Alibaba Cloud
Express Connect

User Guide (New Console)

Issue: 20181121

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 disseminat ed 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, adjustment s, 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 intellectu al 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 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	Select whether the VPCs you want to connect belong to the same account.

Configuration	Description
	• **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	Select the peering connection type: • **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*. In this example, select **VPC-to-VPC**.
Routers to Create	Select the instances to be created: • **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.
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.

Configuration	Description
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.
Specification	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.

1.3 Interconnect a VPC and a VBR

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

Prerequisites

Procedure

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

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

3. Click **Create Peering Connection**.

4. Configure peering connections.

Configuration item	Description
Belong to Same Account	Select whether the VPC and VBR you want to connect belong to the same account or different accounts. • **Yes**: 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. • **No**: 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 a peering connection type: • **VPC-to-VPC**: Establish a peering connection between two VPCs. • **VBR-to-VPC**: Establish a peering connection between a VPC and a VBR.

Configuration item	Description
	In this example, select **VBR-to-VPC**.
Routers to Create	Select the type of the instance to be created: • **Initiator and Acceptor Routers**: Both the initiator instance and the acceptor instance are created. After creation, the initiator instance automatically connects to the acceptor instance. This option applies only to connections with the same account. • **Initiator Router 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 connections between different accounts . • **Acceptor Router Only**: The acceptor instance is created. Only VPC is available for the acceptor router type. This option applies only to connections between different accounts .
Region	Select the region of the VBR.
Access Point	Select the access point to which the VBR connects.
Initiator VBR ID	Select the VBR to which you want to establish the connection.
Acceptor Region	Select the region of the VPC.
Acceptor VPC ID	Select the ID of the VPC.
Bandwidth	Select a bandwidth for the connection. Use the default bandwidth for the acceptor instance.
Validity	Select the subscription duration. If you want automatic renewal after expiration, check 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.

- **Temporarily Upgrade**: Temporarily increase the bandwidth of the initiator instance.

  The upgrade interval is two hours. The price is charged by the hour. It will take effect immediately after the payment. Services will not be interrupted during the upgrade.

  When the upgrade duration ends, the initiator instance automatically returns to the original bandwidth. Your service will not be interrupted when the initiator instance returns to the original bandwidth, but intermittent disconnection may occur. We recommend that your applications have re-connection functionalities.

1.5 Manage Pay-As-You-Go instances

You can delete your Pay-As-You-Go instances, change their bandwidths, or change their billing method to Subscription.

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:

- **Initiate Connection**: When creating a peering connection between two different accounts, you must initiate the connection from the initiator after adding the peer instance. The connection can be initiated only from the initiator instance.

- **Upgrade/Downgrade**: Change the bandwidth of the initiator instance.

- **Switch to Subscription**: Change the billing method of the initiator to Subscription.

- **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.

- **Delete**: Delete the unconnected or suspended instance.

1.6 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**.
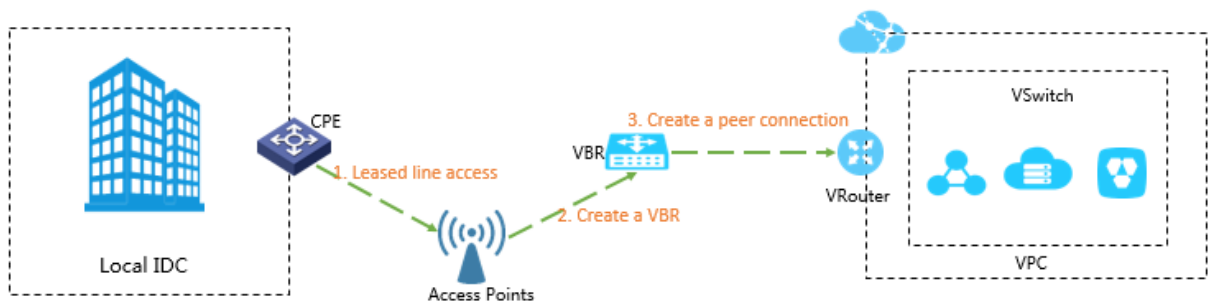
2 Physical connection

2.1 Leased line access process

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

Connection process

As shown in the following figure, after connecting your local 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. Finally, you will need to establish a peering connection between the VBR and VPC, and build a private network connection between your local IDC and Alibaba Cloud.

