Alibaba Cloud Express Connect

Getting Started (New Console)

Issue: 20181129

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.	 **Note:** 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]`*
{} or {a|b}	It indicates that it is a required value, and only one item can be selected.	`swich` *`{stand | slave}`*

Contents

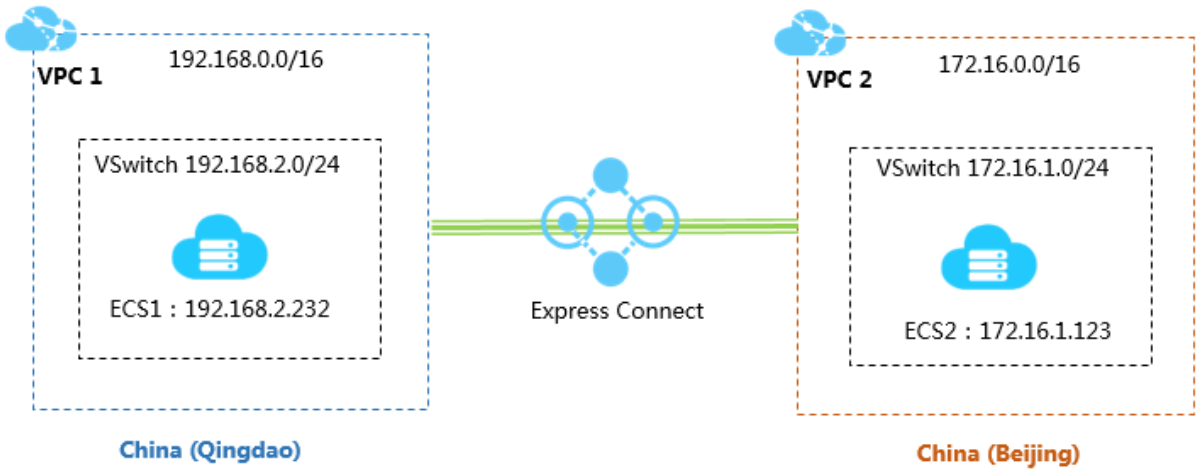
1 Interconnect two VPCs under the same account

This tutorial describes how to use Express Connect to connect two VPCs under the same account.

Note:
If this is the first time that you are using Express Connect to interconnect two VPCs, we recommend that you use Cloud Enterprise Network (CEN). For more information, see *Tutorial overview*.

Example

This tutorial uses the following two VPCs as an example to show you how to fulfill VPC intercommunication by using Express Connect.



Prerequisites

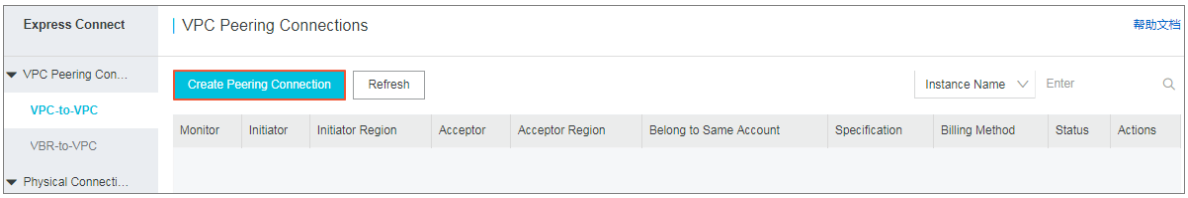
The Classless Inter-Domain Routing (CIDR) blocks of the VPCs or VSwitches that you want to interconnect do not conflict.

Step 1: Create a peering connection

Perform the following steps to create a peering connection:

1. Log on to the *Express Connect* console.
2. In the left-side navigation pane, click **VPC Peering Connections** > **VPC-to-VPC**.
3. Select a region.

   In this example, select **China (Qingdao)**.
4. Click **Create Peering Connection**.



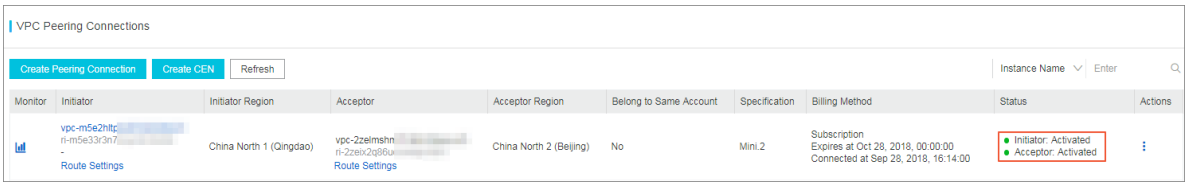
5. Configure the peering connection.

   In this example, use the following configurations:

   - **Connection Type**: Select **VPC-to-VPC**.
   - **Routers to Create**: Select **Initiator and Acceptor**.

