ALIBABA CLOUD

Alibaba Cloud

Apsara Stack Enterprise

Express Connect

User Guide

Product Version: v3.16.2

Document Version: 20220915

Alibaba Cloud

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 because of product version upgrade, adjustment, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and an updated version of this document will be released through Alibaba Cloud-authorized channels from time to time. You should 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 this document based on the "status quo", "being defective", and "existing functions" of its products and services. 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 take legal responsibility for any errors or lost profits incurred by any organization, company, or individual arising from download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, take responsibility for any indirect, consequential, punitive, contingent, 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 contents in Alibaba Cloud documents, including but not limited to pictures, architecture design, page layout, and text description, 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 this document 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 directly contact Alibaba Cloud for any errors of this document.

Document conventions

Style	Description	Example
Danger	A danger notice 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.
Warning	A warning notice 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 restart an instance.
Notice	A caution notice indicates warning information, supplementary instructions, and other content that the user must understand.	Notice: If the weight is set to 0, the server no longer receives new requests.
Note	A note indicates supplemental instructions, best practices, tips, and other content.	Note: You can use Ctrl + A to select all files.
>	Closing angle brackets are used to indicate a multi-level menu cascade.	Click **Settings**> **Network**> **Set network type**.
Bold	Bold formatting is used for buttons , menus, page names, and other UI elements.	Click **OK**.
`Courier font`	Courier font is used for commands	Run the `cd /d C:/window` command to enter the Windows system folder.
Italic	Italic formatting is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	This format is used for an optional value, where only one item can be selected.	`ipconfig [-all|-t]`
{} or {a|b}	This format is used for a required value, where only one item can be selected.	`switch {active|stand}`

Table of Contents

1.What is Express Connect?

This topic provides an overview of Express Connect. Express Connect allows you to establish private connections to enable fast, stable, and secure communication between different networking environments. You can use Express Connect to ensure network stability and prevent data breaches.

Features

You can use a leased line provided by an Internet Service Provider (ISP) to establish a physical connection between your data center and an Alibaba Cloud access point. After the physical connection is established, you can create a virtual border router (VBR) to connect your data center with Alibaba Cloud to build a hybrid cloud.

The physical connections of Express Connect do not traverse the Internet, and therefore feature faster speeds, lower latency, greater security, and higher reliability compared with Internet connections.

Express Connect enables you to create a peering connection between two Virtual Private Clouds (VPCs) as a channel for private communication.

Benefits

Express Connect provides the following benefits:

- High-speed interconnections

  Powered by the network virtualization technology of Alibaba Cloud, Express Connect allows networks to connect and exchange traffic at high speeds within internal networks without carrying traffic across the Internet. The impact of distance on network performance is minimized to ensure low-latency and high-bandwidth communication.

- Stability and reliability

  Built on the state-of-the-art infrastructure of Alibaba Cloud, Express Connect guarantees stable and reliable communication between networks.

- Security

  Express Connect implements cross-network communication at the network virtualization layer, where data is transmitted over separate and private channels within the infrastructure of Alibaba Cloud, mitigating the risks of data breaches.

- Buy-as-you-need service

  Express Connect delivers connectivity with a wide range of bandwidth options. You can choose based on the needs of your business to get the best value for your purchase.

2.Log on to the Express Connect console

This topic describes how to log on to the Apsara Uni-manager Management Console to manage your Express Connect services. The Google Chrome browser is used as an example.

Prerequisites

- Before you log on to the Apsara Uni-manager Management Console, you must obtain the URL of the console from the engineer that deploys the service.
- We recommend that you use the Google Chrome browser.

Procedure

1. In the address bar of the browser, enter the URL of the Apsara Uni-manager Management Console and press the Enter key.
2. Enter your username and password.

   Obtain the username and password that are used to log on to the console from the operations administrator.

