ALIBABA CLOUD

Alibaba Cloud

Virtual Private Cloud

Route tables

Document Version: 20220507

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.Route table overview ---------- 05

1.Route table overview

After you create a virtual private cloud (VPC), the system creates a system route table for the VPC and adds system routes to the route table. The system routes are used to route traffic of the VPC. You cannot create or delete a system route table. However, you can add custom routes to a system route table. Custom routes are used to route traffic to specified destinations.

Route tables

- **System route tables**

  After you create a VPC, the system creates a system route table to manage routes of the VPC. By default, vSwitches in the VPC use the system route table. You cannot create or delete a system route table. However, you can add custom routes to a system route table.

- **Custom route tables**

  You can create a custom route table in a VPC and associate the custom route table with a vSwitch. This allows you to manage network traffic in a more flexible manner. For more information, see Create a custom route table.

When you manage route tables, take note of the following limits:

- Each VPC can contain at most 10 route tables including the system route table.
- Only one route table can be associated with each vSwitch. The routing policies of a vSwitch are managed by the route table that is associated with the vSwitch. You can associate one route table with multiple vSwitches.
- After you create a vSwitch, the system route table is associated with the vSwitch by default.
- If a custom route table is associated with a vSwitch and you want to replace the custom route table with the system route table, you must disassociate the custom route table from the vSwitch. If you want to associate a different custom route table with the vSwitch, you can directly replace the original custom route table without the need to disassociate the original custom route table.

Regions that support custom route tables

Area	Region
Asia Pacific	China (Qingdao), China (Beijing), China (Zhangjiakou), China (Hohhot), China (Ulanqab), China (Hangzhou), China (Shanghai), China (Shenzhen), China (Heyuan), China (Guangzhou), China (Chengdu), China (Hong Kong), Japan (Tokyo), South Korea (Seoul), Singapore (Singapore), Australia (Sydney), Malaysia (Kuala Lumpur), Indonesia (Jakarta), Philippines (Manila), Thailand (Bangkok), and India (Mumbai)
Europe & Americas	US (Silicon Valley), US (Virginia), Germany (Frankfurt), and UK (London)
Middle East	UAE (Dubai)

Routes

Each item in a route table is a route. A route consists of the destination CIDR block, the next hop type, and the next hop. The destination CIDR block is the IP address range to which you want to forward network traffic. The next hop type specifies the type of the cloud resource that is used to transmit network traffic, such as an Elastic Compute Service (ECS) instance, a VPN gateway, or a secondary elastic network interface (ENI). The next hop is the specific cloud resource that is used to transmit network traffic.

Routes are classified into system routes, custom routes, and dynamic routes.

- **System routes**

  System routes are classified into IPv4 routes and IPv6 routes. You cannot modify system routes.

  - After you create a VPC and vSwitches, the system automatically adds the following IPv4 routes to the route table:
    - A route whose destination CIDR block is 100.64.0.0/10. This route is used for communication among cloud resources within the VPC.
    - Routes whose destination CIDR blocks are the same as the CIDR blocks of the vSwitches in the VPC. These routes are used for communication among cloud resources within the vSwitches.

    For example, if you create a VPC whose CIDR block is 192.168.0.0/16 and two vSwitches whose CIDR blocks are 192.168.1.0/24 and 192.168.0.0/24, the following system routes are automatically added to the route table of the VPC. The "-" sign in the following table indicates that the item is not applicable.

Destination CIDR block	Next hop	Route type	Description
100.64.0.0/10	-	System route	Created by system.
192.168.1.0/24	-	System route	Created with vSwitch(vsw-m5exxjccadi03tvx0****) by system.
192.168.0.0/24	-	System route	Created with vSwitch(vsw-m5exxjccadi03tvx0****) by system.

  - If IPv6 is enabled for your VPC, the following IPv6 routes are automatically added to the system route table of the VPC:
    - A custom route whose destination CIDR block is `::/0` and whose next hop is an IPv6 gateway. Cloud resources deployed in the VPC use this route to access the Internet through IPv6 addresses.
    - System routes whose destination CIDR blocks are the same as the IPv6 CIDR blocks of the vSwitches in the VPC. These routes are used for communication among cloud resources within the vSwitches.