     The system sets the selected local VPC as the connection initiator, sets the peer VPC as the acceptor, and automatically connects the initiator and the acceptor.
   - **Local Region**: Select the region of the local VPC. In this example, select **China (Qingdao)**.
   - **Local VPC ID**: Select the local VPC, that is, the initiator of the connection. In this example, select **VPC1**.
   - **Peer Region**: Select the region of the peer VPC. In this example, select **China (Beijing)**.
   - **Peer VPC ID**: Select the peer VPC to be connected. In this example, select **VPC2**.
   - **Specification**: Select a bandwidth for the interconnection. In this example, select **2 Mb**.
6. Click **Buy Now** and complete the payment.
7. Go back to the **VPC Peering Connections** page to check the created peering connection.

   When the initiator and the acceptor are both in the activated state, the connection is established successfully.

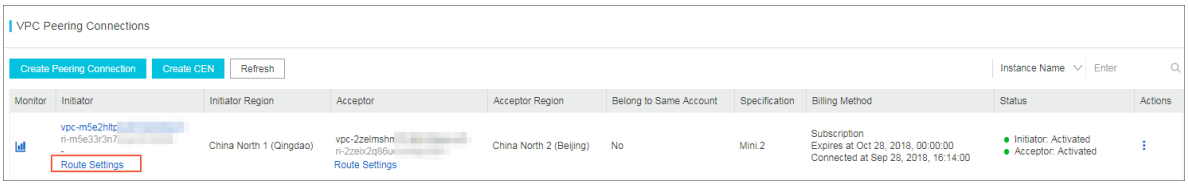


Step 2: Configure routes

After establishing the peering connection, add a route for each of the two interconnected VPCs.

Perform the following steps to configure the routes:

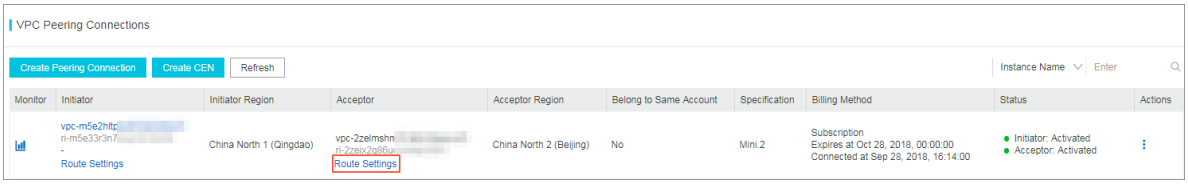
1. On the **VPC Peering Connections** page, find the created peering connection.
2. Click **Route Settings** under the initiator instance.



3. Click **Add Route Entry**, enter the destination CIDR block of the VPC or VSwitch that you want to connect, and then click **Confirm**.

   In this example, enter the CIDR block of the peer VPC: 172.16.0.0/16.

4. Click **Route Settings** under the acceptor instance.



5. Click **Add Route Entry**, enter the destination CIDR block of the VPC or VSwitch that you want to connect, and then click **Confirm**.

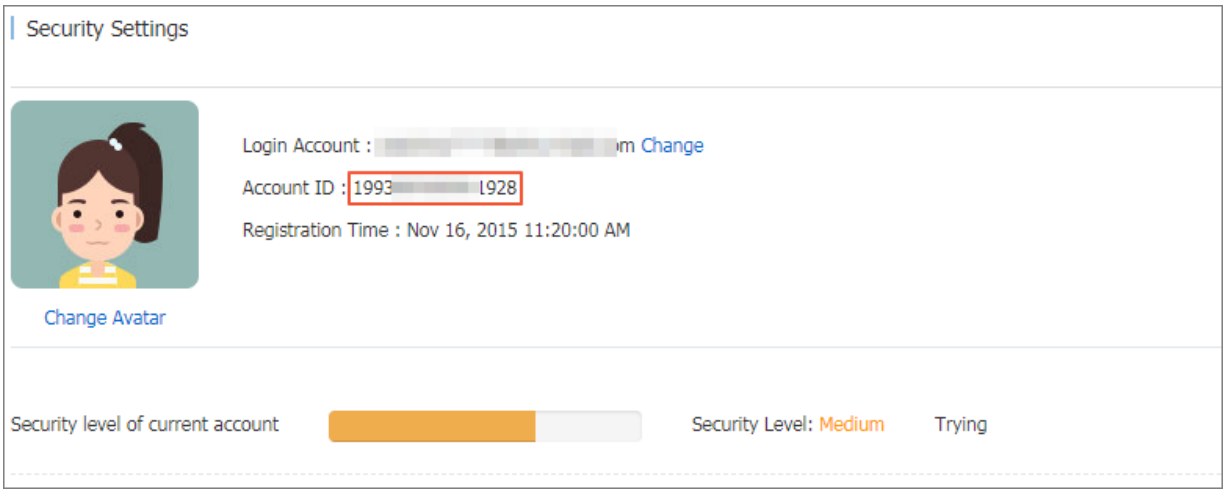
Step 3: Configure security groups

After establishing the peering connection between the two VPCs, you need to configure security groups to enable the intercommunication of ECS instances in these two VPCs.

