. By default, the on-premises data center cannot communicate with branch 1 or branch 2. If you want the on-premises data center to communicate with branch 1, you can use route maps.

Step 1: Set a route map that allows the on-premises data center to access branch 1

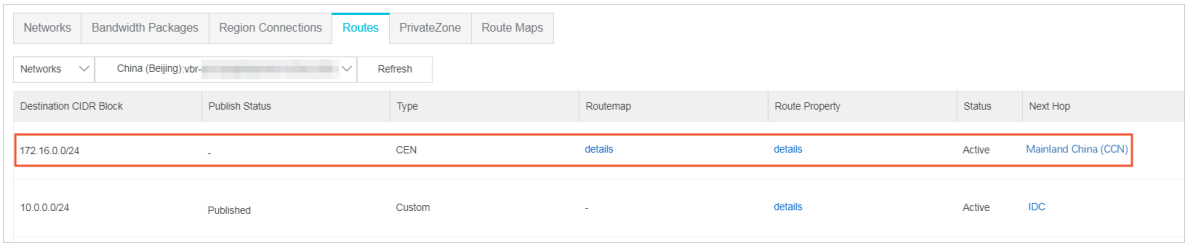
To set a route map that allows the on-premises data center to access branch 1, follow these steps:

1. Log on to the CEN console.
2. In the left-side navigation pane, click Instances.
3. On the Instances page, find the target CEN instance and click Manage in the Actions column.
4. On the CEN page, click Route Maps and then click Add Route Map.

5. In the Add Route Map dialog box, configure the route map according to the following information and then click OK.
   - Priority: Enter the priority of the route map. A smaller number represents a higher priority. In this example, enter 20.
   - Region: Select the region to which the route map is applied. In this example, select China (Beijing).
   - Transmit Direction: Select the direction of the route map. In this example, select Export from Regional Gateway.
   - Match Condition: Set the matching conditions of the route map. In this example, add two matching conditions:
     - Source Instance ID: Enter the instance ID of SAG1.
     - Target Instance ID: Enter the instance ID of the VBR.
     - Route Prefix: Enter 172.16.0.0/24.
   - Match Mode: Select the matching mode of the route map. In this example, select Permit.



After you add the route map, you can view the route that allows the on-premises data center to access branch 1 on the Routes tab.

