Alibaba Cloud
Express Connect

Getting Started (New Console)

Issue: 20190320

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 Connect VPCs

You can use CEN and Express Connect to connect different VPCs.

Overview

To meet various demands of different application scenarios, Alibaba Cloud provides several products for connecting VPCs. You can use CEN or Express Connect to connect VPCs. We recommend that you use CEN because it is easy to configure and automatically distributes and learns routes.

· *CEN*

You can use Cloud Enterprise Network (CEN) to build an intranet connection between multiple VPCs or between a VPC and a local data center. CEN provides automatic route distribution and learning, which ensures rapid network convergence and enhances the quality and security of cross-network communication.

· *Express Connect*

You can use Express Connect to build an intranet connection between two VPCs.

Scenarios

Scenario	Product	Method
Connect VPCs in the same region and under the same account	*CEN*	*Connect VPCs in the same region and under the same account*
	Express Connect	*Interconnect two VPCs under the same account*
Connect VPCs in the same region but under different accounts	*CEN*	*Connect VPCs in the same region but under different accounts*
	Express Connect	*Interconnect two VPCs under different accounts*
Connect VPCs in different regions but under the same account	*CEN*	*Connect VPCs in different regions but under the same account*

Scenario	Product	Method
	Express Connect	*Interconnect two VPCs under the same account*
Connect VPCs in different regions and under different accounts	*CEN*	*Connect VPCs in different regions and under different accounts*
	Express Connect	*Interconnect two VPCs under different accounts*

2 Interconnect two VPCs under the same account

This tutorial describes how to use Express Connect to connect two VPCs under the same account.
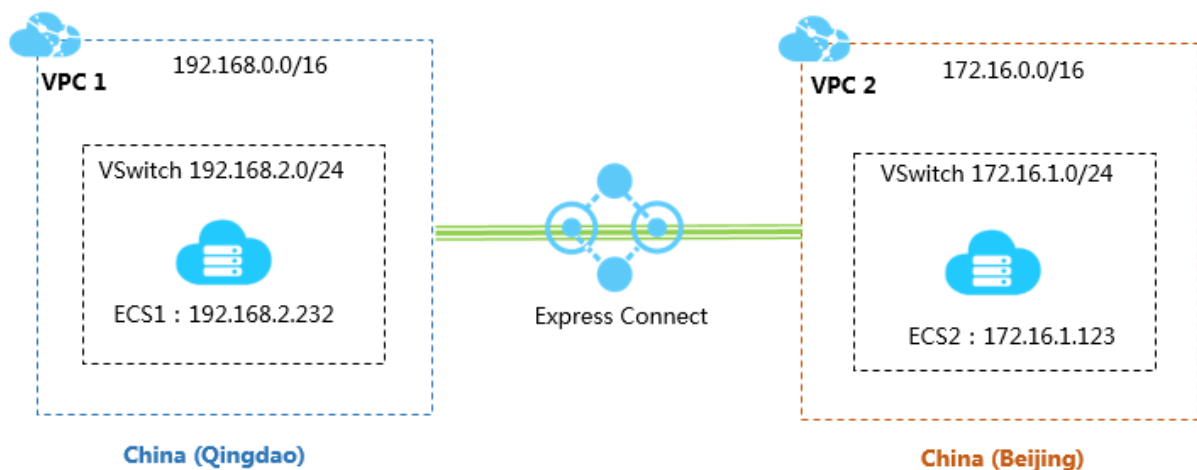
> 📋 **Note:**
>
> If this is the first time that you are using Express Connect to interconnect two VPCs, we recommend that you use Cloud Enterprise Network (CEN). For more information, see *Tutorial overview*.