   > **Note** If this is the first time you log on to the Apsara Uni-manager Management Console, you must change your password as prompted. For higher security, the password must meet the minimum complexity requirements. The password must be 8 to 20 characters in length and must contain at least two of the following character types:
   >
   > - Uppercase or lowercase letters.
   > - Digits.
   > - Special characters such as exclamation points (!), at signs (@), number signs (#), dollar signs ($), and percent signs (%).

3. Click **Log On**.
4. In the top navigation bar, choose **Products > Networking > Express Connect**.

3.VPC peering connections

3.1. Peering connections

You can create a peering connection between two virtual private clouds (VPCs) or between a VPC and a virtual border router (VBR).

Initiator and acceptor

One end of a peering connection functions as the initiator and the other end functions as the acceptor. Only the initiator can initiate the peering connection. The acceptor must wait for the initiator to initiate the peering connection. The concepts of initiator and acceptor are used only to control how a peering connection is established. Data transmission between the initiator and acceptor is bidirectional. Therefore, after a peering connection is established, both the initiator and acceptor can send and receive data.

If you create a peering connection for two VPCs within the same account, the system of Express Connect automatically creates the initiator and acceptor. You do not need to manually initiate the connection. The system automatically sends the connection request and enables the connection. If you create a peering connection for two VPCs that belong to different accounts, you must manually initiate the connection.

The following table describes the differences between an initiator and acceptor.

Item	Initiator	Acceptor
Whether the configuration of the peer is required before the connection is initiated	Yes	Yes
Initiate the connection	Supported	Not supported
Send messages to the peer after the connection is established	Supported	Supported

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

Connection process	Initiator status	Acceptor status
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

3.2. Connect two VPCs

This topic describes how to create a peering connection between two virtual private clouds (VPCs).

Procedure

1. Log on to the Express Connect console
2. In the left-side navigation pane, click **VPC-to-VPC**.
3. On the **VPC-to-VPC** page, click **Create Peering Connection**.
4. On the page that appears, set the following parameters and click **Submit**.

Parameter	Description
Scenario	
Connection Type	Select **VPC-to-VPC** to create a peering connection between two VPCs.
Local Configurations	
Organization	Select the organization to which the initiator VPC belongs.
Resource set	Select the resource group to which the initiator VPC belongs.
Region	Select the region where the initiator VPC is deployed.
Router type	Use the default value **vRouter** for this parameter.
Local VPC ID	Select the ID of the initiator VPC.
Peer Configurations	
Organization	Select the organization to which the acceptor VPC belongs.
Resource set	Select the resource group to which the acceptor VPC belongs.
Peer Region	Select the region where the acceptor VPC is deployed.
Peer Router Type	Use the default value **vRouter** for this parameter.
Peer VPC ID	Select the ID of the acceptor VPC.

Parameter	Description
Basic Information	
Bandwidth	Specify the maximum bandwidth.

What's next

After you create a peering connection, you can specify names for the initiator and acceptor.

1. On the **VPC-to-VPC** page, find the initiator or acceptor that you want to manage and click the icon below the ID.
2. In the **Rename** dialog box, enter a name and click **OK**.

3.3. Connect a VBR to a VPC

This topic describes how to create a peering connection between a virtual border router (VBR) and a virtual private cloud (VPC).

Procedure

1. Log on to the Express Connect console
2. In the left-side navigation pane, click **VBR-to-VPC**.
3. On the **VBR-to-VPC** page, click **Create Peering Connection**.
4. On the page that appears, set the following parameters and click **Submit**.

Parameter	Description
Scenario	
Connection Type	Use the default value **VBR-to-VPC** for this parameter.
Common Settings	
Organization	Select the organization to which the VBR belongs.
Resource set	Select the resource group to which the VBR belongs.
VBR-side Configurations	
Router type	Use the default value **VBR** for this parameter.
Region	Select the region where the VBR is deployed.
Access Point	Select an access point.
VBR ID	Select the ID of the VBR.
Router Interface Specifications	Select the interface specification of the router. In this example, 1,000 Mbit/s is selected.