This tutorial uses the ECS instances and security groups in the following table as an example.

Configuration	Account A	Account A
Account ID	AccountID_A	AccountID_A
ECS instance ID	InstanceID_A	InstanceID_B
Security group ID	SecurityGroupID_A	SecurityGroupID_B

You can view the account ID in the *Account Center*.



Perform the following steps to configure the security group rule:

1. Log on to the *ECS console*.
2. In the left-side navigation pane, click **Networks and Security** > **Security Groups**.
3. Select the region of the instance.
4. Find the target security group and then click **Add Rules**.
5. On the **Security Group Rules** page, click **Add Security Group Rule**.
6. Configure the security group rule, select the protocol type, and enter the port range.

> **Note:**
> For cross-region VPC interconnection, select the CIDR block authorization type and enter the CIDR block of the peer VPC.
>
> If you select the security group authorization type, make sure that the VPCs are in the same region.

In this example, select the CIDR block authorization type.

Step 4: Test the connection

After establishing the peering connection and adding the routes, you can log on to an ECS instance of either VPC and ping the IP address of an ECS instance in the other VPC. If the ping succeeds, the connection between the two VPCs is successful.

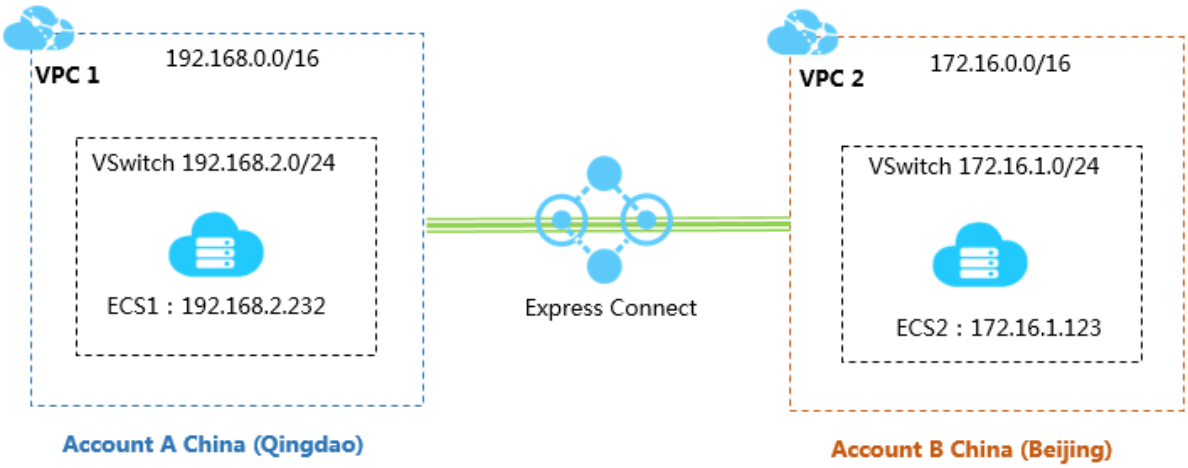
2 Establish an intranet connection between VPCs under different accounts

This tutorial guides you to use Express Connect to connect two VPCs under different accounts.

Note:
If you use Express Connect to connect two VPCs for the first time, we recommend that you use CEN. For more information, see *Tutorial overview*.

Example

To connect VPCs under different accounts, you must create the initiator and acceptor respectively, establish a peering connection and configure the routes. This tutorial takes the following two VPCs as an example. VPC1 under account A acts as the initiator and VPC2 under account B acts as the acceptor.



Prerequisites

- You have obtained the Alibaba Cloud account ID of the peer end and the VRouter ID of the VPC to connect.
- Make sure that the CIDR blocks of the VPCs or VSwitches to be interconnected do not conflict with each other.

Step 1 Create the initiator

To create the initiator, complete these steps:

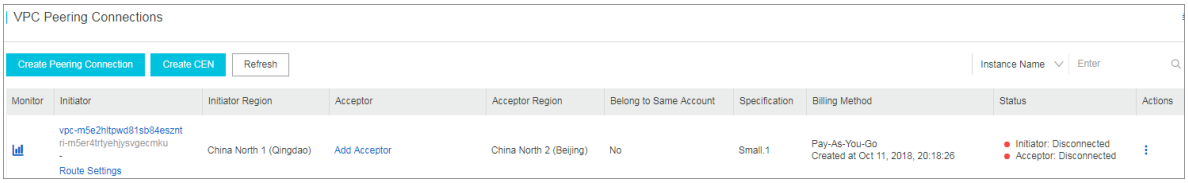
1. Use account A to log on to the *Express Connect console*.
2. In the left-side navigation pane, click**VPC Peering Connections** > **VPC-to-VPC**.

