

Alibaba Cloud Express Connect User Guide (New Console)

Issue: 20190408

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 <code>cd / d C :/ windows</code> command to enter the Windows system folder.
<i>Italics</i>	It is used for parameters and variables.	<code>bae log list --instanceid <i>Instance_ID</i></code>
[] or [a b]	It indicates that it is an optional value, and only one item can be selected.	<code>ipconfig [-all -t]</code>

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

Legal disclaimer.....	I
Generic conventions.....	I
1 Peering connection.....	1
1.1 What is a peering connection?.....	1
1.2 Interconnect two VPCs.....	2
1.3 Interconnect a VPC and a VBR.....	5
1.4 Manage Subscription instances.....	7
1.5 Delete peering connections.....	7
2 Physical connection.....	9
2.1 Physical connection process.....	9
2.2 Apply for leased line connection.....	10
2.3 Create redundant physical connections.....	13
2.4 Delete a physical connection.....	20
2.5 Access points.....	22
2.6 NSP partners.....	25
3 Virtual border router.....	27
3.1 Create a virtual border router.....	27
3.2 Configure BGP.....	28
3.3 Add route entries.....	32
3.4 Establish peering connections.....	33
4 Configure health checks.....	34
5 Manage quotas.....	36

1 Peering connection

1.1 What is a peering connection?

You can establish a peering connection between two VPCs or between a VPC and a Virtual Border Router (VBR).

Initiator and acceptor

When you establish a peering connection, one end (VPC or VBR) of the connection is the initiator, and the other end is the acceptor. Only the initiator can initiate a connection. The acceptor can only wait for the initiator to initiate a connection. The initiator and the acceptor are only used to control the process of connection establishment. After the connection is established, the communication link is bidirectional and there is no difference between the initiator and the acceptor.

For interconnections between VPCs under the same account, Express Connect provides an option to create the initiator and the acceptor at the same time. You do not need to manually initiate the connection. The system will automatically initiate and establish the connection. For interconnections between VPCs under different accounts, you must manually initiate a connection.

The following table compares the initiator and acceptor.

Item	Initiator	Acceptor
Is this end charged when VPCs are interconnected in the same region?	No	No
Is this end charged when VPCs are interconnected between different regions ?	Yes	No
Is it required to configure peer information before initiating a connection?	Yes	Yes
Can this end initiate a connection?	Yes	No
Can this end send messages to the peer end after a connection is established?	Yes	Yes

Connection process and status

In the peering connection process, the initiator initiates a connection. The acceptor then receives the connection, after which the connection is established successfully.

During different stages of the connection process, the status of a peering connection is also different, as shown in the following table.



Note:

If you choose to create both ends at the same time when establishing a peering connection, the system automatically initiates and establishes a connection. In this case, the initiator and the acceptor become activated after being created.

Connection process	Initiator status	Acceptor status
The initiator initiates a connection.	Connecting	Accepting
The connection is established.	Activated	Activated
The connection is suspended.	Suspending	Suspending
The connection is broken.	Suspended	Suspended
A connection is re-initiated.	Activating	Activating
The connection is established.	Activated	Activated

1.2 Interconnect two VPCs

You can interconnect two VPCs by creating a peering connection between them.

Context



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](#).

Procedure

1. 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.

Configuration	Description
Account	<p>Select whether the VPCs you want to connect belong to the same account.</p> <ul style="list-style-type: none">· Same as Peer's: If the VPCs to be connected belong to the same account, the system creates an initiator instance and an acceptor instance at the same time, and automatically establishes a connection between them.· Different from Peer's: If the VPCs to be connected belong to different accounts, you must create an initiator instance and an acceptor instance separately before initiating the connection from the initiator instance.
Connection Type	<p>Select the peering connection type:</p> <ul style="list-style-type: none">· VPC-to-VPC: Establish a peering connection between two VPCs.· VBR-to-VPC: Establish a peering connection between a VPC and a VBR. For more information, see Interconnect a VPC and a VBR. <p>In this example, select VPC-to-VPC.</p>

Configuration	Description
Routers to Create	<p>Select the instances to be created:</p> <ul style="list-style-type: none"> · Initiator and Acceptor: Both an initiator instance and an acceptor instance are created. After the creation, the initiator instance automatically connects to the acceptor instance. This option applies only to connections under the same account. · Create Initiator: An initiator instance is created and the initiator instance can initiate the connection actively. The initiator router type can be VPC or VBR. If VBR-to-VPC is selected for the peering connection type, only VBR is available for the initiator router type. This option applies only to connections between different accounts. · Acceptor Only: An acceptor instance is created. Only VPC is available for the acceptor router type. This option applies only to connections between different accounts. <div style="background-color: #f0f0f0; padding: 10px; margin-top: 10px;">  Note: Only Pay-As-You-Go billing supports creating an acceptor separately. The acceptor instance is free of charge. </div>
Local VPC ID	Select the ID of the local VPC (the initiator or the acceptor of the connection).
Local Region	Select the region of the local VPC.
Peer VPC ID	Select the ID of the peer VPC (the initiator or the acceptor of the connection).
Peer Region	Select the region of the peer VPC.
Bandwidth	Select a bandwidth for the connection. Use the default bandwidth for the acceptor instance.

Configuration	Description
Validity	Select a validity period for your subscription. If you want the subscription to automatically renew when it expires, select the Auto Renew check box.

1.3 Interconnect a VPC and a VBR

You can fulfill intercommunication between a VPC and a Virtual Border Router (VBR) by creating a peering connection.

Procedure

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.


Configuration	Description
Account	Select whether the VPC and the VBR you want to connect belong to the same account. Select a validity period for your subscription. <ul style="list-style-type: none"> · Same as Peer's : If the VPC and VBR to be connected belong to the same account, the system creates an initiator instance and an acceptor instance at the same time, and automatically establishes a connection between them. · Different from Peer's: If the VPC and VBR to be connected belong to different accounts, you need to create an initiator instance and an acceptor instance respectively before initiating the connection from the initiator instance.
Connection Type	Select the peering connection type: <ul style="list-style-type: none"> · VPC-to-VPC: Establish a peering connection between two VPCs. · VBR-to-VPC: Establish a peering connection between a VPC and a VBR. <p>In this example, select VBR-to-VPC.</p>

Configuration	Description
Routers to Create	<p>Select the instances to be created:</p> <ul style="list-style-type: none"> · Initiator and Acceptor: Both an initiator instance and an acceptor instance are created. After the creation, the initiator instance automatically connects to the acceptor instance. This option applies only to connection under the same account. · Initiator Only: The initiator instance is created and the initiator instance can initiate the connection actively. If VBR-to-VPC is selected for the connection type, only VBR is available for the route type of the initiator. This option applies only to connection between different accounts. · Acceptor Only: An acceptor instance is created. Only VPC is available for the acceptor router type. This option applies only to connection between different accounts.
Local Region	Select the region of the VBR.
Local Access Point	Select the access point to which the VBR connects.
Local VBR ID	Select the VBR to which you want to establish the connection .
Peer Region	Select the region of the peer VPC.
Peer VPC ID	Select the ID of the peer VPC.
Bandwidth	Select a bandwidth for the connection. Use the default bandwidth for the acceptor instance.
Validity	Select a validity period for your subscription. If you want the subscription to automatically renew when it expires, select the Auto Renew check box.