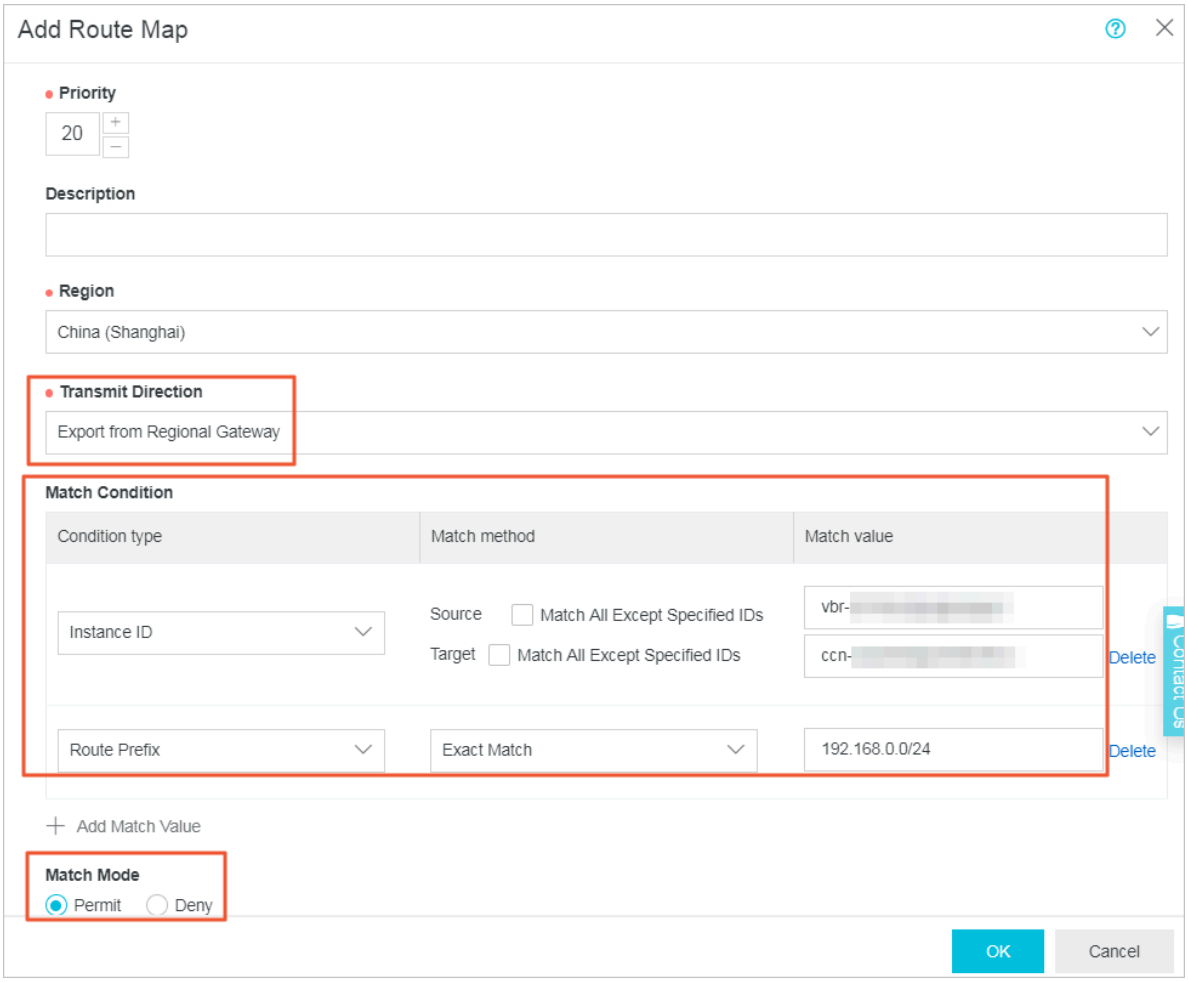


Step 2: Set a route map that allows the CCN to access the on-premises data center

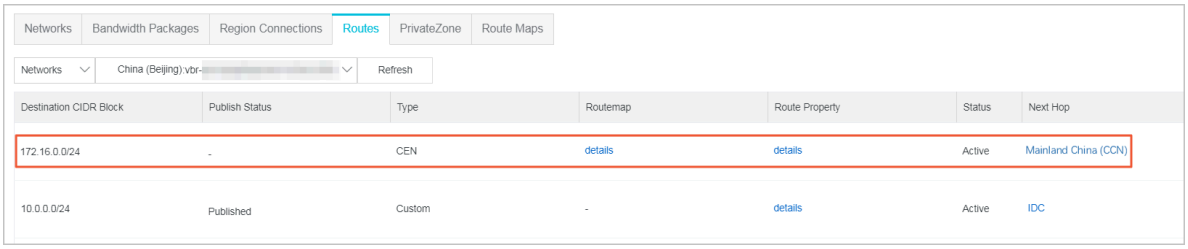
To set a route map that allows the CCN to access the on-premises data center, follow these steps:

1. Log on to the CEN console.
2. In the left-side navigation pane, click Instances.
3. On the Instances page, find the target CEN instance and click Manage in the Actions column.
4. On the CEN page, click Route Maps and then click Add Route Map.