To establish a physical connection, you must first connect the leased line to an access point. You can apply for the connection in the Alibaba Cloud console or through one-stop access service.

Self-service application

The process for self-service access application is shown in the following figure.
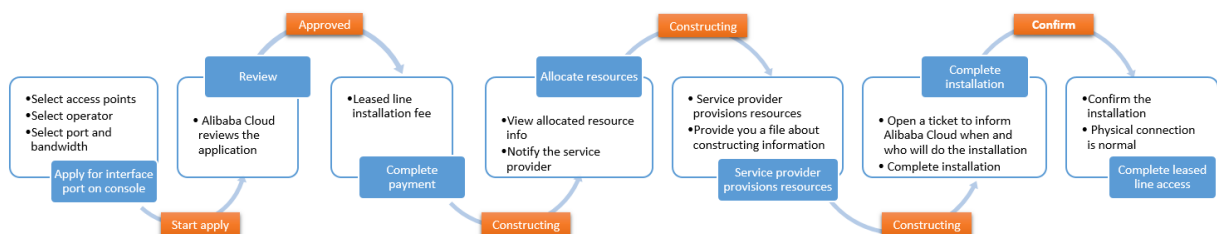
One-stop access

The one-stop access service is provided by the service provider. You only need to provide the information about the leased line access in the Alibaba Cloud console. The service provider will complete interface application, construction, and leased line access for you.

2.2 Apply for leased line access through self-service

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 access, pay attention to the following restrictions:

- Physical connections do not support interfaces of SDH 155M CPOS, V.35 or G.703.

- Alibaba Cloud provides one or more access points in each accessible region. Different access points have different service provider restrictions. Before applying for leased line access, you must submit a ticket to obtain an access point and the restriction information of your service provider.

Procedure

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. Set the parameters, and then click **OK**.

Configuration	Description
Name	Enter a name for the leased line.
Access Point	Select the nearest access point to your local 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 submit a ticket to obtain access point information and select the optimal access point.
Service Provider	Select the service provider of the leased line.
Port Type	Select the access port type.
Bandwidth	Enter the access bandwidth.
Location	Enter the location of your local IDC.
Redundancy	Select a requested 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.

Configuration	Description
	• 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. 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.

7. 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. The physical connection interface status becomes **Connecting**.

8. Click **View** to view the details, such as IDC location, network location, and port information.

9. 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.

10. Submit a ticket to inform Alibaba Cloud after-sales personnel of the information about the leased line deployed by the service provider.
   On the next workday, Alibaba Cloud after-sales personnel will schedule an access to the IDC for your service provider and give you the contact information of the reception personnel in the IDC.

11. Inform your service provider of the construction time and the reception personnel.

12. Wait for the service provider to complete the construction.

   After the service provider completes the construction in the Alibaba Cloud IDC, the physical connection interface status becomes **Pending Confirmation**.

13. After your service provider notifies you that the physical connection is deployed, find the physical connection in the console and click **Confirm**.

After confirmation, the physical connection interface status changes to **Enabled**, indicating that the leased line access is completed.

Physical Connection Interfaces						
Apply for New Interface One-Stop Service Refresh					Instance ID ∨ Enter	
Instance ID/Name	Access Point	Service Provider	Port Type	Bandwidth	Status	Actions
pc-2zeoaxkq3jot5p71qcnuy TEST	Beijing-Daxing-A	China Telecom	100 Mbit/s Electrical Port	5Mbps	● Enabled	Edit Terminate Connection

2.3 Establish a leased-line connection through one-stop access service

You need to connect the leased line of your service provider to an Alibaba Cloud access point before you can establish a physical connection. You can quickly establish a leased-line connection through one-stop access service.