1.4 Manage Subscription instances

You can change the bandwidths of your Subscription instances and pay for the change.

Procedure

1. Log on to the [Express Connect](#) console.
2. In the left-side navigation pane, click VPC Peering Connections > VPC-to-VPC or VPC Peering Connections > VBR-to-VPC.
3. Select the region where your instance is located and find your target instance.
4. Click  and select the operation you want to perform:
 - **Renew:** When the initiator instance is overdue for more than 24 hours, the physical connection interface stops forwarding data and is locked. To avoid affecting your business, we recommend that you renew your account in a timely manner.
 - **Renew and Upgrade/Downgrade:** Change the bandwidth while you renew your account. The change takes effect in the next billing cycle.
 - **Upgrade:** Increase the bandwidth of the initiator instance.
 - **Suspend Initiator/Acceptor:** Suspend the activated instance. Data will no longer be forwarded after the suspension.
 - **Activate Initiator/Acceptor:** Activate the suspended instance. Data forwarding will be restored after the activation.

1.5 Delete peering connections

Before you can delete a peering connection, you must first delete the route entries of its initiator and acceptor.

Step 1: Delete route entries




Perform the following steps to delete the custom route entries:

1. Log on to the [Express Connect](#) console.
2. In the left-side navigation pane, click PVC Peering Connections > VPC-to-VPC.
3. Select a region and find your target peering connection.
4. Click the VPC ID of the initiator. On the VPC Details page, click the VPC ID again.

5. In the Network Resources area, click the route table link. On the displayed Route Tables page, click the route table ID.
6. Find the custom route entry destined for the local IDC and then click Delete.
7. In the displayed dialog box, click OK.
8. Repeat the preceding steps to delete the route entries of the acceptor.

Step 2: Delete the peering connection

Perform the following steps to delete the 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 and find your target peering connection.
4. Click  > Suspend Initiator. In the displayed dialog box, click Confirm.
5. Click  > Suspend Acceptor. In the displayed dialog box, click Confirm.
6. Click  > Delete. In the displayed dialog box, click Confirm.

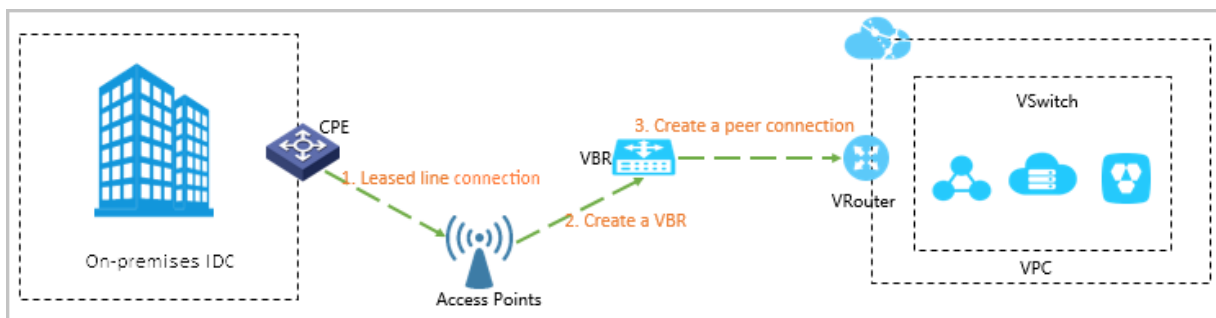
2 Physical connection

2.1 Physical connection process

By using a leased line from your service provider, you can connect your on-premises IDC to an Alibaba Cloud access point to build hybrid clouds and expand your local network.

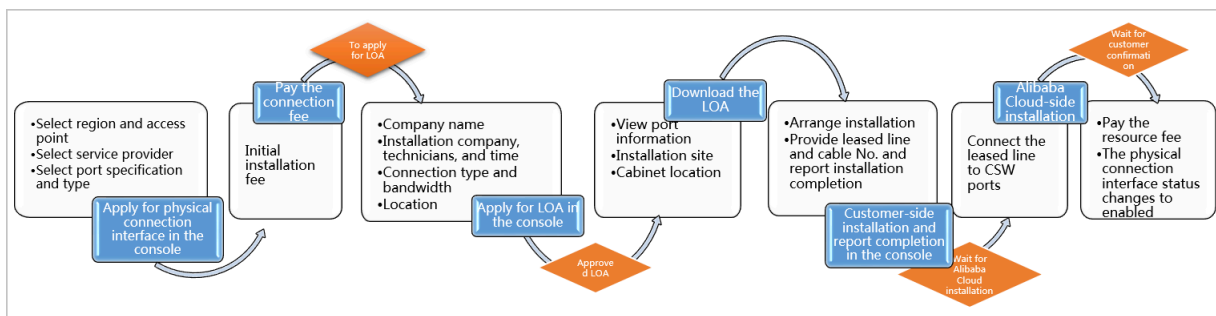
Physical connection process

As shown in the following figure, after connecting your on-premises IDC to the nearest Alibaba Cloud access point through a leased line from your service provider, you need to create a VBR for the leased line as a router between the local Customer-Premises Equipment (CPE) and the VPC. Then, you need to add the VBR to the Cloud Enterprise Network, or establish a peering connection between the VBR and the VPC so that the IDC can communicate with other VPCs.



Leased line connection process

To establish a physical connection, you must first connect the leased line to an access point. The process is shown in the following figure.



2.2 Apply for leased line connection

You need to connect the leased line from your service provider to an Alibaba Cloud access point before you can establish a physical connection.

Prerequisites

Before applying for leased line connection, pay attention to the following restrictions:

- Physical connections do not support interfaces of SDH 155M CPOS, V.35, or G.703.
- Alibaba Cloud provides multiple access points in all regions, except for the China North 1 (Qingdao) and US (Silicon Valley) regions. Different access points have different service provider restrictions. For more information, see [Access points](#).

Procedure

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 physical connection interface, and complete the payment for an initial installation fee.


Configuration	Description
Region	Select the region where the leased line is deployed.
SP	Select the service provider of the leased line.
Access Point	Select the nearest access point to your on-premises IDC. Access points are Alibaba Cloud IDCs in different regions. Each region has one or more access points. Different access points correspond to different access locations and have different access capabilities. You can open a ticket to obtain detailed information about the location of access points.
Port Specification	Port specifications include 1G and below, 10G, 40G, and 100G. If you select 40G or 100G, you need to enable a whitelist. Note that different specifications incur different resource fees.
Port Type	Select the access port type. Available port types vary according to the selected access point. The console will display the available port types accordingly.

Configuration	Description
Redundancy	<p>Select a required physical connection to provide an Equal-Cost Multi-Path routing (ECMP) redundant link for this leased line. Two physical connections accessing the same region can be used as redundant physical connections.</p> <ul style="list-style-type: none"> · When accessing different access points, both physical connections naturally provide redundancy to each other. · When both physical connections access the same access point, you need to specify one as the redundancy of the other. Redundant physical connections are allocated to different physical access devices.

5. Go back to 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.

6. Click Apply for LOA in the Actions column.
7. On the Apply for LOA page, enter the leased line connection information, and click Add Field Engineer to add the information of a data center cable installation technician or representative. Multiple technicians can be added.