Parameter	Description
Router Interface Name	Enter a name for the VBR interface.
Description	Enter a description.
VPC-side Configurations	
Router type	Use the default value **vRouter** for this parameter.
Region	Select the region where the VPC is deployed.
Availability Zone	Select a zone in the region to which the VPC belongs.
VPC ID	Select the ID of the VPC.
Router Interface Name	Enter a name for the VPC router interface.
Health Check Source IP Address	Enter the source IP address for health checks. **Note** The source IP address for health checks must be an idle IP address that belongs to the CIDR block of a vSwitch in the specified VPC.
Health Check Destination IP Address	Enter the destination IP address for health checks. **Note** The destination IP address must be the IP address of the customer-premises device that is connected to the VBR by using the Express Connect circuit.
Description	Enter a description.

3.4. Delete a peering connection

This topic describes how to delete a peering connection.

Procedure

1. Log on to the Express Connect console.
2. In the left-side navigation pane, choose **VPC Peering Connections > VPC-to-VPC**.
3. Find the target peering connection and choose > **Suspend Initiator** in the **Actions** column.
4. Find the target peering connection and choose > **Suspend Acceptor** in the **Actions** column.
5. Find the target peering connection and choose > **Delete** in the **Actions** column.

6. In the **Delete Peering Connection** dialog box, click **Confirm**.

4.Physical connections

4.1. Connections over Express Connect circuits

Express Connect enables fast and secure data transmission between data centers and Apsara Stack. You can lease an Express Connect circuit from a connectivity provider and use the Express Connect circuit to connect a data center to an Apsara Stack access point. Connections over Express Connect circuits are not exposed to the Internet. Compared with Internet connections, connections over Express Connect circuits are safer, faster, and more reliable with lower network latency.

Connection methods

You can apply for an Express Connect circuit to establish a connection.

You can lease an Express Connect circuit to connect your data center to an access point of Apsara Stack. The Express Connect circuit is dedicated to you. To perform this operation, log on to the Express Connect console. For more information, see Create a physical connection.

4.2. Create a connection over an Express Connect circuit

Before you create a connection over an Express Connect circuit, you must confirm the location of the access point, apply for an Express Connect circuit in the Express Connect console, and then create a virtual border router (VBR).

Step 1: Confirm the access point

An access point is where network services are provided and supports multiple types of connections between a data center and Apsara Stack. When you select an access point, take note of the elements such as the region, colocation provider, and port type. When you select an access point, you must confirm the Apsara Stack region that you want to access.

Step 2: Apply for an Express Connect circuit

1. Log on to the Express Connect console.
2. In the left-side navigation pane, click **Exclusive Physical Connection**.
3. On the **Express Connect Circuit** page, click **Apply for Express Connect Circuit**.
4. On the Create Physical Connection page, set the following parameters and click **Submit**.

Parameter	Description
Area	
Organization	Select the organization to which the connection over the Express Connect circuit belongs.

Parameter	Description
Resource set	Select the resource group to which the connection over the Express Connect circuit belongs.
Region	Select the region where you want to create a connection over the Express Connect circuit.
Basic Information	
Physical Connection Name	Enter a name for the connection over the Express Connect circuit.
Description	Enter a description for the connection over the Express Connect circuit.
Peer Address	Enter the address of the data center that you want to connect by using the Express Connect circuit.
Physical Connection Configurations	
Access Point	Select an access point to connect to the data center. Access points are Apsara Stack data centers located in different regions. Each region provides one or more access points. The access points allow you to connect to Apsara Stack from different geographical locations and support different connection types.
Port Type	Select a port type. Valid values: ○ **100 M Copper Ethernet Port** ○ **1 GE copper Electrical Port** ○ **1 GE copper Single-mode Optical Port** ○ **10 GE copper Electrical Port** ○ **10 GE copper Single-mode Optical Port**
Access Device	Select the device to connect the Express Connect circuit.
Physical Port	Enter a name for the port on the access device.
Physical Connection Bandwidth	Enter a maximum bandwidth value for the connection over the Express Connect circuit. Minimum value: 2. Unit: Mbit/s. You cannot enter a value higher than the limit specified by the port type.