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.
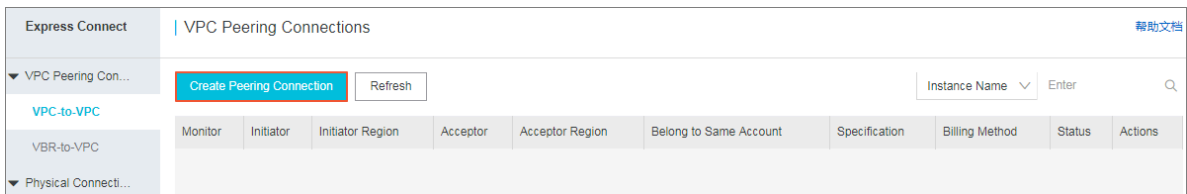
Step 1: Create a peering connection

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.
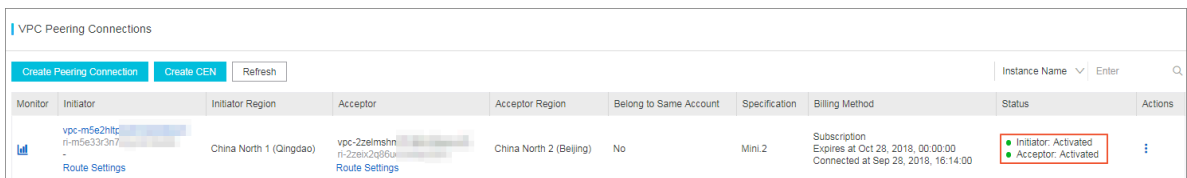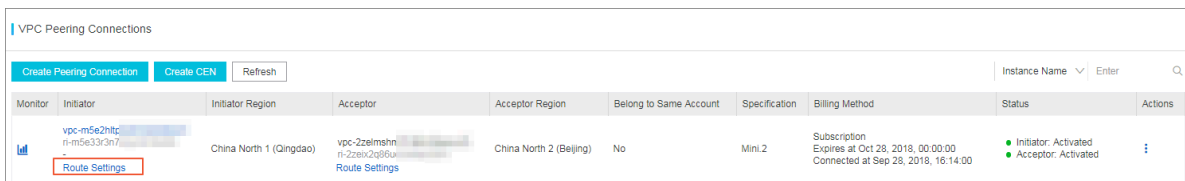

Step 2: Configure routes

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.
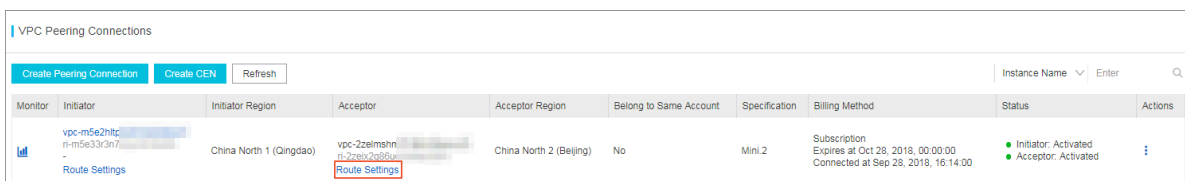
5. Click Add Route Entry, enter the destination CIDR block of the VPC or VSwitch that you want to connect, and then click Confirm.
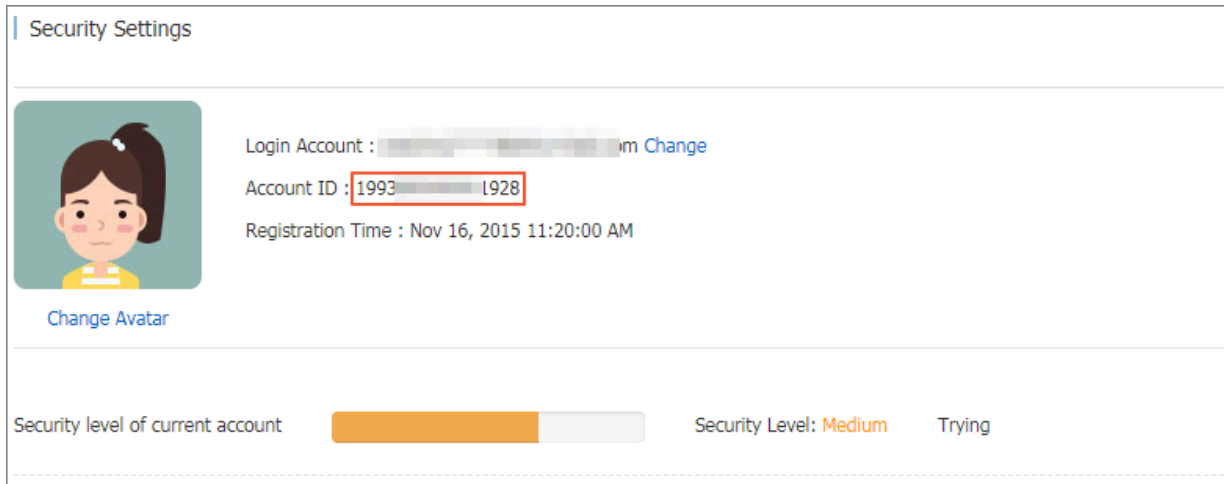
Step 3: Configure security groups

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*.