Configuration	Description
Company Name	Enter the company name that you set when you registered your account.
Construction Company	Enter the name of your designated data center cable installation company.
Construction Type	Select the required leased line type: MSTP, MPLSVPN, FIBRE , or Others.
Scheduled Construction Time	Set the date and time when the data center cable installation technician or representative from the installation company will go to complete the leased line connection at the Alibaba Cloud IDC site.
Location	Optional. Enter the location of your on-premises IDC.
Bandwidth	<p>Optional. Enter the bandwidth of the leased line.</p> <div style="background-color: #f0f0f0; padding: 5px;">  Note: The bandwidth value you enter does not affect the fees charged to your account or your usage of the leased line. </div>

8. Click OK. Your application is then sent to Alibaba Cloud personnel for review, and the physical connection interface enters the In Application state.
9. After the application is approved, download the LOA in the console.

The physical connection interface enters the Approved LOA state. Click View LOA in the Actions column to view the installation information, such as the location of Alibaba Cloud IDC site, cabinet location, and port information.

10. At this stage, we recommend that you instruct your installation company to start installation. 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 Alibaba Cloud IDC, and click OK.

The physical connection interface enters the Waiting state.

11. 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.

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

13. After payment, the physical connection interface changes to the Enabled state, indicating that the leased line connection is completed.

Physical Connection Interfaces							Help Document
Instance ID/Name	Access Point	Service Provider	Port Spec	Billing Method	Status	Actions	
pc-bp-leaser	Hangzhou-Yuhang-A	China Unicom	1G	Expires at Mar 29, 2019, 00:00:00	Enabled	Renew Auto Renew	



Note:

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

2.3 Create redundant physical connections

You can use two physical connections to connect an on-premises IDC to Alibaba Cloud. In this way, a high-quality and highly reliable intranet communication can be established between the on-premises IDC and Alibaba Cloud.

Example

This topic takes the following scenario as an example to describe how to connect an on-premises IDC to Alibaba Cloud through redundant physical connections.

A company has an on-premises IDC (CIDR block: 172.16.0.0/12) in Beijing, and has a VPC (CIDR block: 192.168.0.0/16) in the China (Beijing) region. To solve the issue of Single Points of Failure (SPOFs), the company plans to apply for two physical connections that are provided by two different service providers to connect the on-premises IDC to Alibaba Cloud.

Step 1: Apply for a physical connection interface

Set the name of this first physical connection interface to `leasedline1`. This topic provides only general configuration information. For detailed configuration information, see [Apply for leased line connection](#).

1. Apply for a physical connection interface and pay the initial installation fee.
 - **Region:** Select the region where the leased line is deployed.
 - **SP:** Select the service provider of your leased line. In this example, select China Unicom.
 - **Access Point:** Select an access point that is closest in geographical proximity to your on-premises IDC. In this example, select Qingdao-Laoshan-A-CU.
 - **Port Specification:** Select the required 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:** Select None.
2. Click **Apply for LOA** in the **Actions** column.
3. Enter your company name, the name of the data center cable installation company, the scheduled installation date and time, and the contact information of data center cable installation technician or representative, and select a construction type.

4. 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.
5. After the installation is complete, click Delivery Report on the Physical Connection Interfaces page, enter the leased line code and the label numbers of cables at the installation site, and click OK. The physical connection interface enters the Waiting state.
6. Alibaba Cloud will connect the cables to the corresponding CSW ports according to the information you provided. After you confirm that the physical connection interface has been deployed, pay the resource fee. When the physical connection interface changes to the Enabled state, the leased line connection is completed.

Step 2: Apply for a second physical connection interface

Set the name of the second physical connection interface to leasedline2. This topic provides only general configuration information. For detailed configuration information, see [Apply for leased line connection](#).

1. Apply for a physical connection interface and pay the initial installation fee.
 - **Region:** Select the region where the leased line is deployed.
 - **Access Point:** Select an access point that is closest in geographical proximity to your on-premises IDC. In this example, select Qingdao-Laoshan-A-CU.
 - **SP:** Select the service provider of your leased line. In this example, select China Unicom.
 - **Port Specification:** Select the required 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:** Select the first physical connection interface you have applied for. Make sure that you have paid the initial installation fee.



Note:

- If the access point of the second physical connection interface is the same as that of the first physical connection interface, select the ID of the first

physical connection. Make sure that you have paid the initial installation fee for the first physical connection.

- If the access point of the second physical connection interface is different from that of the first physical connection interface, the two connections create a redundant connection by default, so you do not need to select a physical connection ID.

2. Click Apply for LOA in the Actions column.
3. Enter your company name, the name of the data center cable installation company, the scheduled installation date and time, and the contact information of data center cable installation technician and representative, and select a construction type.
4. 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.
5. After the installation is complete, click Delivery Report on the Physical Connection Interfaces page, enter the leased line code and the label numbers of cables at the installation site, and click OK. The physical connection interface enters the Waiting state.
6. Alibaba Cloud will connect the cables to the corresponding CSW ports according to the information you provided. After you confirm that the physical connection interface has been deployed, pay the resource fee. When the physical connection interface changes to the Enabled state, the leased line connection is completed.

Step 3: Create a VBR

To create a VBR, follow these steps:

1. On the Virtual Border Routers page, click Create VBR.

2. Configure the VBR. The VBR configurations in this example are as follows:

- **Account:** Select Current Account.
- **Name:** Enter vbr1.
- **Physical Connection Interface:** Select the first physical connection interface.
- **VLANID:** Enter 2333.
- **Gateway IP Address on Alibaba Cloud Side:** Enter 10.0.0.1.
- **Gateway IP Address on Customer Side:** Enter 10.0.0.2.
- **Subnet Mask:** Enter 255.255.255.252.

3. Repeat the preceding steps to create a VBR named vbr2 for the second physical connection interface.

The screenshot shows the 'Virtual Border Routers (VBRs)' management page. It includes a 'Create VBR' button and a 'Refresh' button. Below is a table listing the VBR instances:

Instance ID/Name	Access Point	Physical Connection Interface	Route Table	VLAN ID	Status	Actions
vbr-m5e836f9mr vbr2	Qingdao-Laoshan-A	pc-m5e1k419n	vtb-m5equtyjz3	244	Active	Edit Delete
vbr-m5eqpkru8u vbr1	Qingdao-Laoshan-A	pc-m5emcb6n	vtb-m5erwi2pq	2333	Active	Edit Delete

Step 4: Establish a peering connection

To establish a peering connection between your VBR and your VPC, follow these steps:

1. On the VPC Peering Connections page, click Create Peering Connection.
2. Configure the peering connection. The configurations in this example are as follows:
 - **Connection Type:** Select VBR-to-VPC.
 - **Routers to Create:** Select Initiator and Acceptor.
 - **Local Region:** Select the region of the VBR. In this example, select China (Beijing).
 - **Local VBR ID:** Select the created VBR.
 - **Peer Region:** Select the region to which the VPC belongs. In this example, select China (Beijing).
 - **Peer VPC ID:** Select the VPC to be connected.
 - **Bandwidth:** In this example, select 100 Mb.
3. Go back to the VPC Peering Connections page to view the status of the peering connection. The connection is successfully established if the status of both the acceptor and the initiator is activated.