    > **Note** If you create a custom route table and associate the custom route table with a vSwitch for which IPv6 is enabled, you must add a custom route whose destination CIDR block is `::/0` and whose next hop is the IPv6 gateway. For more information, see Add a custom route entry.

- **Custom routes**

You can add custom routes to replace system routes or route traffic to a specified destination. You can specify the following types of next hops when you create a custom route:

- ECS instance: Traffic that is destined for the destination CIDR block is routed to the specified ECS instance in the VPC.

  You can select this type if you want to access the Internet or other applications through applications that are deployed on the ECS instance.
- VPN gateway: Traffic destined for the destination CIDR block is routed to the specified VPN gateway.

  You can select this type if you want to connect a VPC to another VPC or an on-premises network through the VPN gateway.
- NAT gateway: Traffic destined for the destination CIDR block is routed to the specified NAT gateway.

  You can select this type if you want to connect a VPC to the Internet through the NAT gateway.
- Router interface (to VPC): Traffic that is destined for the destination CIDR block is routed to the specified VPC.

  You can select this type if you want to connect two VPCs through Express Connect circuits.
- Router interface (to VBR): Traffic that is destined for the destination CIDR block is routed to the specified virtual border router (VBR).

  You can select this type if you want to connect a VPC to an on-premises network through Express Connect circuits.
- Secondary ENI: Traffic that is destined for the destination CIDR block is routed to the specified secondary ENI.
- Transit router: Traffic that is destined for the destination CIDR block is routed to the specified transit router.
- IPv6 gateway: Traffic that is destined for the destination CIDR block is routed to the specified IPv6 gateway.

  You can select this type if you want to implement IPv6 communication through an IPv6 gateway. You can forward traffic to the specified IPv6 gateway only if a route is added to the system route table and an IPv6 gateway is created in the region where the vSwitch associated with the system route table is deployed.

- **Dynamic routes**

  Dynamic routes are routes learned by Cloud Enterprise Network (CEN) instances, or routes learned by VPN gateways or VBRs through Border Gateway Protocol (BGP).

Route priorities

The priorities of routes take effect based on the following rules:

- If the same destination CIDR block is specified for different routes:
  - You can implement load balancing only if you select router interface (to VBR) as the next hop type and configure health checks.
  - You can implement active/standby routing only if you select router interface (to VBR) as the next hop type and configure health checks.

- In other cases, the destination CIDR blocks of different routes must be unique. The destination CIDR blocks of custom routes and dynamic routes cannot be the same as those of system routes. The destination CIDR blocks of custom routes cannot be the same as those of dynamic routes.

- If the destination CIDR blocks of different routes overlap:

  The route with the longest prefix prevails and determines how network traffic is routed. The destination CIDR blocks of custom routes and dynamic routes can contain the CIDR blocks of system routes, but cannot be more specific than the CIDR blocks of system routes.

- If the destination CIDR blocks of different routes are different:

  You can specify the same next hop for different routes.

The following table shows the route table of a VPC. The "-" sign indicates that the item is not applicable.

Destination CIDR block	Next hop type	Next hop	Route type
100.64.0.0/10	-	-	System
192.168.0.0/24	-	-	System
0.0.0.0/0	ECS instance	i-bp15u6os7nx2c9h9****	Custom
10.0.0.0/24	ECS instance	i-bp1966ss26t47ka4****	Custom

The routes whose destination CIDR blocks are `100.64.0.0/10` and `192.168.0.0/24` are system routes. The routes whose destination CIDR blocks are `0.0.0.0/0` and `10.0.0.0/24` are custom routes. Traffic destined for `0.0.0.0/0` is forwarded to the ECS instance whose ID is `i-bp15u6os7nx2c9h9****`, and traffic destined for `10.0.0.0/24` is forwarded to the ECS instance whose ID is `i-bp1966ss26t47ka4****`. Based on longest prefix matching, traffic destined for `10.0.0.1` is forwarded to `i-bp1966ss26t47ka4****`, while traffic destined for `10.0.1.1` is forwarded to `i-bp15u6os7nx2c9h9****`.