Security Settings

Login Account : ██████████████ om Change
Account ID : 1993████████1928
Registration Time : Nov 16, 2015 11:20:00 AM

Change Avatar

Security level of current account   Security Level: Medium   Trying

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.

   > **Notice:**
   >
   > 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.

3 Interconnect two VPCs under different accounts

This tutorial describes how to use Express Connect to connect two VPCs under different accounts.

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

Example

In cross-account VPC interconnection, you need to create an initiator and an acceptor separately, establish a peering connection, and then configure routes. This tutorial uses the following two VPCs as an example. VPC1 under account A acts as the initiator and VPC2 under account B acts as the acceptor.
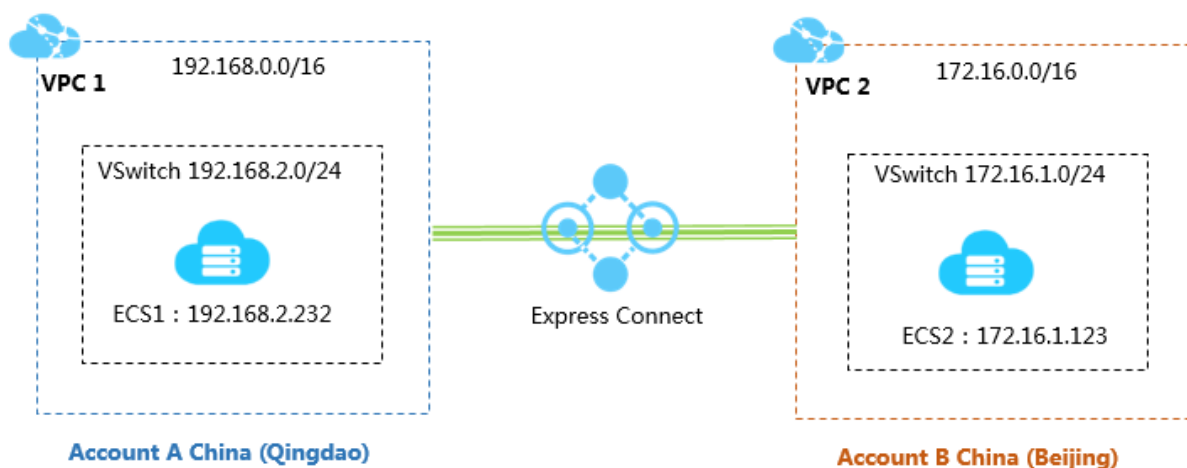
Prerequisites

- You have obtained the Alibaba Cloud account ID of the peer VPC and the VRouter ID of the VPC.
- The Classless Inter-Domain Routing (CIDR) blocks of the VPCs or VSwitches that you want to interconnect do not conflict.

Step 1: Create an initiator

Perform the following steps to create an initiator:

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

3. Click Create Peering Connection.

4. Configure the peering connection.

   Use the following configurations:

   · Account: Select Different from Peer's.

   · Connection Type: Select VPC-to-VPC.

   · Routers to Create: Select Create Initiator.

     Only the initiator can initiate the connection to the acceptor.

   · Local Region: Select the region of the VPC. In this example, select China
     (Qingdao).

   · Local VPC ID: Select the VPC for which the initiator instance is created. In this
     example, select VPC1.

   · Peer Region: Select the region where the VPC to be connected is located. In this
     example, select China (Beijing).

   · Specification: Select a bandwidth for the interconnection. In this example, select
     2 Mb.