3. Click **Create Peering Connection**.
4. Configure the peering connection.

   The following are the configurations used in this tutorial.

   - **Account**: Select **Different Account**.
   - **Connection Type**: Select **VPC-to-VPC**.
   - **Router Creation**: Select **Create Initiator Only**.

     Only the initiator can actively initiate the connection.
   - **Local Region**: Select the region of the VPC. In this tutorial, select **China (Qingdao)**.
   - **VPC ID**: Select the VPC for which the initiator instance is created. In this tutorial, select **VPC1**.
   - **Peer Region**: Select the region where the VPC to connect is located. In this tutorial, select **China (Beijing)**.
   - **Bandwidth**: Select the bandwidth of the interconnection. In this tutorial, select **2Mb**.
5. Click **Buy Now** to complete the payment.
6. Go back to the **VPC Peering Connections** page to view the created initiator instance.



Step 2 Create the acceptor

To create the acceptor, complete these steps:

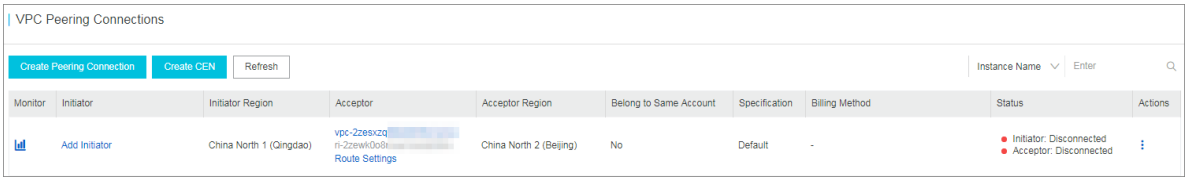
1. Use account B to log on to the *Express Connect console*.
2. In the left-side navigation pane, click **VPC Peering Connections** > **VPC-to-VPC**.
3. Click **Create Peering Connection**.
4. Configure the peering connection.

   The following are the configurations used in this tutorial.

   - **Account**: Select **Different Account**.
   - **Connection Type**: Select **VPC-to-VPC**.
   - **Router Creation**: Select **Create Acceptor Only**.
   - **Local Region**: Select the region where the VPC is located. In this tutorial, select **China (Beijing)**.

- **VPC ID**: Select the VPC for which the acceptor instance is created. In this tutorial, select **VPC2**.
- **Peer Region**: Select the region where the VPC to connect is located. In this tutorial, select **China (Qingdao)**.
- **Bandwidth**: The bandwidth of the acceptor is decided by the initiator. In this tutorial, select **Default**.

5. Click **Buy Now** and complete the payment.
6. On the **VPC Peering Connections** page, view the created acceptor instance, and record the ID of the created acceptor instance (the instance ID in this tutorial is ri-2zeix2q86uoyisagyz0pn).



Step 3 Add the initiator

After creating the initiator and the acceptor, you must add the initiator for the acceptor.

To add the initiator for the acceptor, complete these steps:

1. Use account B to log on to the *Express Connect console*.
2. In the left-side navigation pane, click **VPC Peering Connections** > **VPC-to-VPC**.
3. Select the region of the acceptor.

   In this tutorial, select **China (Beijing)**.
4. Find the created acceptor instance and click **Add Initiator**.

5. On the **Add Instance** page, select **No**, and enter the initiator router interface (In this tutorial, the interface ID is ri-m5e33r3n78zyi5573kf85). Click **OK**.

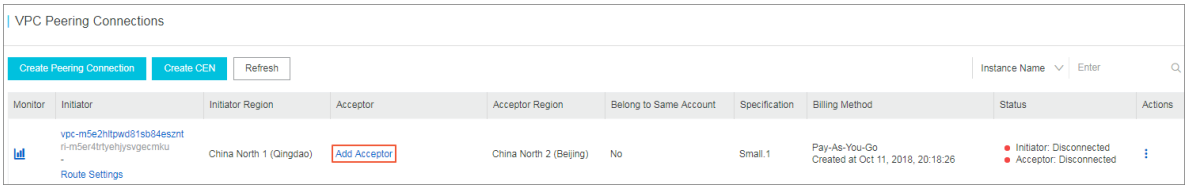
Step 4 Add the acceptor and establish a peering connection

After adding the initiator and acceptor, the initiator can actively initiate the connection to establish a peering connection between the two VPCs.