Limits

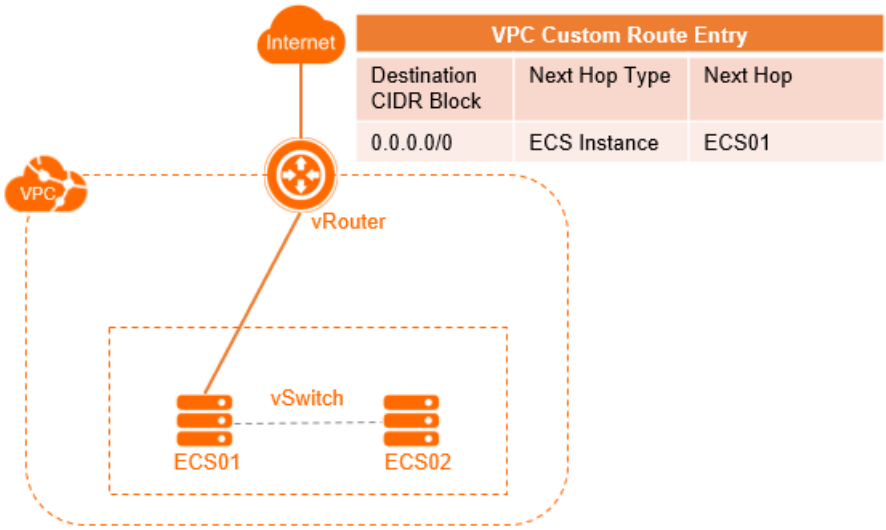
Item	Limit	Adjustable
Number of vRouters that can be created in each VPC	1	N/A
Number of custom route tables that can be created in each VPC	9	You can navigate to the Quota Management page to request a quota increase. For more information, see Manage resource quotas.
Number of custom route entries that can be created in each route table	200	

Item	Limit	Adjustable
VPCs that do not support custom route tables	If the VPC contains an ECS instance of the following types, the VPC does not support custom route tables: For more information, see Advanced VPC features.	
Number of tags that can be added to each route table	20	

Examples

You can add custom routes to a route table to control inbound and outbound traffic transmitted over a VPC.

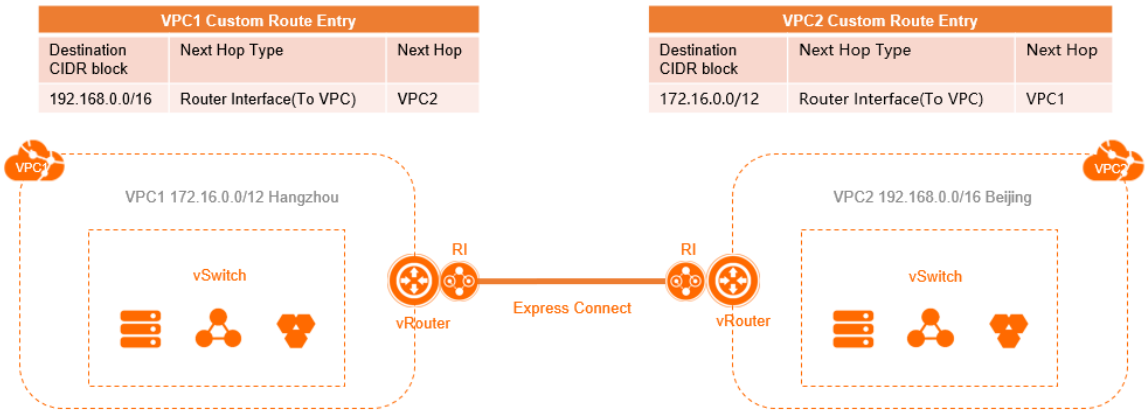
- Connect a VPC to the Internet



The preceding figure shows a NAT gateway that is deployed on an ECS instance (ECS01) in a VPC. To enable the cloud resources in the VPC to access the Internet through the ECS instance, you must add the following custom route to the route table.