4. Repeat the preceding steps to establish a peering connection between the other VBR and the VPC.

Monitor	Initiator	Initiator Region	Acceptor	Acceptor Region	Belong to Same Account	Specification	Billing Method	Status
Route Settings	vbr-m5e836f5mn-167q ri-m5e7wn600ba-1pe4	Qingdao-Laoshan-A	vpc-m5e2n7bpw-1eaznt ri-m5eg41n9j8-1335	China (Qingdao)	Yes	100Mbps	Pay-As-You-Go Created at Dec 21, 2018, 16:09:59 Connected at Dec 21, 2018, 16:09:39	Initiator: Activated Acceptor: Activated
Route Settings	vbr-m5egqkru8u-13b ri-m5eng082y2b-1qj	Qingdao-Laoshan-A	vpc-m5e2n7bpw-1eaznt ri-m5eg41n9j8-1335	China (Qingdao)	Yes	100Mbps	Pay-As-You-Go Created at Dec 21, 2018, 13:57:05 Connected at Dec 21, 2018, 13:57:47	Initiator: Activated Acceptor: Activated

Step 5: Configure routes

After establishing the peering connections, you must configure a route in the VPC that points to the on-premises IDC in the VPC, and configure two routes pointing to the VPC and the on-premises IDC respectively. Lastly, you must add a route pointing to the VPC in the access device of the on-premises IDC.

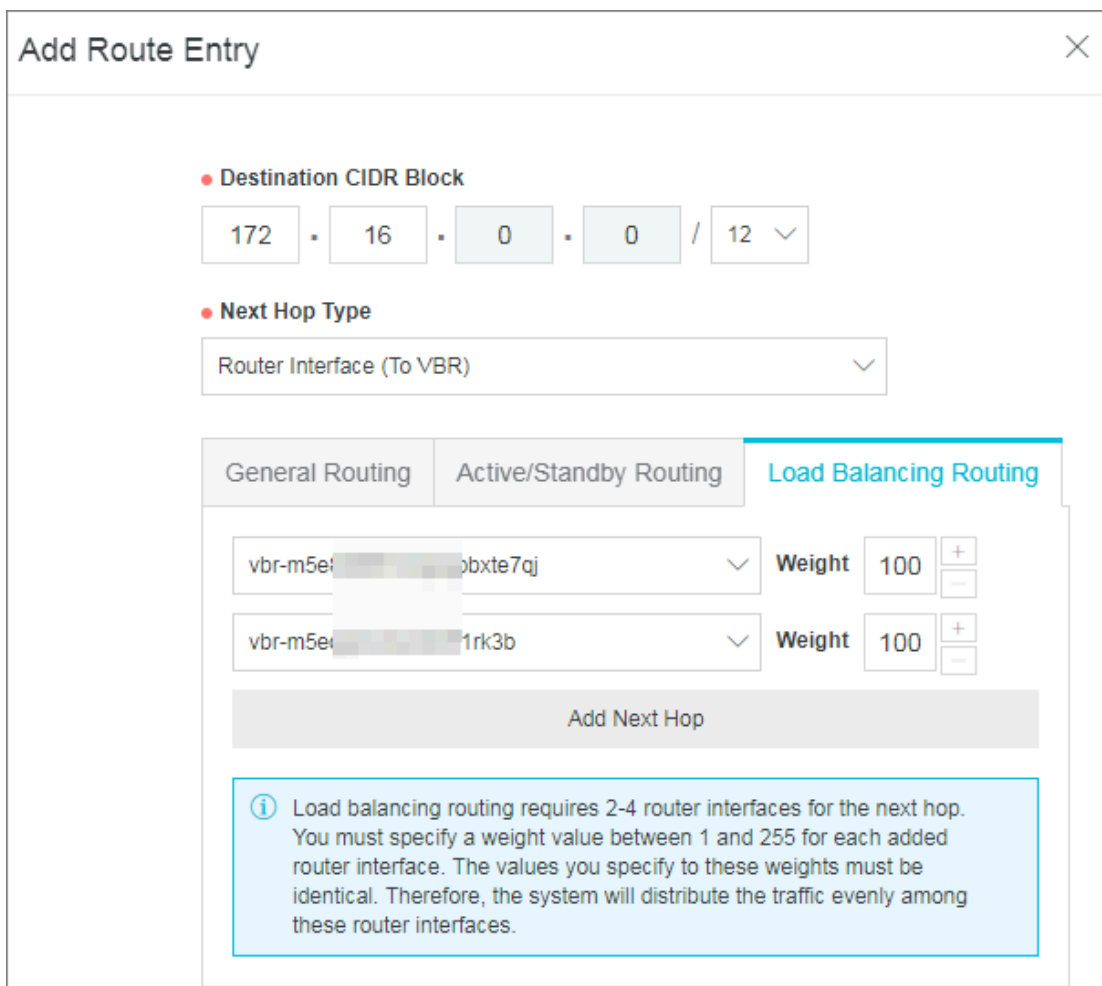
To configure the routes, follow these steps:

1. To configure routes for a VBR:

- a. On the VBR details page, click the Routes tab page, and then click Add Route.
- b. Add a route directing to the VPC:
 - Destination Subnet: Enter the CIDR block of the VPC. In this example, enter 192.168.0.0/16.
 - Next Hop Type: Select VPC.
 - Next Hop: Select the VPC.
- c. Add a route pointing to the physical connection:
 - Destination Subnet: Enter the CIDR block of the on-premises IDC. In this example, enter 172.16.0.0/12.
 - Next Hop Type: Select Physical Connection Interface.
 - Next Hop: Select the physical connection interface.
- d. Repeat the preceding steps to configure routes for the other VBR.

2. To configure a route for the VPC:

- a. On the VPC Peering Connections page, find the created peering connection, and click the VPC ID of the acceptor to open the VPC Details page. Here, you can view the ID of the route table.
- b. On the [Route Tables](#) page, click the target route table ID, and then click Add Route Entry.
- c. Configure a route:
 - Destination CIDR Block: Enter the CIDR block of the on-premises IDC. In this example, enter 172.16.0.0/12.
 - Next Hop Type: Select Router Interface (To VBR).
 - Next Hop: Select Load Balancing Routing, and then select the created VBR.



d. Configure a route for the on-premises IDC.

You can configure a static route or BGP dynamic routing to forward data between the on-premises IDC to VBR:

- Static route

Example:

```
ip route 192 . 168 . 0 . 0 / 16 10 . 100 . 0 . 1
```

- Dynamic routes

You can also use BGP to forward data between the on-premises IDC and the VBR. For more information, see [Configure BGP](#).




Note:

The advertised CIDR block must be the CIDR block of the VPC that will be used to communicate with the on-premises IDC. In this example, enter 192.168.0.0/16.