Context

> 📋 **Note:**
>
> Physical connections do not support interfaces of SDH 155M CPOS, V.35 or G.703.

Procedure

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

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

3. Click **One-Stop Service**.

4. Set the parameters.

Configuration	Description
Bandwidth	Select a bandwidth for the leased-line access.
Access City	Select the city where your local IDC is located.
Access Address	Enter the address of your local IDC.
Interface Type	Select the access port type.
Service Provider	Select the service provider of the leased line.
Alibaba Cloud Region	Select the Alibaba Cloud region that you want to access.
Multi-Line Access	Select whether to apply for multiple leased lines as Equal-Cost Multi-Path routing (ECMP) redundancy links.

Configuration	Description
Leased Line Type	Select a leased line type: • **Layer2 Leased Line (MSTP)**: traditional physical connection access. • **Layer3 Leased Line (MPLS-VPN)**: MPLS-VPN access.
Contact Name	Enter the name of the contact responsible for the leased-line access.
Mobile Phone No.	Enter the mobile phone number of the contact responsible for the leased-line access.
E-mail	Enter the E-mail box of the contact responsible for the leased-line access.

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

    The physical connection interface status is **Applying**.

6. After the service provider notifies you that the leased line is deployed, find the leased line on the console and click **Confirm**.

    After confirmation, the physical connection interface status changes to **Enabled**, indicating that the leased-line access is completed.

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.
VLAN ID	Enter the VLAN ID of the VBR, ranging from 0 to 2999. • 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.

Configuration	Description
	• 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. 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.
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 transmissi on 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 **Add BGP CIDR Block**.
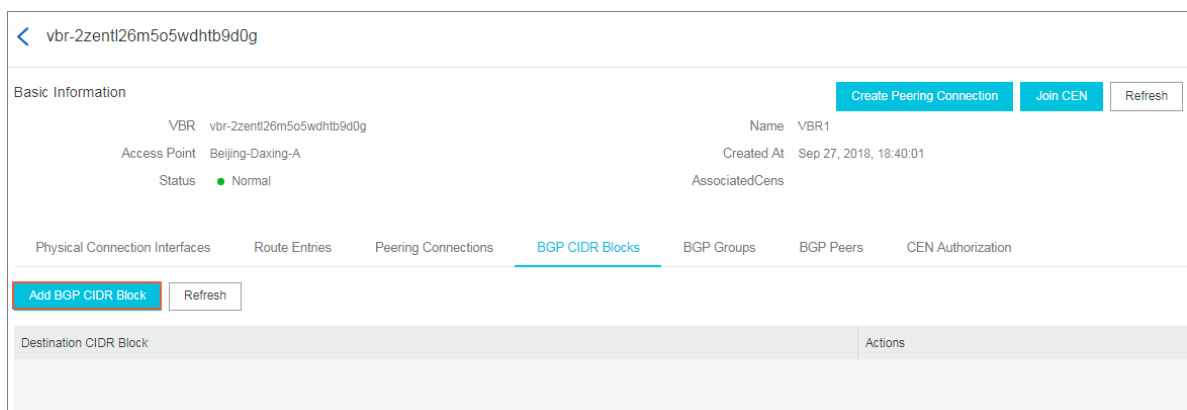
5. Enter the CIDR block to be added, and then click **OK**.

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**.