Destination CIDR block	Next hop type	Next hop
0.0.0.0/0	ECS instance	ECS01

- Connect two VPCs through Express Connect



The preceding figure shows that VPC1 (172.16.0.0/12) is connected to VPC2 (192.168.0.0/16) through Express Connect. After you create router interfaces, you must add the following routes to the VPCs:

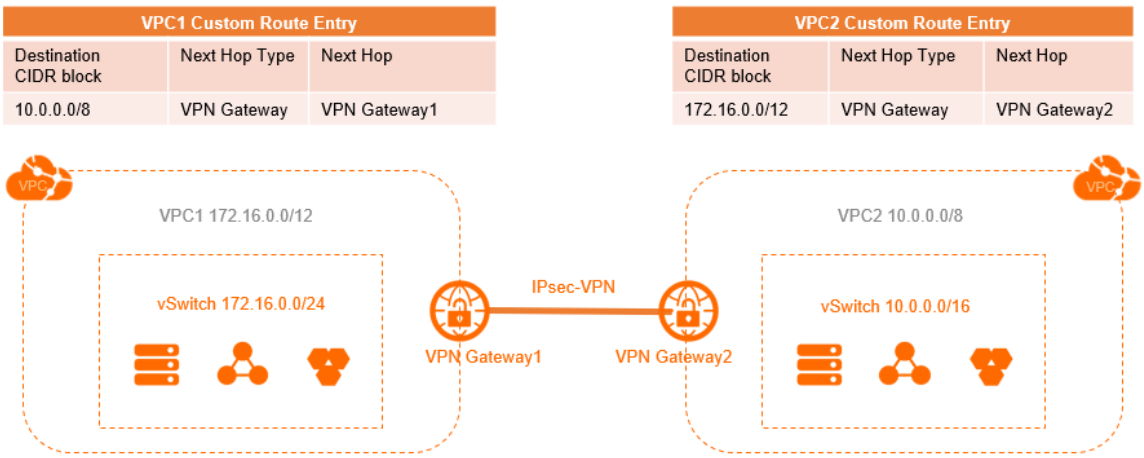
- Add the following route to VPC1

Destination CIDR block	Next hop type	Next hop
192.168.0.0/16	Router interface (to VPC)	VPC2

- Add the following route to VPC2

Destination CIDR block	Next hop type	Next hop
172.16.0.0/12	Router interface (to VPC)	VPC1

- Connect two VPCs through a VPN connection



The preceding figure shows that VPC1 (172.16.0.0/12) is connected to VPC2 (10.0.0.0/8) through a VPN connection. After you configure the VPN gateways, you must add the following routes to the VPCs.