5. Return to the **Express Connect Circuit** page. You can view that the connection is in the **Allocating** state.

Step 3: Enable the connection over the Express Connect circuit

1. After resources are allocated, the connection changes to the Pending state. Click **Enable Connection** in the **Actions** column.

2. Refresh the **Express Connect Circuit** page. The state of the connection changes to **Enabled**.

Step 4: Create a VBR

After the connection is enabled, you must create a VBR to route network traffic between the data center and Apsara Stack.

1. Log on to the Express Connect console.
2. In the left-side navigation pane, click **Virtual Border Router**.
3. On the **VBRs** page, click **Create VBR**.
4. In the **Create VBR** dialog box, set the following parameters and click **OK**.

Parameter	Description
Basic Information	
Account Type	○ **Current Organization**: creates a VBR for the current organization. ○ **Another Organization**: creates a VBR for another organization. In this example, **Current Organization** is selected.
Resource Set	Select a resource set for the VBR. You must set this parameter if **Account Type** is set to **Current Organization**.
Name	Enter a name for the VBR. You must set this parameter if **Account Type** is set to **Current Organization**.
Organization UID	You must set this parameter if the account type is set to **Another Organization**. In this case, enter the ID of the Apsara Stack account for which you want to create the VBR.
Express Connect Circuit Configurations	
Express Connect Circuit	Select an Express Connect circuit that is enabled and works as expected.

Parameter	Description
VLAN ID	Enter a VLAN ID for the VBR. Valid values: 0 to 2999. ◦ If the VLAN ID is set to 0, the switch port on the VBR is a Layer 3 router interface instead of a VLAN interface. When a Layer 3 router interface is used, each Express Connect circuit corresponds to one VBR. ◦ If the VLAN ID is set to a value from 1 to 2999, the switch port on the VBR is a Layer 3 VLAN subinterface. When a Layer 3 VLAN subinterface is used, each VLAN ID corresponds to one VBR. In this case, the Express Connect circuit with which the VBR is associated can be used to connect to VPCs that belong to different Apsara Stack accounts. VBRs in different VLANs are isolated from each other at Layer 2. **Notice** The VLAN ID that you specify for the VBR and that of the customer-premises device must be the same.
IPv4 Address of Gateway at Alibaba Cloud Side	Enter an IPv4 address for the gateway that is deployed on Apsara Stack. In this example, `192.168.101.5` is used.
IPv4 Address of Gateway at Customer Side	Enter an IPv4 address for the gateway that is deployed in the data center. In this example, `192.168.101.6` is used.
Subnet Mask (IPv4 Address)	Enter the subnet mask of the specified IPv4 addresses. In this example, `255.255.255.252` is used. You can enter a long subnet mask because only two IP addresses are required.
IPv6 Support	Specify whether to enable IPv6. ◦ **Disable**: disables IPv6. ◦ **Enable**: enables IPv6. The VPC can communicate with the data center over IPv6.
IPv6 Address of Gateway at Alibaba Cloud Side	Enter an IPv6 address for the gateway that is deployed on Apsara Stack. Example: `2001:XXXX:3c4d:0015:0000:0000:0000:1a2b`.
IPv6 Address of Gateway at Customer Side	Enter an IPv6 address for the gateway that is deployed in the data center. Example: `2001:XXXX:3c4d:0015:0000:0000:0000:2a2b`.
Subnet Mask (IPv6 Address)	Enter the subnet mask of the specified IPv6 addresses. Example: `2408:4004:cc:400::/56`. The two IPv6 addresses must fall within the same subnet.

5. If the VBR is in the **Active** state, **ping** the IP addresses to check the network connectivity between the gateway in the data center and the gateway on Apsara Stack.

Step 5: Create a peering connection between the VBR and the VPC

After you complete the preceding steps, you must create a peering connection between the VBR and the VPC that you want to connect. This way, the VPC and the data center can communicate with each other over a private connection.