<	vbr-2zentl26m5o5wdhtb9d0g					
Basic Information				Create Peering Connection	Join CEN	Refresh
	VBR vbr-2zentl26m5o5wdhtb9d0g			Name VBR1		
	Access Point Beijing-Daxing-A			Created At Sep 27, 2018, 18:40:01		
	Status ● Normal			AssociatedCens		

Physical Connection Interfaces	Route Entries	Peering Connections	BGP CIDR Blocks	BGP Groups	BGP Peers	CEN Authorization

Add Route Entry Refresh						
Route Table ID	Destination CIDR Block	Status	Next Hop Instance	Next Hop Type	Route Type	Actions
			没有数据			

5. Configure the route entry and then click **OK**.

Configuration	Description
Destination Subnet	Enter the destination subnet.
Next Hop Type	Select the type of the next hop: • **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 NSP partners

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

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

> **Note:**
>
> You must sign contracts and obtain services from third-party network service providers when using NSP partners to access Alibaba Cloud. Additionally, the SLA protection and any issues outside Alibaba Cloud are the responsibility of NSP partners.

Partners	Hong Kong -A	Hong Kong -B	Tokyo -A	Tokyo -B	Singa -A	Singa -B	Sydne -A	Sydne -B	Frank -A	Frank -B	San Jose -A	Ashb -A	Dubai -A
China Telecom Global	✓	—	—	—	—	—	—	—	—	✓	—	—	—
China Unicom Global	—	✓	—	—	—	—	—	—	—	—	—	—	—
Epsilon	—	—	—	—	✓	✓	—	—	—	—	—	✓	✓
euNetworks	—	—	—	—	—	—	—	—	✓	—	—	—	—
GTT	—	—	—	—	✓	—	—	—	—	—	—	—	—
TATA	—	✓	—	—	✓	—	—	—	—	—	—	—	—
Megaport	✓	✓	—	—	✓	✓	✓	✓	—	—	✓	✓	—
PCCW	✓	✓	—	—	✓	✓	—	—	—	—	—	—	—
Reliance	—	—	—	—	✓	—	—	—	—	—	—	—	—
SingTel	—	—	—	—	✓	✓	—	—	—	—	—	—	—
Vodafone	—	—	—	—	—	—	—	—	✓	—	—	—	—

Partners	Hong Kong -A	Hong Kong -B	Tokyo -A	Tokyo -B	Singa -A	Singa -B	Sydn -A	Sydn -B	Frank -A	Frank -B	San Jose -A	Ashb -A	Dubai -A
Zenlayer	✓	—	✓	✓	✓	—	—	—	—	✓	✓	✓	—
SoftBank	—	—	✓	✓	—	—	—	—	—	—	—	—	—
Intercloud	—	—	—	—	—	—	—	—	—	✓	—	—	—
Equinix	✓	—	—	—	✓	—	—	✓	—	✓	✓	✓	—
HGC	✓	✓	—	—	—	—	—	—	—	—	—	—	—
NextDC	—	—	—	—	—	—	✓	✓	—	—	—	—	—

5 Access points of international regions

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

The available access points for international regions are listed in the following table.

Area	Country (City)	Access point	Location
Asia Pacific	Hong Kong	Hong Kong-Kwai Chung-A	Equinix
		Hong Kong-Chai Wan-B	MEGA
	Singapore	Singapore-A	Equinix
		Singapore-B	Global Swich
	Australia (Sydney)	Australia-Sydney-A	Global Swich
		Australia-Sydney-B	Equinix
	Malaysia (Kuala Lumpur)	Malaysia-Kuala Lumpur-A	NTT
		Malaysia-Kuala Lumpur-B	AIMS
	Indonesia (Jakarta)	Indonesia-Jakarta-A	DCI
	Japan (Tokyo)	Japan-Tokyo-A	Equinix
		Japan-Tokyo-B	Equinix
Europe and America	USA (Silicon Valley)	USA-San Jose-A	Equinix
	US (Virginia)	United States-Ashburn-A	Equinix
		United States-Virginia-C	Cyrusone
		United States-Virginia-D	Coresite
	Germany (Frankfurt)	Germany-Frankfurt-A	Vodafone
		Germany-Frankfurt-B	Equinix
	UK (London)	UK-London-A	DRT

Area	Country (City)	Access point	Location
		United Kingdom-London-B	ARK
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	NTT