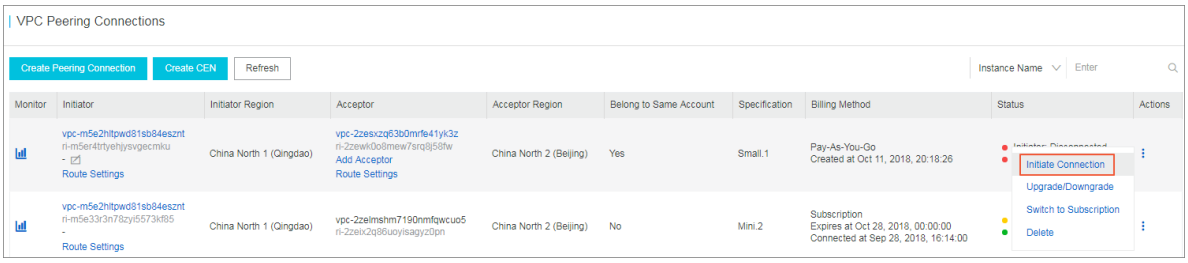
In this tutorial, the initiator is the VPC under account A. To establish the peering connection, complete these steps:

1. Use account A to log on to the *Express Connect console*.
2. In the left-side navigation pane, click **VPC Peering Connections** > **VPC-to-VPC**.
3. Select the region of the initiator instance.

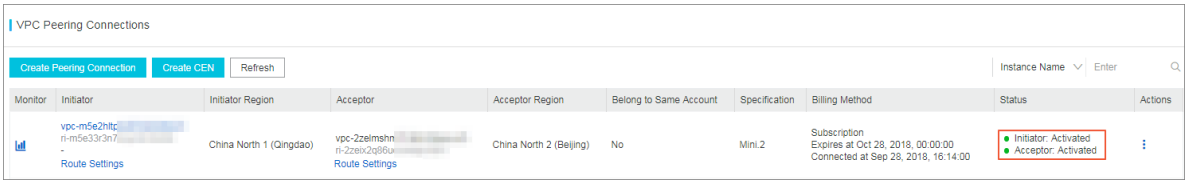
   In this tutorial, select **China (Hangzhou)**.
4. Click **Add Acceptor**.



5. On the **Add Instance** page, select **No**, and enter the acceptor router interface (In this tutorial, the interface ID is ri-2zeix2q86uoyisagyz0pn). Click **OK**.
6. Click  > **Initiate Connection**.



After the connection is successfully established, the status of the initiator and acceptor becomes activated.



Step 5 Configure the routes

After establishing the peering connection, you must add routes for the interconnected VPCs.

To configure the routes, complete these steps:

1. Use account A to log on to the *Express Connect console*.
2. On the **VPC Peering Connections** page, find the created peering connection.
3. Find the initiator instance and click **Route Settings**.

4. Click **Add Route Entry**, enter the CIDR block of the VPC or VSwitch to connect, and click **Confirm**.

   In this tutorial, enter the CIDR block of the peer VPC, that is, 172.16.0.0/16.

5. Use account B to log on to the *Express Connect console*.
6. Find the acceptor instance and click **Route Settings**.

7. Click **Add Route Entry**, enter the CIDR block of the VPC or VSwitch to connect, and click **Confirm**.

   In this tutorial, enter the CIDR block of the peer VPC, that is 192.168.0.0/16.

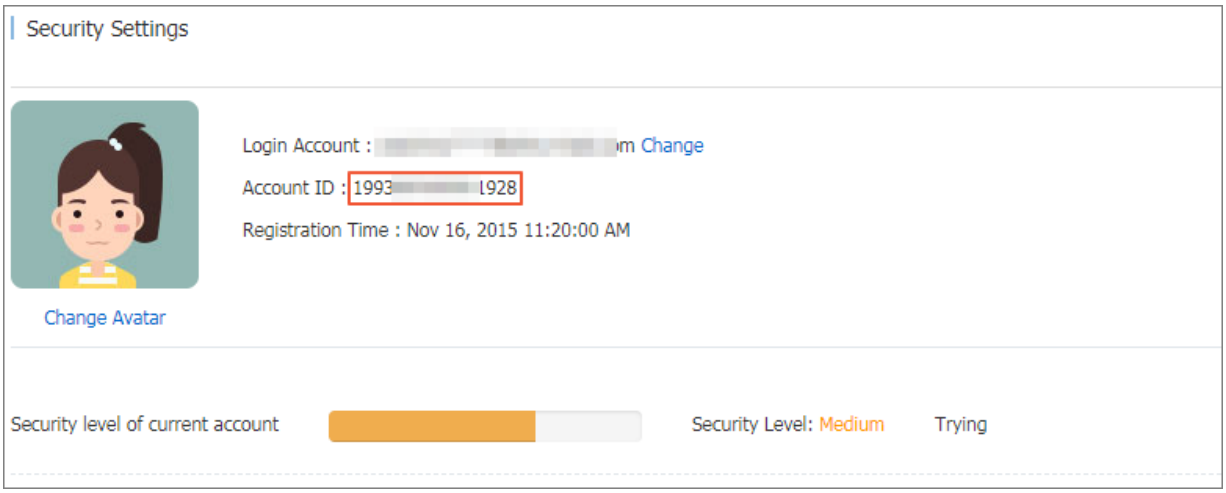
Step 6 Configure security groups

After establishing the peering connection between the two VPCs, you also need to configure security group rules so that ECS instances in the two VPCs can communicate with each other.