1. Log on to the Express Connect console.
2. In the left-side navigation pane, click **VBR-to-VPC**.
3. On the **VBR-to-VPC** page, click **Create Peering Connection**.
4. On the page that appears, set the following parameters and click **Submit**.

Parameter	Description
Scenario	
Connection Type	Use the default value **VBR-to-VPC** for this parameter.
Common Settings	
Organization	Select the organization to which the VBR belongs.
Resource set	Select the resource group to which the VBR belongs.
VBR-side Configurations	
Router type	Use the default value **VBR** for this parameter.
Region	Select the region where the VBR is deployed.
Access Point	Select an access point.
VBR ID	Select the ID of the VBR.
Router Interface Specifications	Select the interface specification of the router. In this example, 1,000 Mbit/s is selected.
Router Interface Name	Enter a name for the VBR interface.
Description	Enter a description.
VPC-side Configurations	
Router type	Use the default value **vRouter** for this parameter.
Region	Select the region where the VPC is deployed.
Availability Zone	Select a zone in the region to which the VPC belongs.
VPC ID	Select the ID of the VPC.
Router Interface Name	Enter a name for the VPC router interface.

Parameter	Description
Health Check Source IP Address	Enter the source IP address for health checks. **Note** The source IP address for health checks must be an idle IP address that belongs to the CIDR block of a vSwitch in the specified VPC.
Health Check Destination IP Address	Enter the destination IP address for health checks. **Note** The destination IP address must be the IP address of the customer-premises device that is connected to the VBR by using the Express Connect circuit.
Description	Enter a description.

4.3. Delete a connection over an Express Connect circuit

This topic describes how to delete a connection over an Express Connect circuit.

Context

To delete a connection over an Express Connect circuit, perform the following operations:

1. Delete the routes on the router of the virtual private cloud (VPC) and routes on the virtual border router (VBR).
2. If Border Gateway Protocol (BGP) routing is configured, delete the BGP peers and BGP groups.
3. Delete the peering connections.
4. Delete the associated VBRs.
5. Delete the connection over the Express Connect circuit.

Step 1: Delete routes

Delete routes of the VPC and the VBR.

1. To delete custom routes in a route table of a VPC, perform the following operations:
   i. Log on to the VPC console. For more information, see the **Log on to the VPC console** topic in the *VPC user guide*.
   ii. In the left-side navigation pane, click **Route tables**.
   iii. In the top navigation bar, select the region to which the route table belongs.
   iv. On the **Route Tables** page, find the route table and click **Manage** in the **Actions** column.
   v. On the **Route Entry List** tab, find the custom route that you want to delete and click **Delete** in the **Actions** column.
   vi. In the **Delete Route Entry** message, click **OK**.
2. To delete routes on a VBR, perform the following operations:

i. Log on to the Express Connect console.
ii. In the left-side navigation pane, click **Virtual Border Router**.
iii. On the **VBRs** page, select the region where the VBR that you want to manage is deployed and click its ID.
iv. On the **Routes** tab, find the route that you want to delete and click **Delete** in the **Actions** column.
v. In the **Delete Route Entry** message, click **OK**.

Step 2: Delete BGP peers and BGP groups

If BGP is configured, you must perform the following operations to delete the BGP settings:

1. Log on to the Express Connect console.
2. In the left-side navigation pane, click **Virtual Border Router**.
3. On the **VBRs** page, select the region where the VBR that you want to manage is deployed and click its ID.
4. On the **BGP Peers** tab, delete the BGP peers.
5. On the **BGP Groups** tab, delete the BGP groups.
6. On the **Advertised BGP Subnets** tab, delete the BGP CIDR blocks.

Step 3: Delete the peering connections

To delete the peering connection between a VPC and a VBR, perform the following operations:

1. Log on to the Express Connect console.
2. In the left-side navigation pane, click **VBR-to-VPC**.
3. Find the VBR-to-VPC connection that you want to delete and click **Delete** in the **Actions** column.
4. In the **Delete** message, click **Delete**.