5. Click Buy Now and complete the payment.

6. Go back to the VPC Peering Connections page to check the created initiator
   instance.

Step 2: Create an acceptor

Perform the following steps to create an acceptor:

1. Log on to the *Express Connect console* using the credentials of account B.

2. In the left-side navigation pane, click VPC Peering Connections > VPC-to-VPC.

3. Click Create Peering Connection.

4. Configure the peering connection.

   Use the following configurations:

   · Account: Select Different from Peer's.

   · Connection Type: Select VPC-to-VPC.

   · Routers to Create: Select Acceptor Only.

   · Local Region: Select the region of the VPC. In this example, select China
   (Beijing).

   · Local VPC ID: Select the VPC for which the acceptor instance is created. In this
   example, select VPC2.

   · Peer Region: Select the region where the VPC to be connected is located. In this
   example, select China (Qingdao).

   · Specification: The acceptor bandwidth depends on the initiator bandwidth. In
   this example, select Default.

5. Click Buy Now and complete the payment.

6. On the VPC Peering Connections page, check the created acceptor
   instance and note down its ID. In this example, the acceptor instance ID is
   ri-2zeix2q86uoyisagyz0pn.

Step 3: Add the initiator

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

Perform the following steps to add the initiator for the acceptor:

1. Log on to the *Express Connect console* using the credentials of account B.

2. In the left-side navigation pane, click VPC Peering Connections > VPC-to-VPC.

3. Select the region of the acceptor.

   In this example, select China (Beijing).

4. **Find the created acceptor instance and click Add Initiator.**

VPC Peering Connections									
Create Peering Connection	Create CEN	Refresh						Instance Name ∨ Enter	🔍
Monitor	Initiator	Initiator Region	Acceptor	Acceptor Region	Belong to Same Account	Specification	Billing Method	Status	Actions
📊	Add Initiator	China North 1 (Qingdao)	vpc-2zesxzq63b0mrfe41yk3z n-2zewik0o8mew7srq8j58fw Route Settings	China North 2 (Beijing)	No	Default	-	● Initiator: Disconnected ● Acceptor: Disconnected	⋮

5. **On the Add Instance page, select Another Account and enter the initiator router interface. In this example, enter ri-m5e33r3n78zyi5573kf85. Click OK.**

Step 4: Add the acceptor and establish a peering connection

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

In this example, the connection initiator is VPC1 under account A. Perform the following steps to establish a peering connection:

1. Log on to the *Express Connect console* using the credentials of account A.

2. In the left-side navigation pane, click VPC Peering Connections > VPC-to-VPC.

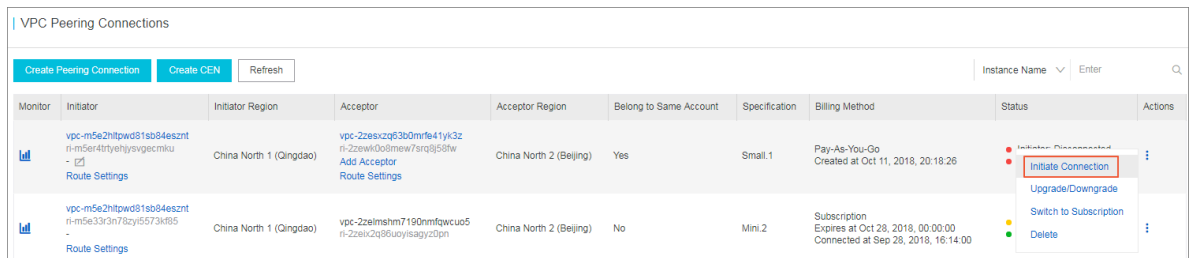3. Select the region of the initiator instance.

    In this example, select China (Qingdao).