This tutorial uses ECS instances and security group configurations in the following table as an example.

Configurations	Account A	Account B
Account ID	AccountID_A	AccountID_B
ECS instance ID	InstanceID_A	InstanceID_B
Security group ID	SecurityGroupID_A	SecurityGroupID_B

You can view the account ID in the *Account Center*.



To configure security groups, complete these steps:

1. Log on to the *ECS console*.
2. In the left-side navigation pane, click **Networks and Security** > **Security Groups**.
3. Select the region of the target instance.
4. Find the target security group and then click **Add Rules**.
5. On the **Security Group Rules** page, click **Add Security Group Rule**.
6. Configure the security group rule, select the protocol type and enter the port range. Then select the authorization type according to the following information.

Scenario	Authorization type	Configuration
Cross-region VPC interconnection	CIDR block	The CIDR block of the peer VPC.
Same-region VPC interconnection	Security group	The ID of the security group associated with the peer ECS instance. **Note:** If the VPCs to be interconnected belong to different accounts, select to allow other accounts. In the Account ID field, select the peer account ID.

Note:

- If the VPCs to be interconnected are in different regions, select the CIDR block authorizat ion type and enter the CIDR block of the peer VPC. In this tutorial, select the CIDR block authorization type.

- If the VPCs to be interconnected are in the same region, select the security group authorization type. In cross-account interconnection, select **Allow Other Accounts**. In the Account ID field, select the peer account ID.

Step 7 Test the connection

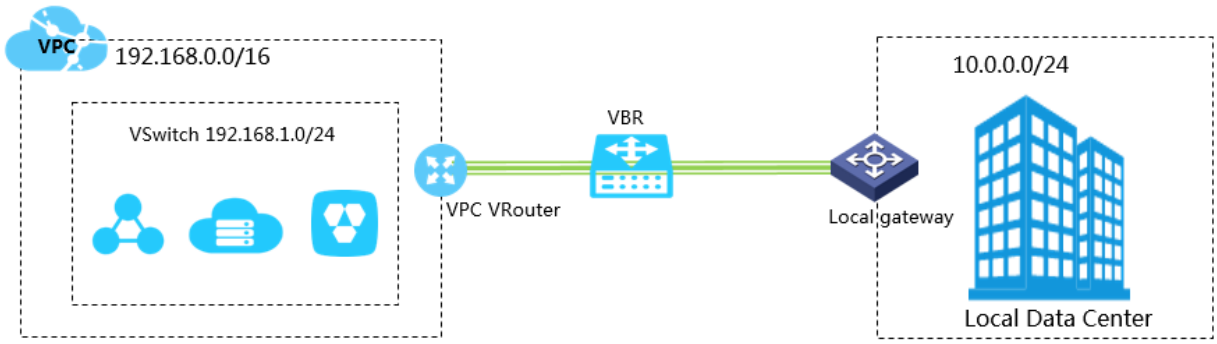
After establishing the peering connection and adding routes, you can log on to an ECS instance in one VPC, and ping the priviate IP of an ECS instance in the peer VPC. If you can successfully ping the private IP, the two VPCs have been successfully connected.

3 Connect a local IDC to a VPC through a physical connection

This tutorial describes how to use Express Connect to implement intercommunication between your local IDC and the Alibaba Cloud VPC.

Example

This tutorial uses the VPC and local IDC configurations shown in the following figure.



Prerequisites

You have submitted a ticket and obtained the geographic position of the access point.

Step 1: Apply for a physical connection interface and complete leased line access

1. Log on to the *Express Connect* console.
2. In the left-side navigation pane, click **Physical Connections** > **Physical Connection Interfaces**.
3. Click **Apply for New Interface**.
4. Configure the interface. Perform the following configurations:
   - **Name**: Enter the name of the physical connection interface.
   - **Access Point**: Select the nearest access point to your local IDC. In this example, select **ap-cn-zhangjiakou-xrt-A**.
   - **Service Provider**: Select your physical connection provider. In this example, select **China Mobile**.
   - **Port Type**: Select the access port of the physical connection. In this example, select **1 Gbit/s Electrical Port**.
   - **Bandwidth**: Enter a bandwidth value (unit: Mbps) based on your specific service needs. In this example, enter **2**.