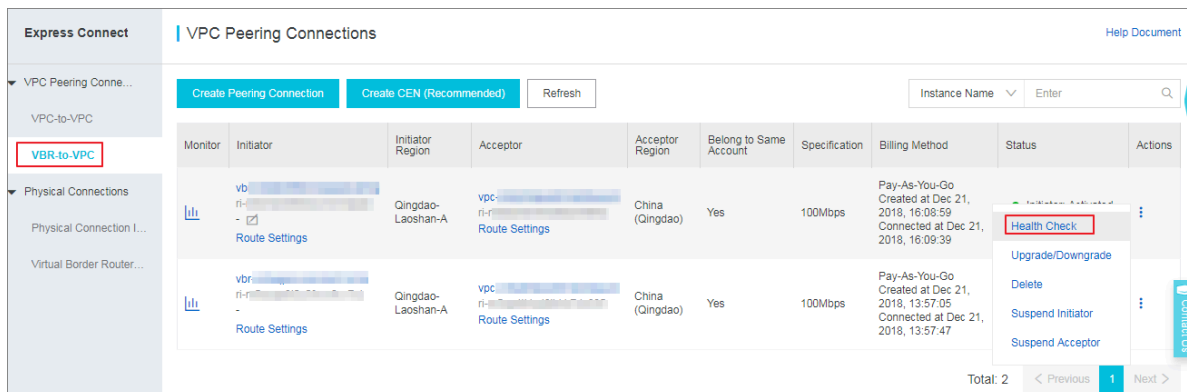
Step 6: Configure health checks

You must configure the health check settings for redundant physical connections. Alibaba Cloud sends a ping packet once every two seconds from each health check IP address to the customer-side IP address of the on-premises IDC. If eight ping packets on one physical connection are sent in succession, and all packets fail to respond, the traffic is switched to the other physical connection.

To configure the health check, follow these steps:

1. On the VBR-to-VPC page, locate the created peering connection, and then click 

> Health Check.



Monitor	Initiator	Initiator Region	Acceptor	Acceptor Region	Belong to Same Account	Specification	Billing Method	Status	Actions
	vb- ri- -	Qingdao-Laoshan-A	vpc- ri- -	China (Qingdao)	Yes	100Mbps	Pay-As-You-Go Created at Dec 21, 2018, 16:08:59 Connected at Dec 21, 2018, 16:09:39	Connected	Health Check Upgrade/Downgrade Delete Suspend Initiator Suspend Acceptor
	vbr- ri- -	Qingdao-Laoshan-A	vpc- ri- -	China (Qingdao)	Yes	100Mbps	Pay-As-You-Go Created at Dec 21, 2018, 13:57:05 Connected at Dec 21, 2018, 13:57:47	Connected	

2. Click Configure, complete the following configurations and then click OK.
 - Source IP: Enter an idle IP of the VSwitch in the connected VPC.
 - Destination IP: Enter the interface IP address of the network device of the on-premises IDC.
3. Repeat the preceding steps to configure a health check for the other peering connection.

2.4 Delete a physical connection

When you no longer need a physical connection, you can delete it by following the steps provided in this topic.



Note:

To delete a physical connection, you must use the following sequence.

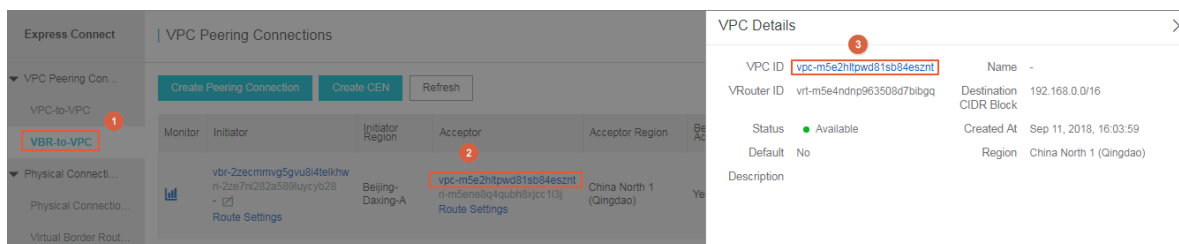
1. Delete the route entries configured in the VBR and the VPC router.
2. Delete related BGP peers and BGP groups if BGP routing is configured.
3. Delete the peering connection between the VPC and the VBR.
4. Delete all associated VBRs.
5. Delete the physical connection.

Follow these steps to delete a physical connection:

Step 1: Delete route entries

Follow these steps to delete the custom route entries in the VPC and VBR:

1. Log on to the [Express Connect](#) console.
2. In the left-side navigation pane, click VPC Peering Connections > VBR-to-VPC.
3. Select the region where your VBR-to-VPC connection is located and find the connection.
4. Click the ID of the acceptor VPC. On the VPC Details page, click the VPC ID again.



5. In the Network Resources area, click the route table link. Then click the route table ID.
6. Locate the custom route entry destined for the on-premises IDC and then click Delete.
7. In the displayed dialog box, click OK.
8. In the left-side navigation pane, click Physical Connections > Virtual Border Routers (VBRs).
9. Select the region of the VBR and then click the ID of the target VBR instance.
10. Click the Route Entries tab.
11. Delete the route entries added in the VBR.




Step 2: Delete BGP peers and BGP groups

If you have configured BGP, follow these steps to delete the BGP configurations associated with the VBR:

1. Log on to the [Express Connect](#) console.
2. In the left-side navigation pane, click Physical Connections > Virtual Border Routers (VBRs).
3. Select the region of the VBR and then click the ID of the target VBR instance.
4. Click the BGP Peers tab and then delete the created BGP peers.
5. Click the BGP Groups tab and then delete the created BGP groups.
6. Click the BGP CIDR Blocks tab and then delete the added BGP CIDR blocks.

Step 3: Delete peering connections

Follow these steps to delete the peering connection between the VBR and the VPC:

1. Log on to the [Express Connect](#) console.
2. In the left-side navigation pane, click VPC Peering Connections > VBR-to-VPC.
3. Select the region where your VBR-to-VPC connection is located and find the connection.
4. Click  > Suspend Initiator. In the displayed dialog box, click Confirm.
5. Click  > Suspend Acceptor. In the displayed dialog box, click Confirm.
6. Click  > Delete. In the displayed dialog box, click Confirm.

Step 4: Delete the VBRs

Follow these steps to delete the VBRs:

1. Log on to the [Express Connect](#) console.
2. In the left-side navigation pane, click Physical Connections > Virtual Border Routers (VBRs).
3. Select the region where the VBR is located.
4. Find the target VBR and click Delete.
5. In the displayed dialog box, click Confirm.

Step 5: Delete the physical connection

You need to submit a ticket to apply for the deletion of a physical connection. After the physical connection is deleted, you will receive a refund of the resource fee.

2.5 Access points

You can use the leased line provided by your local service provider to access the cloud resources deployed on Alibaba Cloud through access points. Open a ticket or contact your customer manager if you need more information.