4. Click Add Acceptor.

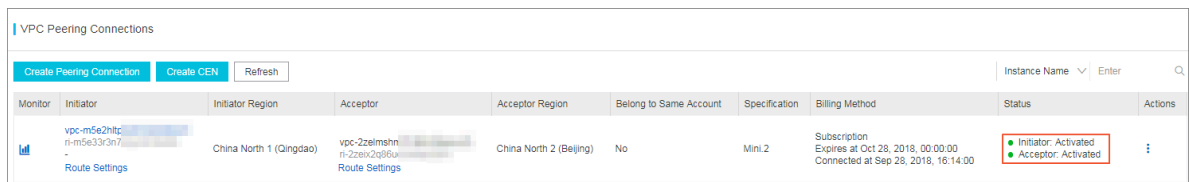| VPC Peering Connections									
Create Peering Connection	Create CEN	Refresh						Instance Name ∨ Enter	🔍
Monitor	Initiator	Initiator Region	Acceptor	Acceptor Region	Belong to Same Account	Specification	Billing Method	Status	Actions
📊	vpc-m5e2hltpwd81sb84esznt ri-m5er4trtyehjysvgecmku - Route Settings	China North 1 (Qingdao)	Add Acceptor	China North 2 (Beijing)	No	Small.1	Pay-As-You-Go Created at Oct 11, 2018, 20:18:26	● Initiator: Disconnected ● Acceptor: Disconnected	⋮

5. **On the Add Instance page, select Another Account and enter the acceptor router interface. In this example, enter ri-2zeix2q86uoyisagyz0pn. Click OK.**

6. Click [⋮] > **Initiate Connection.**

When the connection is established, the initiator and the acceptor enter the activated state.

Step 5: Configure routes

After establishing a peering connection, you need to add a route for each of the two VPCs.

Perform the following steps to configure the routes:

1. Log on to the *Express Connect console* using the credentials of account A.

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 be connected, and click Confirm.

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

5. Log on to the *Express Connect console* using the credentials of account B.

6. Find the acceptor instance and click Route Settings.

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

   In this example, enter the CIDR block of the peer VPC: 192.168.0.0/16.

Step 6: Configure security groups

After establishing a peering connection between 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 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*.

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. Then select the authorization type according to the following information.

Scenario	Authorization type	Description
Cross-region VPC interconnection	CIDR block	The CIDR block of the peer VPC.

Scenario	Authorization type	Description
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 Allow Other Accounts and in the Account ID field, enter the peer account ID.

Notice:

· If the VPCs to be interconnected are in different regions, select the CIDR block authorization type and enter the CIDR block of the peer VPC. In this example, 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 and in the Account ID field, enter 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 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.

4 Connect an on-premises IDC to a VPC through a physical connection

This topic describes how to use Express Connect to implement intercommunication between your on-premises IDC and the Alibaba Cloud VPC.

Example

This topic uses the VPC and on-premises IDC configurations shown in the following figure.
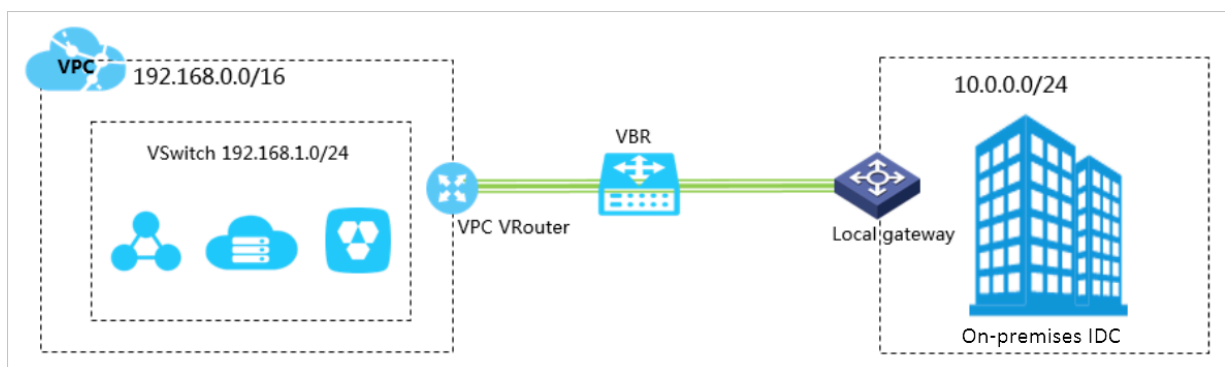
Step 1: Apply for a physical connection interface

1. Log on to the *Express Connect* console.

2. In the left-side navigation pane, choose Physical Connections > Physical Connection Interfaces.

3. Click Apply for New Interface.

4. Configure the interface by setting the following configurations:

   · Region: Select the region where the leased line is deployed. In this example,
     select China North 3 (Zhangjiakou).

   · SP: Select the service provider of your leased line. In this example, select China
     Unicom.