- **Location**: Enter the address of your local IDC.
- **Redundancy**: If you want to implement Equal-Cost Multi-Path (ECMP) routing through two physical connections, you can select another physical connection to provide redundancy in this physical connection.

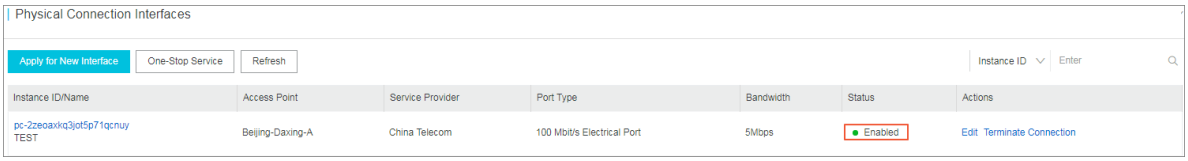
  In this example, do not select a redundant physical connection.

5. Click **OK**. On the **Physical Connection Interfaces** page, check the physical connection interface you have applied for.

   The physical connection interface status is **Applying**.
6. Wait for Alibaba Cloud to review your application. Normally, the review will be completed on the next workday. When the physical connection interface status becomes **Approved**, click **Pay for Connection** and complete the payment.

   The system automatically allocates you a port and a physical connection ID.
7. The physical connection interface status becomes **Connecting**. Click **View** to view the details, such as IDC location, cabinet location, and port information.
8. Notify your service provider of the port information. After conducting a resource survey, the service provider will provide a list of personnel who will be sent to the Alibaba Cloud IDC at the access point, and provide relevant information, such as arrival time and physical connection ID. **Open a new ticket** to inform Alibaba Cloud after-sales personnel of the information about the leased line to be deployed by the service provider.
9. On the next workday, Alibaba Cloud after-sales personnel will schedule a visit to the IDC for your service provider and give you the contact information of the reception personnel in the IDC. You need to notify your service provider of the preceding information. After the service provider completes deployment in the Alibaba Cloud IDC, Alibaba Cloud after-sales personnel will change the physical connection interface status to **Pending Confirmation**.
10. After your service provider notifies you that the physical connection is deployed, find the physical connection in the console and click **Confirm**.

    When the physical connection interface status changes to **Enabled**, the physical connection is completed.



Step 2: Create a virtual border router

After the physical connection is established, you need to create a Virtual Border Router (VBR) for it as a forwarding bridge between the VPC and your local IDC.

To create a VBR, perform the following steps:

1. Log on to the *Express Connect* console.
2. In the left-side navigation pane, click **Physical Connections** > **Virtual Border Routers (VBRs)**.
3. Click **Create VBR**. In this example, configure the VBR as follows:
   - **Account**: Select **Current Account**.
   - **Name**: Enter the VBR name.
   - **Physical Connection Interface**: Select the physical connection interface created in Step 1.
   - **VLAN ID**: Enter the VLAN ID. In this example, enter 1678.
   - **Gateway IP Address on Alibaba Cloud Side**: Enter the gateway from the VPC to your local IDC. In this example, enter 10.0.0.1.
   - **Gateway IP Address on Customer Side**: Enter the gateway from your local IDC to the VPC. In this example, enter 10.0.0.2.
   - **Subnet Mask**: Enter the subnet mask of the IP address on Alibaba Cloud side and customer side. In this example, enter 255.255.255.0.
4. Click **OK**.

Step 3: Create a peering connection

After the physical connection is established, you also need to establish a peering connection between the VBR associated with the physical connection and the VPC to be connected.

To create a peering connection, perform the following steps:

1. Log on to the *Express Connect* console.
2. In the left-side navigation pane, click **VPC Peering Connections** > **VBR-to-VPC**.
3. Click **Create Peering Connection**.
4. Configure the peering connection.

   Perform the following configurations:

   - **Belongs to Current Account** : Select **Yes**.
   - **Connection Type**: Select **VBR-to-VPC**.

- **Routers to Create**: Select **Initiator and Acceptor**.

  In physical connection scenarios, the initiator of a peering connection must be a VBR.
- **Local Region**: Select the region where the VBR is located. In this example, select **China (Zhangjiakou-Beijing Winter Olympics)**.
- **Local Access Point**: Select the access point of the physical connection. In this example, select **ap-cn-zhangjiakou-xrt-A**.
- **Local VBR ID**: Select the created VBR. In this example, select **VBR1**.
- **Peer Region**: Select the region where the peer VPC is located. In this example, select **China (Zhangjiakou-Beijing Winter Olympics)**.
- **Peer VPC ID** : Select the peer VPC. In this example, select **VPC1**.
- **Bandwidth**: Select the bandwidth for intercommunication. In this example, select **1Gb**.