Step 4: Delete the associated VBRs

1. Log on to the Express Connect console.
2. In the left-side navigation pane, click **Virtual Border Router**.
3. On the **VBRs** page, find the VBR that you want to delete and click **Delete** in the **Actions** column.
4. In the **Delete VBR** message, click **OK**.

Step 5: Delete the connection over the Express Connect circuit

1. Log on to the Express Connect console.
2. In the left-side navigation pane, click **Exclusive Physical Connection**.
3. On the **Exclusive Physical Connection** page, find the connection that you want to disable and click **Terminate Connection** in the **Actions** column.
4. In the **Terminate Connection** message, click **OK**.
5. On the **Express Connect Circuit** page, find the connection that you want to delete and click **Delete** in the **Actions** column.
6. In the **Delete Physical Connection** message, click **OK**.

5.VBRs

5.1. VBRs

Virtual border routers (VBRs) are an abstraction of Express Connect circuits that are isolated and virtualized by using the Layer 3 overlay and vSwitch technologies in the Software Defined Network (SDN) architecture. A VBR is deployed between the customer-premises equipment (CPE) and a virtual private cloud (VPC) and is used to exchange data between the VPC and data center.

> **Note** Similar to VPC routers, each VBR manages a route table. You can add routes to the route table of a VBR to control network traffic forwarding.

Features

A VBR provides the following features:

- Exchanges data between a VPC and a data center.
- Determines the type of virtual interface of an Express Connect circuit: Layer 3 router interface or Layer 3 Virtual Local Area Network (VLAN) subinterface.
- Adds or identifies VLAN tags if a Layer 3 VLAN subinterface is used.
- Supports Border Gateway Protocol (BGP) routing.
  - BGP is a dynamic routing protocol based on Transmission Control Protocol (TCP). BGP is used to exchange routing and network accessibility information across autonomous systems. When you create a connection over an Express Connect circuit, you can configure BGP routing between your data center and the associated VBR. This way, the data center and the VBR can communicate with each other through a private connection. This helps you to set up a hybrid cloud with higher efficiency, flexibility, and security.
  - VBRs support BGP dynamic routing in both IPv4 and IPv6 networks.

Limits

- VBRs do not support source address-specific policy-based routes.
- Each VBR has one and only one route table.
- VBRs support only BGP-4.
- You can create at most eight BGP peers for each VBR.
- Each BGP peer supports at most 110 dynamic routes. Routes are denied when the upper limit is exceeded.
- To configure BGP when you connect to a VPC, you must specify an Autonomous System Number (ASN) for the VPC. The ASN that you specify must be different from the ASNs of the vSwitches in the VPC.

5.2. Create a VBR

After an Express Connect circuit is enabled, you must create a virtual border router (VBR) for the Express Connect circuit. The VBR is used to route traffic between the virtual private cloud (VPC) and the data center that are connected through the Express Connect circuit.

Context

A VBR is a router deployed between a VPC and the customer-premises equipment (CPE) in a data center. Each VBR is associated with a route table. To manage traffic forwarding on a VBR, you can add routes to the route table that is associated with the VBR.

A VBR provides the following features:

- Exchanges data between a VPC and a data center.
- Determines the type of virtual interface of an Express Connect circuit: Layer 3 router interface or Layer 3 Virtual Local Area Network (VLAN) subinterface.
- Adds or identifies VLAN tags if a Layer 3 VLAN subinterface is used.
- Supports Border Gateway Protocol (BGP) routing.
  - BGP is a dynamic routing protocol based on Transmission Control Protocol (TCP). BGP is used to exchange routing and network accessibility information across autonomous systems. When you create a connection over an Express Connect circuit, you can configure BGP routing between your data center and the associated VBR. This way, the data center and the VBR can communicate with each other through a private connection. This helps you to set up a hybrid cloud with higher efficiency, flexibility, and security.
  - VBRs support BGP dynamic routing in both IPv4 and IPv6 networks.