Access points in Mainland China

Area	Country (Region)	Access point	Service provider
Mainland China	China (Qingdao)	Qingdao-Laoshan-A	China Unicom
	China (Beijing)	Beijing-Daxing-A	GDS Services
		Beijing-Daxing-B	China Unicom
		Beijing-Changping-A	China Telecom
		Beijing-Yizhuang-A	21vianet
		Beijing-Yizhuang-B	China Unicom
		Beijing-Yizhuang-C	China Mobile
		Beijing-Fengtai-A	CNIX
		Beijing-Shunyi-A	China Telecom
	China (Zhangjiakou)	Zhangjiakou-Xiaoertai-A	Alibaba Cloud

Area	Country (Region)	Access point	Service provider
		Zhangjiakou-Miaotan-A	Alibaba Cloud
	China (Hohhot)	Hohhot-Shengle-A	China Telecom
		Hohhot-Xincheng-A	China Unicom
	China (Hangzhou)	Hangzhou-Yuhang-A	Alibaba Cloud
		Hangzhou-Linan-A	Watone Cloud
		Hangzhou-Xiaoshan-A	China Unicom
		Hangzhou-Xiaoshan-B	China Telecom
		Hangzhou-Xiaoshan-D	China Mobile
		Hangzhou-Jianggan-B	21vianet
		Hangzhou-Deqing-A	China Unicom
		China (Shanghai)	Shanghai-Baoshan-A
	Shanghai-Baoshan-B		China Unicom
	Shanghai-Baoshan-C		21vianet
	Shanghai-Pudong-A		China Mobile
	Shanghai-Pudong-B		China Telecom
	Shanghai-Pudong-D		China Unicom
	Shanghai-Jiading-A		China Telecom
	China (Shenzhen)	Shenzhen-Futian-A	GDS Services
		Shenzhen-Longhua-A	China Telecom
		Shenzhen-Yantian-A	China Unicom
		Shenzhen-Nanshan-A	21vianet

Area	Country (Region)	Access point	Service provider
		Shenzhen-Longgang-A	China Mobile

Access points outside Mainland China

Area	Country (Region)	Access point	Service provider
Asia Pacific	China (Hong Kong)	HK-KwaiChung-A	Equinix
		HK-ChaiWan-B	MEGA
		HK-Fanling-C	PCCW
	Singapore	Singapore-A	Equinix
		Singapore-B	GlobalSwitch
		Singapore-C	DRT
	Australia (Sydney)	Australia-Sydney-A	GlobalSwitch
		Australia-Sydney-B	Equinix
	Malaysia (Kuala Lumpur)	Malaysia-KualaLumpur-A	NTT
		Malaysia-KualaLumpur-B	AIMS
	Indonesia (Jakarta)	Indonesia-Jakarta-A	DCI
		Indonesia-Jakarta-B	NTT
	Japan (Tokyo)	Japan-Tokyo-A	Equinix
		Japan-Tokyo-B	Equinix
		Japan-Tokyo-C	NEC
Europe and America	US (Silicon Valley)	US-San Jose-A	Equinix
	US (Virginia)	US-Ashburn-A	Equinix
		US-Virginia-D	Coresite
	Germany (Frankfurt)	Germany-Frankfurt-A	E-shelter
		Germany-Frankfurt-B	Equinix
	UK (London)	UK-London-A	DRT
		UK-London-B	ARK
		UK-London-C	Telehouse

Area	Country (Region)	Access point	Service provider
		UK-London-D	Equinix
Middle East and India	UAE (Dubai)	UAE-Dubai-A	Equinix
		UAE-Dubai-B	Khazna
	India (Mumbai)	India-Mumbai-A	CtrlS
		India-Mumbai-B	GPX
		India-Mumbai-C	NM

2.6 NSP partners

If your local infrastructure is not within the reach of Alibaba Cloud Express Connect, or if your data does not require a large bandwidth connection, you can use Alibaba Cloud's growing NSP partners to help you build a physical connection to connect your on-premises data center to Alibaba Cloud.

The following table lists the NSP partners of Alibaba Cloud. They can help you establish a network connection between Alibaba Cloud access points and your on-premises data center to build a hybrid cloud.



Note:

You must sign contracts with and obtain services from third-party network service providers when using NSP partners to access Alibaba Cloud. Furthermore, the NSP partners that you sign agreements with are deemed responsible for service guarantees as defined in the SLA, in addition to being responsible for providing one or more solutions to any service issues that result from use of NSP partner networks. Alibaba Cloud holds no responsibility for actions resulting from use of NSP partner networks.

Partner	Mainland China	Hong Kong	Tokyo	Singapore	Sydney	Frankfurt	San Jose	Ashburn	Dubai
China Unicom	#	—	—	—	—	—	—	—	—
China Telecom Global	—	#	—	—	—	#	—	—	—

Partner	Mainland China	Hong Kong	Tokyo	Singapore	Sydney	Frankfurt	San Jose	Ashburn	Dubai
China Unicom Global	—	#	—	—	—	—	—	—	—
Epsilon	—	—	—	#	—	—	—	#	#
GTT	—	—	—	#	—	—	—	—	—
TATA	—	#	—	#	—	—	—	—	—
Megaport	—	#	—	#	#	—	#	#	—
PCCW	—	#	—	#	—	—	—	—	—
Reliance	—	—	—	#	—	—	—	—	—
SingTel	—	—	—	#	—	—	—	—	—
Vodafone	—	—	—	—	—	#	—	—	—
SoftBank	—	—	#	—	—	—	—	—	—
Intercloud	—	—	—	—	—	#	—	—	—
Equinix	—	#	—	#	#	#	#	#	—
HGC	—	#	—	—	—	—	—	—	—
NextDC	—	—	—	—	#	—	—	—	—

3 Virtual border router

3.1 Create a virtual border router

After establishing a physical connection, you need to create a Virtual Border Router (VBR) for the leased line as a forwarding bridge for data from the VPC to your local IDC.

Context

VBR is a router between the VPC and the Custom-Premises Equipment (CPE) in your local IDC. VBR has a route table. You can configure route entries in the route table to forward traffic. VBR provides the following functions:

- Exchanges data packets as an intermediate router between the VPC and the local IDC.
- Decides the port mode of the physical connection: Layer-3 route interface mode or VLAN-based Layer-3 sub-interface mode.
- Attaches or identifies VLAN tags in Layer-3 sub-interface mode.
- Supports BGP dynamic routing.

Procedure

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.
4. Configure the VBR, and then click OK.

Configuration	Description
Belongs to Current Account	Create a VBR for all physical connections under the same account or a different account.
Account	If you want to create a VBR for the physical connections under a different account, enter the account ID of the physical connection owner.

Configuration	Description
VLAN ID	<p>Enter the VLAN ID of the VBR, ranging from 0 to 2999.</p> <ul style="list-style-type: none"> When the VLAN ID is 0, it indicates that the switch port of the VBR uses Layer-3 route interface mode instead of VLAN mode. In Layer-3 route interface mode, each physical connection corresponds to a VBR. When the VLAN ID is a value from 1 to 2999, it indicates that the switch port of the VBR uses VLAN-based Layer-3 sub-interface mode. In Layer-3 sub-interface mode, each VLAN ID corresponds to a VBR. In this mode, the physical connection of the VBR can connect the VPCs under multiple accounts. The VBRs of different VLANs are isolated from one another by the Layer-2 network. <p>For example, a company has multiple subdivisions or subsidiaries. Each has an independent Alibaba Cloud account, and each account has an independent VPC. If the company applies for a physical connection, it needs to plan a VLAN ID for each subdivision or subsidiary. When creating router interfaces, the company uses VLAN IDs to identify the subsidiaries or subdivisions that use the physical connection, isolating them from each other by using the Layer-2 network.</p>
Gateway IP Address on Alibaba Cloud Side	Enter the IP address of the gateway from the VPC to your local IDC.
Gateway IP Address on Customer Side	Enter the IP address of the gateway from your local IDC to the VPC.
Subnet Mask	Enter the subnet mask of the gateway IP address on the Alibaba Cloud side and the gateway IP address on the customer side. Only two IP addresses are required. Therefore, you can enter a longer subnet mask.