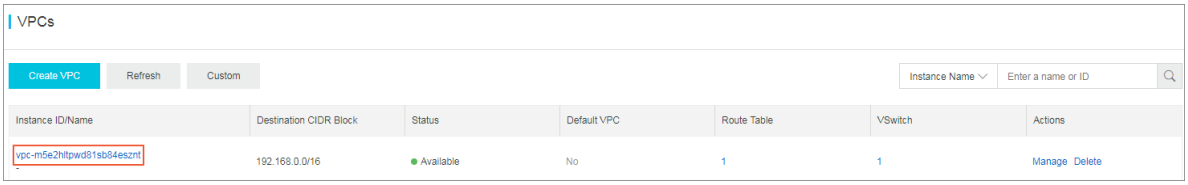
5. Click **Buy Now** and complete the payment.
6. Check the created peering connection. When the initiator and the acceptor are in **Activated** status, the peering connection is established successfully.

Step 4: Configure VPC routing

After establishing a peering connection, you need to add a route entry destined for your local IDC to the VPC.

To forward the traffic destined for your local IDC (11.11.11.0/24) to the VBR, perform the following steps:

1. On the VPCs page, locate the intercommunicated VPC, and then click the ID of the VPC.



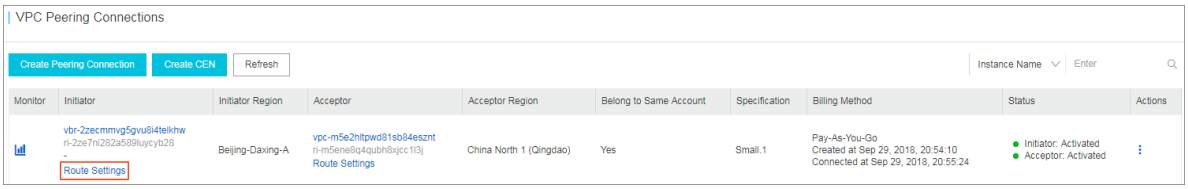
2. In the **Network Resources** area, click the route table link.
3. On the **Route Tables** page, click the route table ID of the VPC, and then click **Add Route Entry**.
4. Configure the route entry as follows and then click **OK**:

- **Destination CIDR Block**: Enter the CIDR block of your local IDC. In this example, enter 10.0.0.0/24.
- **Next Hop Type**: Select **Router Interface (To VBR)**.
- **General Routing**: Select the VBR associated with the physical connection.

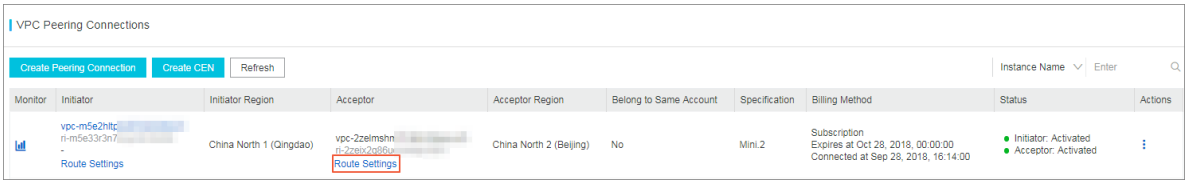
Step 5: Configure VBR routing

To configure VBR routing destined for your local IDC and the VPC respectively, perform the following steps:

1. Log on to the *Express Connect* console.
2. In the left-side navigation pane, click **VBR-to-VPC**.
3. Locate the target VBR, and then click **Route Settings**.



4. Click **Add Route Entry**.
5. In the displayed dialog box, enter the CIDR block of the VPC (In this example, enter 192.168.0.0/16), and then click **Confirm**.
6. Click **Route Settings** under the acceptor associated with the VBR instance.



7. Click **Add Route Entry**.
8. Enter the CIDR block of your local IDC (In this example, enter 10.0.0.0/24), and then click **Confirm**.

Step 6: Configure routing for your local IDC

Now the route configuration for the Alibaba Cloud side is completed. On the physical connection device, you still need to configure a route destined for the VPC. You can configure a static route or BGP route as follows to forward data from your local IDC to VBR:

- Static route

Example:

```
ip route 192.168.0.0/16 10.0.0.2
```

- Dynamic route

  You can also forward data between your local IDC and the VBR by configuring BGP. For more information, see *Configure BGP*.

After the route configuration is completed, the intranet communication link between your local IDC and VPC (local IDC→physical connection→VBR→VPC) is established.

> **Note:**
> You can manage the access between your local IDC devices and Alibaba Cloud products by adjusting the ECS security group rules or adding an RDS whitelist.

Step 7: Test the connection

After the VPC is connected to the local data center, test the speed of the leased lines to ensure that they can meet service needs.