Procedure

1. Log on to the Express Connect console.
2. In the left-side navigation pane, click **Virtual Border Router**.
3. On the **VBRs** page, click **Create VBR**.
4. In the **Create VBR** panel, set the following parameters and click **OK**.

Parameter	Description
Basic Information	
Account Type	○ **Current Organization**: creates a VBR for the current organization. ○ **Another Organization**: creates a VBR for another organization. In this example, **Current Organization** is selected.
Resource Set	Select a resource set for the VBR. You must set this parameter if **Account Type** is set to **Current Organization**.
Name	Enter a name for the VBR. You must set this parameter if **Account Type** is set to **Current Organization**.
Organization UID	You must set this parameter if the account type is set to **Another Organization**. In this case, enter the ID of the Apsara Stack account for which you want to create the VBR.
Express Connect Circuit Configurations	
Express Connect Circuit	Select an Express Connect circuit that is enabled and works as expected.

Parameter	Description
VLAN ID	Enter a VLAN ID for the VBR. Valid values: 0 to 2999. ◦ If the VLAN ID is set to 0, the switch port on the VBR is a Layer 3 router interface instead of a VLAN interface. When a Layer 3 router interface is used, each Express Connect circuit corresponds to one VBR. ◦ If the VLAN ID is set to a value from 1 to 2999, the switch port on the VBR is a Layer 3 VLAN subinterface. When a Layer 3 VLAN subinterface is used, each VLAN ID corresponds to one VBR. In this case, the Express Connect circuit with which the VBR is associated can be used to connect to VPCs that belong to different Apsara Stack accounts. VBRs in different VLANs are isolated from each other at Layer 2. **Notice** The VLAN ID that you specify for the VBR and that of the customer-premises device must be the same.
IPv4 Address of Gateway at Alibaba Cloud Side	Enter an IPv4 address for the gateway that is deployed on Apsara Stack. In this example, `192.168.101.5` is used.
IPv4 Address of Gateway at Customer Side	Enter an IPv4 address for the gateway that is deployed in the data center. In this example, `192.168.101.6` is used.
Subnet Mask (IPv4 Address)	Enter the subnet mask of the specified IPv4 addresses. In this example, `255.255.255.252` is used. You can enter a long subnet mask because only two IP addresses are required.
IPv6 Support	Specify whether to enable IPv6. ◦ **Disable**: disables IPv6. ◦ **Enable**: enables IPv6. The VPC can communicate with the data center over IPv6.
IPv6 Address of Gateway at Alibaba Cloud Side	Enter an IPv6 address for the gateway that is deployed on Apsara Stack. Example: `2001:XXXX:3c4d:0015:0000:0000:0000:1a2b`.
IPv6 Address of Gateway at Customer Side	Enter an IPv6 address for the gateway that is deployed in the data center. Example: `2001:XXXX:3c4d:0015:0000:0000:0000:2a2b`.
Subnet Mask (IPv6 Address)	Enter the subnet mask of the specified IPv6 addresses. Example: `2408:4004:cc:400::/56`. The two IPv6 addresses must fall within the same subnet.

5.3. Configure BGP

You can configure Border Gateway Protocol (BGP) routing to enable communication between a data center and a virtual border router (VBR). You must add the BGP peer that communicates with the VBR to a BGP group, and then advertise the BGP CIDR block on the VBR.

Context

BGP is a dynamic routing protocol based on Transmission Control Protocol (TCP). BGP is used to exchange routing information and network accessibility information in different autonomous systems. When you create a connection over an Express Connect circuit, you can configure BGP routing between your data center and the associated VBR to enable private communication. BGP allows you to build hybrid clouds in a more efficient, flexible, and reliable manner.

Before you configure BGP routing, you must create a BGP group. BGP groups are used to simplify BGP configurations. You can save time and effort by adding BGP peers that use the same configurations to a BGP group. You need to only create a BGP group with an Autonomous System Number (ASN) and add BGP peers that meet your requirements to the BGP group. After you add the BGP peers to the BGP group, the BGP peers share the configurations of the BGP group. This saves you the need to configure each BGP peer separately.