3.2 Configure BGP

You can establish Border Gateway Protocol (BGP) routing between a local IDC and a Virtual Border Router (VBR). You only need to add BGP peers that communicate with

the VBR to the corresponding BGP group, and then add the BGP CIDR block to the VBR.

**Note:**

Express Connect allows you to establish BGP routing only between a VBR and a local IDC. In the VBR, you must add a route entry destined for the physical connection and a route entry destined for the VPC. For more information, see [Add route entries](#).

BGP overview

BGP is a dynamic routing protocol based on TCP. It is mainly used to exchange routing and network accessibility information among ASs. You can use BGP to implement intranet connection between the local IDC and VBR for physical connections. BGP can help you build hybrid clouds in a more efficient, flexible, and reliable manner.

Before configuring BGP, you need to create a BGP group. BGP groups are used to simplify BGP configurations. Combining repeated configurations into a BGP group can make configurations easier. You only need to create a BGP group according to the ASN and add qualified BGP peers to the group. The added BGP peers will inherit the configurations of the BGP group. You do not need to configure the BGP peers separately.

Limits

BGP has the following limits:

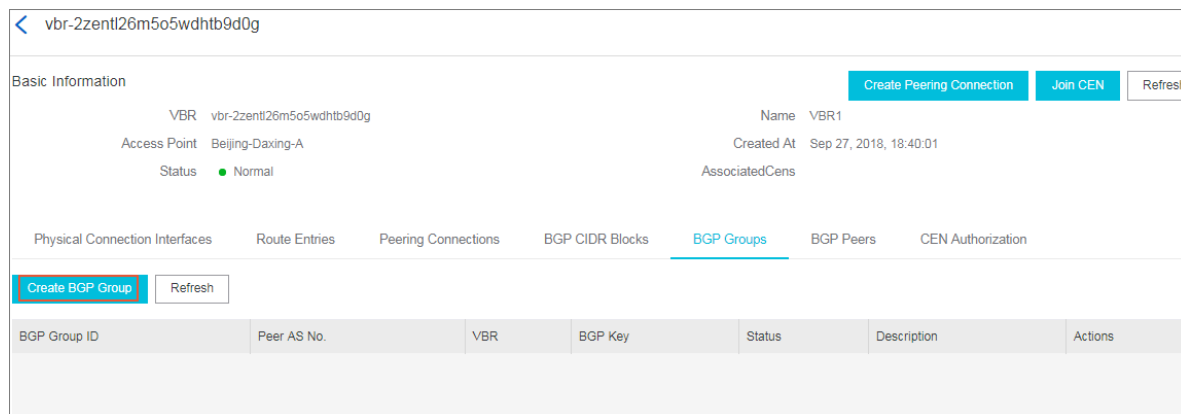
- VBR can establish BGP peers only with the peer local IDC. Static routing is still required between the VBR and the VPC.
- The supported BGP version is BGP4.
- VBR supports IPv4 BGP, but does not support IPv6 BGP.
- A maximum of eight BGP peers can be created under each VBR.
- A maximum of 100 dynamic route entries can be added to a BGP peer.
- The Autonomous System Number (ASN) of Alibaba Cloud is 45104. It supports the transmission of 2-byte or 4-byte ASNs from the customer side.

Step 1: Create a BGP Group

Before configuring BGP routing, you need to create a BGP group based on the requested ASN.

To create a BGP group, 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. Select a region and click the ID of the target VBR.
4. Click the BGP Groups tab, and then click Create BGP Group.



5. Configure the BGP group, and then click OK.

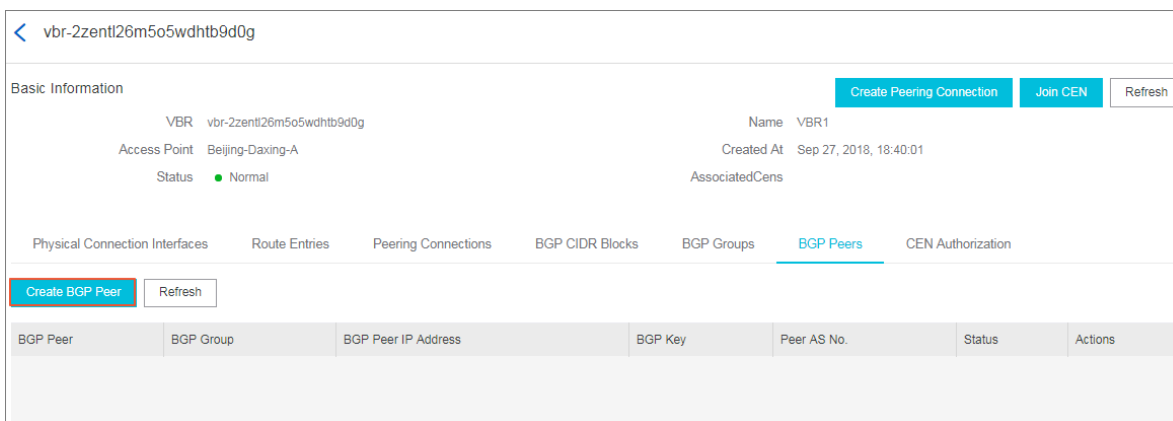
Configuration	Description
Name	Name of the BGP group
Peer ASN	AS number of the local IDC network
BGP Key	Key of the BGP group
Description	Description of the BGP group

Step 2: Add a BGP peer

To add a BGP peer, 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. Select a region and click the ID of the target VBR.

4. Click the BGP Peers tab page, and then click Create BGP Peer.



5. Configure the BGP peer, and then click OK.

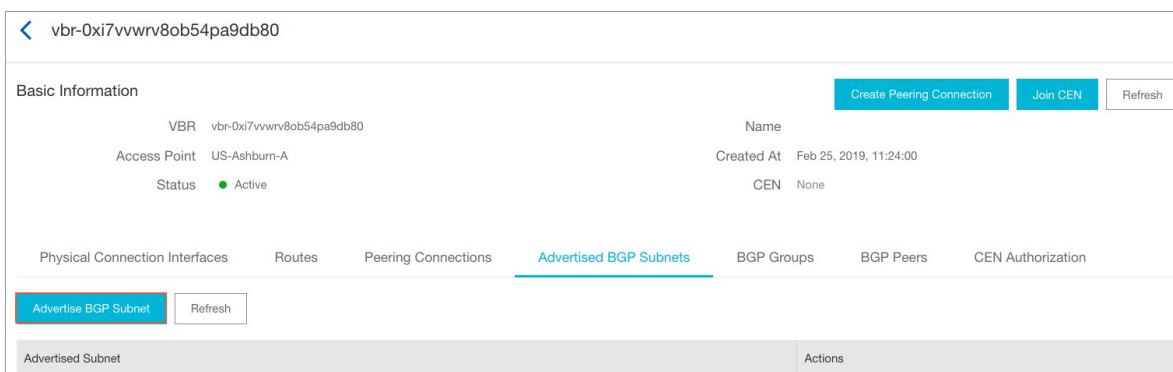
Configuration	Description
BGP Group	BGP group to which you want to add the BGP peer
BGP peer IP Address	IP address of the BGP peer

Step 3: Add the BGP CIDR block

After configuring the BGP peer, you need to add the CIDR block of the local IDC.