5. In the Add Route Map dialog box, configure the route map according to the following information and then click OK.
   - Priority: Enter the priority of the route map. A smaller number represents a higher priority. In this example, enter 20.
   - Region: Select the region to which the route map is applied. In this example, select China (Shanghai).
   - Transmit Direction: Select the direction of the route map. In this example, select Export from Regional Gateway.
   - Match Condition: Set the matching conditions of the route map. In this example, add two matching conditions:
     - Source Instance ID: Enter the instance ID of the VBR.
     - Target Instance ID: Enter the instance ID of the CCN.
     - Route Prefix: Enter 192.168.0.0/24.
   - Match Mode: Select the matching mode of the route map. In this example, select Permit.



After you add the route map, you can view the route that allows the CCN to access the on-premises data center on the Routes tab.

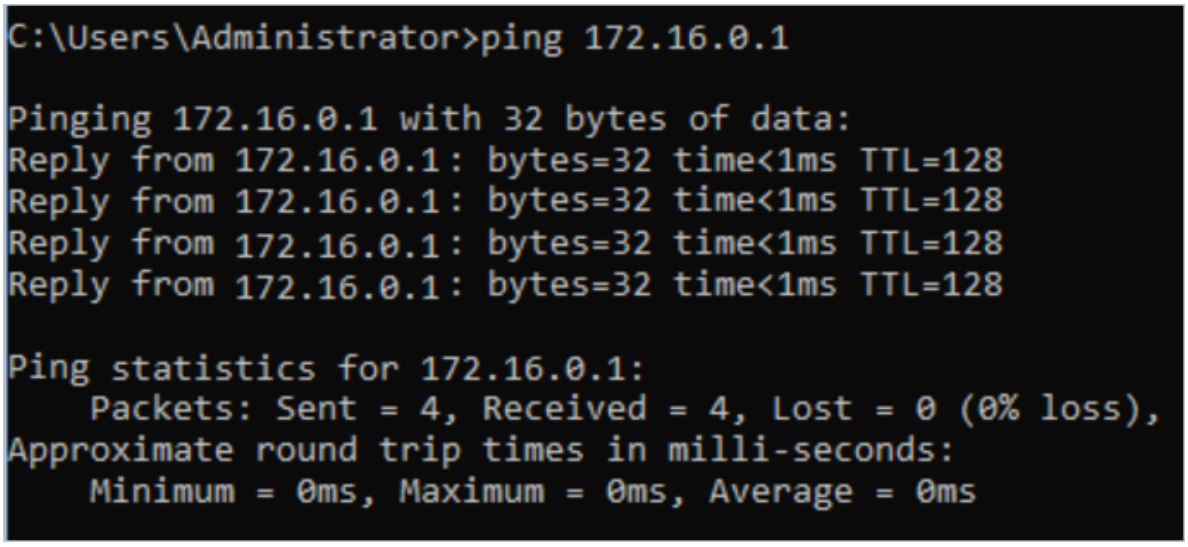


Step 3: Test the network connectivity

To test the network connectivity between the on-premises data center and branch 1, follow these steps:

1. Open the command prompt of the PC at the on-premises data center.
2. Use the `ping` command to `ping` the IP address of branch 1.

   The output shows that the PC of the on-premises data center can access branch 1.



3. Open the command prompt of the PC at branch 1.

4. Use the `ping` command to `ping` the IP address of the PC at the on-premises data center.

   The output shows that branch 1 can access the on-premises data center.

```
C:\Users\Administrator>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:
Reply from 192.168.0.1 : bytes=32 time<1ms TTL=128
Reply from 192.168.0.1 : bytes=32 time<1ms TTL=128
Reply from 192.168.0.1 : bytes=32 time<1ms TTL=128
Reply from 192.168.0.1 : bytes=32 time<1ms TTL=128

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

To test the network connectivity between the on-premises data center and branch 2, follow these steps:

1. Open the command prompt of the PC at the on-premises data center.
2. Use the `ping` command to `ping` the IP address of branch 2.

   The output shows that the PC of the on-premises data center cannot access branch 2.

```
C:\Users\Administrator>ping 10.0.0.1

Pinging 10.0.0.1 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.0.0.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```