Limits

Before you configure BGP, take note of the following limits:

- VBRs can establish peering relationships only with data centers that are connected to the VBRs through connections over Express Connect circuits. Static routing is still required between the VBRs and VPCs.
- VBRs support only BGP-4.
- You can create at most eight BGP peers for each VBR.
- Each BGP peer supports at most 110 dynamic routes. Routes are denied when the upper limit is exceeded.
- To configure BGP when you connect to a VPC, you must specify an ASN for the VPC. The ASN that you specify must be different from the ASNs of the vSwitches in the VPC.

Step 1: Create a BGP group

Before you configure BGP routing, you must create a BGP group with the requested ASN.

1. Log on to the Express Connect console.
2. In the left-side navigation pane, click **Virtual Border Router**.
3. On the **VBRs** page, find the VBR that you want to manage and click its ID.
4. Click the **BGP Groups** tab and click **Create BGP Group**.
5. In the **Create BGP Group** dialog box, set the following parameters and click **OK**.

Parameter	Description
Name	Enter a name for the BGP group. The name must be 2 to 128 characters in length and can contain letters, digits, periods (.), underscores (_), and hyphens (-). The name must start with a letter.
Peer ASN	Enter the ASN of the data center.
BGP Key	Enter the key of the BGP group.

Parameter	Description
Description	Enter a description for the BGP group. The description must be 2 to 256 characters in length. It must start with a letter but cannot start with `http://` or `https://`.
Local AS	Enter the ASN at the Alibaba Cloud side.

Step 2: Add a BGP peer

1. Log on to the Express Connect console.
2. In the left-side navigation pane, click **Virtual Border Router**.
3. On the **VBRs** page, find the VBR that you want to manage and click its ID.
4. Click the **BGP Peers** tab and click **Create BGP Peer**.
5. In the **Create BGP Peer** dialog box, set the following parameters and click **OK**.

Parameter	Description
BGP Group	Select the BGP group to which you want to add the BGP peer.
BGP Peer IP Address	Enter the IP address of the BGP peer.

Step 3: Advertise the BGP CIDR block

After you configure BGP peers, you must advertise the CIDR block of the VPC to complete the BGP configuration. After the BGP session is established, the VBR automatically learns the CIDR block of the data center.

1. Log on to the Express Connect console.
2. In the left-side navigation pane, click **Virtual Border Router**.
3. On the **VBRs** page, find the VBR that you want to manage and click its ID.
4. Click the **Advertised BGP Subnets** tab and click **Advertise BGP Subnet**.
5. In the **Advertise BGP Subnet** dialog box, enter the CIDR block that you want to advertise and click **OK**.

5.4. Add routes

This topic describes how to add routes to the route table of a virtual border router (VBR) to manage traffic forwarding.

Context

You must add a route that points to the associated Express Connect circuit and a route that points to the virtual private cloud (VPC). This way, network traffic can be forwarded between the VPC and the data center. You can also configure BGP routing for a VBR. For more information, see Configure BGP.

Procedure

1. Log on to the Express Connect console.

2. In the left-side navigation pane, click **Virtual Border Router**.
3. On the **VBRs** page, find the VBR that you want to manage and click its ID.
4. Click the **Routes** tab and click **Add Route**.
5. In the **Edit Route Entry** dialog box, set the following parameters and click **OK**.

Parameter	Description
Next Hop Type	Select the next hop type. Valid values: ○ **VPC**: The VBR routes network traffic to a VPC. ○ **Physical Connection Interface**: The VBR routes network traffic to an Express Connect circuit.
Destination CIDR Block	Enter the destination CIDR block.
Next Hop	Select the next hop based on the specified type.

5.5. Create a peering connection

This topic describes how to create a peering connection. After you create a virtual border router (VBR), you must create a peering connection between the VBR and a virtual private cloud (VPC). This way, the VBR can route traffic between the VPC and the data center that is connected to the VBR.

For more information about how to create a peering connection, see Connect two VPCs.