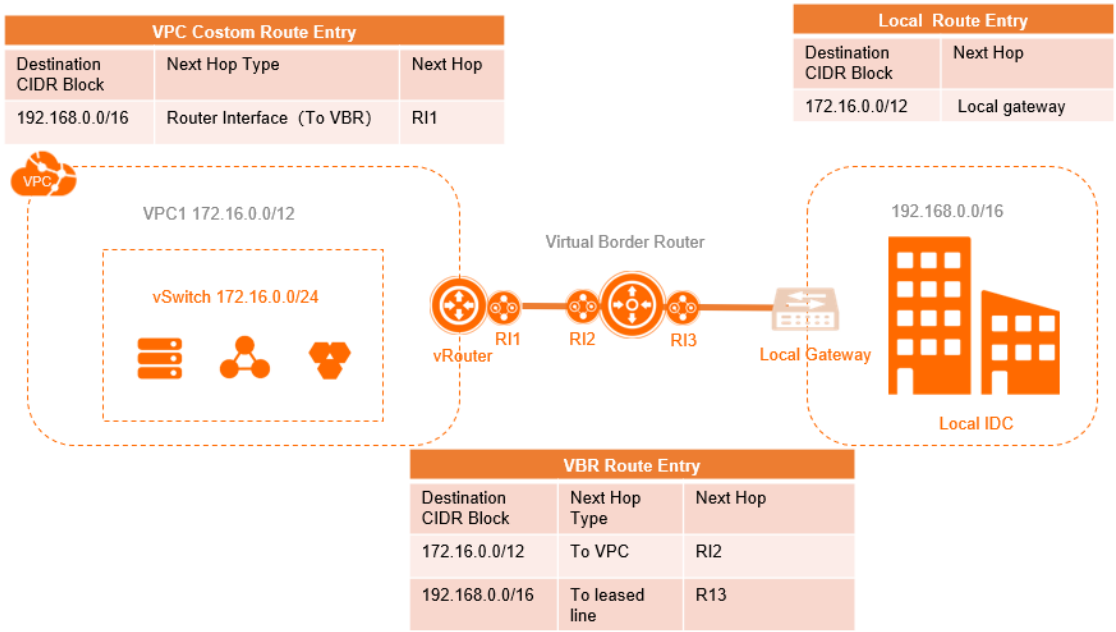
- Add the following route to VPC1

Destination CIDR block	Next hop type	Next hop
10.0.0.0/8	VPN gateway	VPN gateway 1

- Add the following route to VPC2

Destination CIDR block	Next hop type	Next hop
172.16.0.0/12	VPN gateway	VPN gateway 2

- Connect a VPC to a data center through Express Connect



The preceding figure shows that a VPC is connected to an on-premises network through Express Connect. After you configure the Express Connect circuit and the VBR, you must add the following routes:

- Add the following route to the VPC

Destination CIDR block	Next hop type	Next hop
192.168.0.0/16	Router interface (to VBR)	Router interface RI1

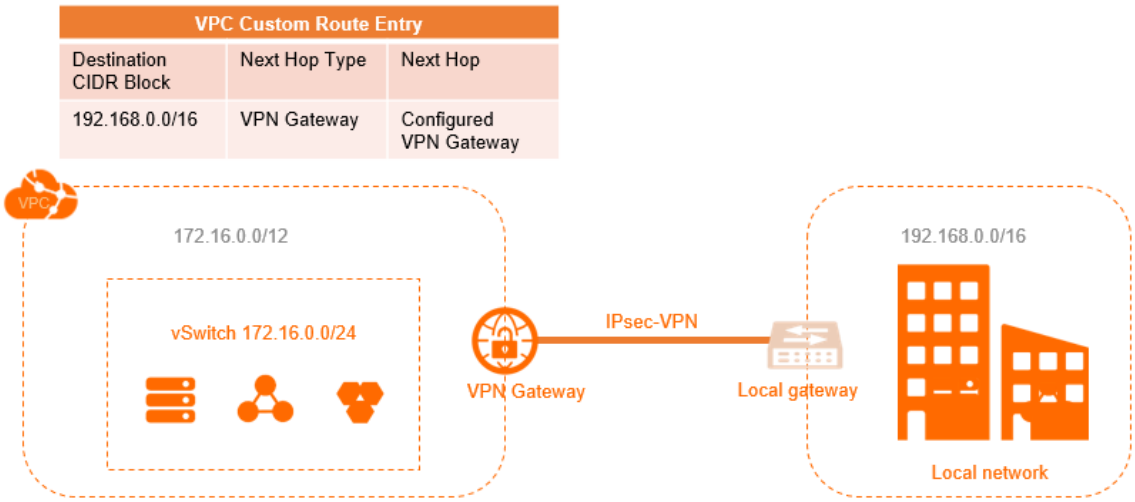
- Add the following routes to the VBR

Destination CIDR block	Next hop type	Next hop
192.168.0.0/16	Express Connect circuit	Router interface RI3
172.16.0.0/12	VPC	Router interface RI2

- Add the following route to the on-premises network

Destination CIDR block	Next hop type	Next hop
172.16.0.0/12	On-premises gateway	On-premises gateway device

- Connect a VPC to a data center through a VPN gateway



The preceding figure shows that a VPC (172.16.0.0/12) is connected to a data center (192.168.0.0/16) through a VPN gateway. After you configure the VPN gateway, you must add the following route to the VPC.

Destination CIDR block	Next hop type	Next hop
192.168.0.0/16	VPN gateway	The configured VPN gateway