To add the CIDR block of the local IDC, 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. Select a region and click the ID of the target VBR.
4. Click the BGP CIDR Blocks tab, and then click Advertise BGP Subnet.



5. Enter the CIDR block to be added, and then click OK.

3.3 Add route entries

VBR has a route table. You can configure route entries in the route table to forward traffic.

Context

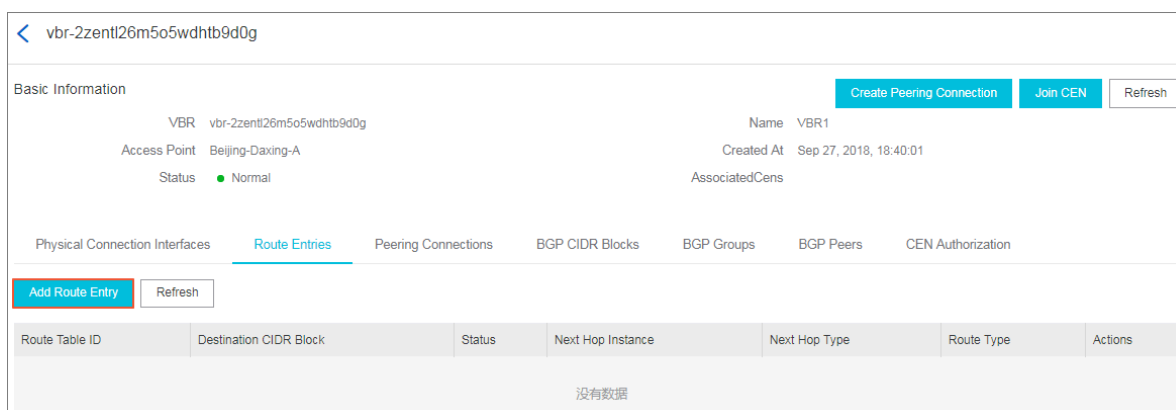
In the VBR, you must add one route entry directed to the physical connection and another route entry directed to the VPC to forward the traffic of the VPC and the local IDC, respectively. VBR allows you to configure BGP routing for the local IDC. For more information, see [Configure BGP](#).

When you manage the route entries of VBR, pay attention to the following restrictions:

- Each route table supports 48 custom route entries.
- Source address policy routing is not supported.

Procedure

1. Log on to the [Express Connect](#) console.
2. In the left-side navigation pane, click Physical Connections > Virtual Border Routers (VBRs).
3. Select the region of the VBR and then click the VBR ID.
4. Click the Route Entries tab and then click Add Route Entry.



5. Configure the route entry and then click OK.

Configuration	Description
Destination Subnet	Enter the destination subnet.

Configuration	Description
Next Hop Type	Select the type of the next hop: <ul style="list-style-type: none">· VPC: Forwards data to the selected VPC.· Physical Connection Interface: Forwards data to the selected physical connection interface.
Next Hop	Select the next hop instance that receives the data, based on the next hop type.

3.4 Establish peering connections

VBR is a data forwarding bridge connecting the VPC and your local IDC. After you create a VBR, you need to establish a peering connection between the VBR and the VPC.

For more information, see [Interconnect two VPCs](#).

4 Configure health checks

To ensure that traffic is distributed to the other physical connection when one physical connection fails, you must configure health checks for the VBRs.

Prerequisites

Make sure that you have established redundant physical connections and added ECMP routes directing to the on-premises IDC in the VPC.

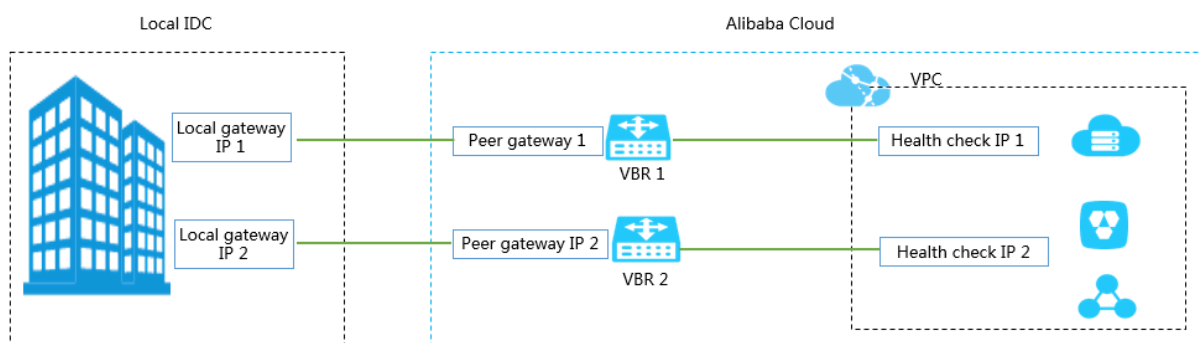
Context

Alibaba Cloud sends a ping packet to the customer-side IP address of the on-premises IDC from each health check IP address every two seconds. If eight successive ping packets on one leased line fail to give response, the traffic is distributed to the other leased line.




Note:

If Control Plane Policing (Copp) (such as Cisco devices) or Local Attack Defense Policy (Huawei devices) is configured on the on-premises IDC, health check packets may be discarded and then the health check link shocks. We recommend that you cancel the control side speed limitation on the network device of the on-premises IDC.



Procedure

1. Log on to the [Express Connect](#) console.
2. In the left-side navigation pane, click VPC Peering Connections > VBR-to-VPC.
3. Locate the target peering connection and click  > Health Check.

4. Click Configure and then configure the health check based on the following information.

Configuration	Description
Source IP	Any idle private IP address in the VPC.
Destination IP	The interface IP address of the network device of the on-premises IDC. If you need to perform an ICMP health check from your on-premises IDC to the VPC to check the connection is normal, we recommend that you set the Destination IP as the source IP address used for health checks of the VPC, and configure a route that points to this address.

5 Manage quotas

You can query the number of remaining resources in your quota through the Express Connect console. If the remaining quota number is insufficient for your requirements, you can open a ticket to apply for an increase to your quota.

操作步骤

1. Log on to the [Express Connect](#) console.
2. In the left-side navigation pane, click Quota Management.
3. View the resource usage of the Express Connect service under your account.
4. To increase your resource quota, click Apply in the Actions column. Then, enter the following information:
 - **Quantity for Application:** the number of resources you require. You must enter a number that is greater than the current quota. For more information about the resource limits of Express Connect, see [Limits](#).
 - **Reason for Application:** your reason for applying for an increase to your quota. We recommend that you include details about your specific scenario.
 - **Mobile/Landline Phone Number:** the mobile or landline phone number of the person to contact.
 - **Email:** the email address of the person to contact.
5. Click OK.

The system then determines whether the quota application is reasonable. If the system determines the request is unreasonable, the application enters the Rejected state. If the request is reasonable, the application enters the Approved state and the quota is automatically upgraded to the specified quota number.

To view a history of quota applications, click Application History in the Application History column.