   · Access Point: Select the nearest access point to your on-premises IDC. In this
     example, select Zhangjiakou-Xiaoertai-A-Ali.

   · Port Specification: Select a port specification. In this example, select 10G. Note
     that different specifications incur different resource fees.

   · Port Type: Select the port type of the physical connection. In this example, select
     1000Base-LX.

   · Redundant Connection ID: If you want to implement Equal-Cost Multi-Path
     (ECMP) routing through two physical connections, you can select another
     physical connection to provide redundancy for this physical connection.

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

5. Click Buy Now and complete the payment for an initial installation fee.

6. On the Physical Connection Interfaces page, check the physical connection
   interface you have applied for.

   The physical connection interface is in the To Apply for LOA state.

7. Click Apply for LOA in the Actions column.

8. Enter your company name, the name of the data center cable installation company
   , the scheduled installation date and time, and the contact information of the data
    center cable installation technician or representative, and select a construction
   type.

9. Click OK. Your application is then sent to Alibaba Cloud personnel for review, and
   the physical connection interface enters the In Application state.

10. After your application is approved, download the LOA to view installation
    information in the console, such as the location of the installation site (the
    Alibaba Cloud IDC site), cabinet location, and port information. At this stage, we
    recommend that you instruct your installation company to start installation.

11. After installation is complete, click Delivery Report on the Physical Connection Interfaces page, enter the leased line code and the label numbers of the cables at the installation site, and click OK.

   The physical connection interface enters the Waiting state.

12. Alibaba Cloud will connect the cables to the corresponding CSW ports according to the information you provided. Alibaba Cloud should complete this step within two working days of you clicking OK in the preceding step.

   The physical connection interface enters the Waiting state.

13. After you confirm that the physical connection interface has been deployed, pay the resource fee and enable the port.

   When the physical connection interface changes to the Enabled state, the leased line connection is completed.

   > **Note:**
   > The estimated time frame of completing the LOA application, installation, and on-site assistance from Alibaba Cloud is subject to local laws and authorities.

Step 2: Create a virtual border router

After the leased line connection is completed, you need to create a Virtual Border Router (VBR) for it as a forwarding bridge between the VPC and your on-premises IDC.

To create a VBR, perform the following steps:

1. Log on to the *Express Connect* console.

2. In the left-side navigation pane, choose 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 on-premises IDC. In this example, enter 10.0.0.1.
- · Gateway IP Address on Customer Side: Enter the gateway from your on-premises 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, choose 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
   the Activated state, 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 on-premises IDC to the VPC.

To forward the traffic destined for your on-premises 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.

	VPCs						
Create VPC	Refresh	Custom				Instance Name ∨	Enter a name or ID
Instance ID/Name		Destination CIDR Block	Status	Default VPC	Route Table	VSwitch	Actions
vpc-m5e2hltpwd81sb84esznt		192.168.0.0/16	● Available	No	1	1	Manage Delete

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 on-premises 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 on-premises 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.

	VPC Peering Connections							
Create Peering Connection	Create CEN	Refresh					Instance Name ∨ Enter	
Monitor	Initiator	Initiator Region	Acceptor	Acceptor Region	Belong to Same Account	Specification	Billing Method	Status	Actions
📊	vbr-2zecmmvg5gvu8i4telkhw ri-2ze7ni282a589iuycyb28 - Route Settings	Beijing-Daxing-A	vpc-m5e2hltpwd81sb84esznt ri-m5ene8q4qubh8xjcc1l3j Route Settings	China North 1 (Qingdao)	Yes	Small.1	Pay-As-You-Go Created at Sep 29, 2018, 20:54:10 Connected at Sep 29, 2018, 20:55:24	● Initiator: Activated ● Acceptor: Activated	⋮

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 Add Route Entry again.

7. Enter the CIDR block of your on-premises IDC (In this example, enter 10.0.0.0/24), and then click Confirm.

Step 6: Configure routing for your on-premises 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 on-
premises 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 on-premises 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 on-premises IDC and VPC (on-premises IDC→physical connection→VBR→VPC)
is established.

> **Note:**
>
> You can manage the access between your on-premises 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 on-premises IDC, test the speed of the leased lines to
ensure that they can meet service needs.