

Alibaba Cloud

Virtual Private Cloud Quick Start

Document Version: 20220608

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 <code>cd /d C:/window</code> command to enter the Windows system folder.
<i>Italic</i>	Italic formatting is used for parameters and variables.	<code>bae log list --instanceid</code> <i>Instance_ID</i>
[] or [a b]	This format is used for an optional value, where only one item can be selected.	<code>ipconfig [-all -t]</code>
{ } or {a b}	This format is used for a required value, where only one item can be selected.	<code>switch {active stand}</code>

Table of Contents

1. Plan networks	05
2. Create an IPv4 VPC	09
3. Create a VPC with an IPv6 CIDR block	11

1. Plan networks

Before you create virtual private clouds (VPCs) and vSwitches, you must plan the number of VPCs and vSwitches, and CIDR blocks of VPCs and vSwitches.

- How many VPCs do I need?
- How many vSwitches do I need?
- How do I specify CIDR blocks?
- How do I specify CIDR blocks if I want to connect a VPC to another VPC or a data center?

How many VPCs do I need?

- One VPC

If you do not need to deploy your applications across regions or isolate service systems, we recommend that you create only one VPC.

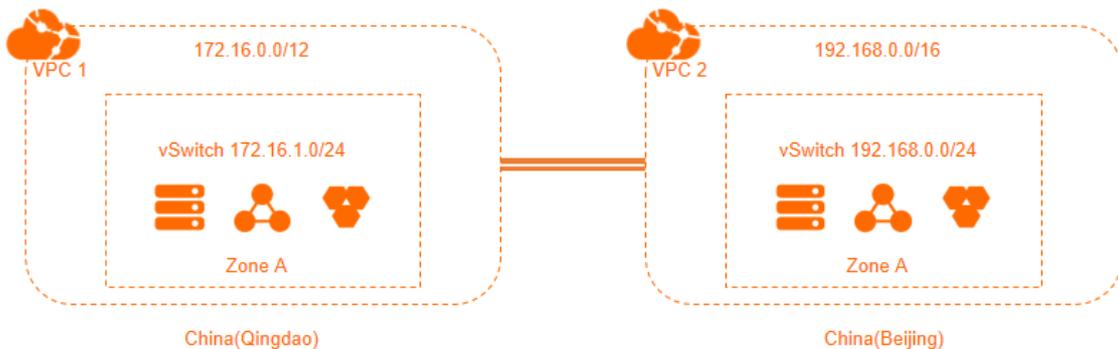


- Multiple VPCs

We recommend that you create multiple VPCs if you have one of the following requirements:

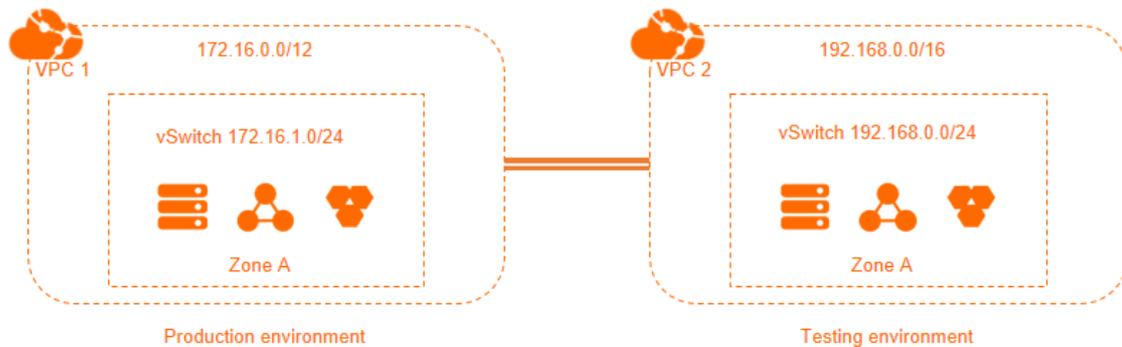
- Cross-region deployment

A VPC cannot be deployed across regions. Therefore, if you want to deploy your application systems in different regions, you must create multiple VPCs. You can use Cloud Enterprise Network (CEN), Express Connect, or VPN Gateway to connect VPCs that are deployed in different regions.



- Service isolation

If you want to isolate your service systems in the same region by using VPCs, you must create multiple VPCs. For example, you can use multiple VPCs to isolate the test environment from the production environment. You can use CEN, Express Connect, or VPN Gateway to connect VPCs that are deployed in the same region.



How many vSwitches do I need?

You can determine the number of vSwitches based on the following suggestions:

- We recommend that you create at least two vSwitches for each VPC and deploy these vSwitches in different zones to implement cross-zone disaster recovery.

Network latency between different zones in the same region is typically low. However, you must check the actual network latency after you deploy your services. The network latency may be increased due to the complex network topology. We recommend that you optimize and adapt the system to meet your requirements for high availability and low latency.

- In addition, the scale and planning of your service system must also be taken into consideration when you determine the number of vSwitches to be created. If you want the frontend system to communicate with the Internet, we recommend that you deploy different frontend systems in different vSwitches and deploy backend systems in other vSwitches. This improves service availability.

How do I specify CIDR blocks?

When you create VPCs and vSwitches, you must specify their private IP address ranges in CIDR notation.

- Specify VPC CIDR blocks

You can specify 192.168.0.0/16, 172.16.0.0/12, 10.0.0.0/8, or one of their subnets as the CIDR block of a VPC. You can also specify a custom CIDR block. 192.168.0.0/16, 172.16.0.0/12, and 10.0.0.0/8 are standard private CIDR blocks defined by the Request For Comments (RFC) series. When you specify CIDR blocks for VPCs, take note of the following rules:

- If you have only one VPC and the VPC does not need to communicate with a data center, you can specify one of the RFC CIDR blocks or their subsets as the VPC CIDR block.
- If you have multiple VPCs or want to set up a hybrid cloud environment between a VPC and your data center, we recommend that you specify the subsets of the RFC CIDR blocks for your VPCs. In this case, we recommend that you set the subnet mask length to 16 bits or less. Make sure that the CIDR blocks of the VPCs and your data center do not overlap.
- You cannot specify 100.64.0.0/10, 224.0.0.0/4, 127.0.0.0/8, 169.254.0.0/16, or one of their subnets as the VPC CIDR block.

- You must check whether a classic network is used before you specify a CIDR block for your VPC. If a classic network is used and you want to connect Elastic Compute Service (ECS) instances in the classic network to a VPC, we do not recommend that you specify 10.0.0.0/8 as the VPC CIDR block. This is because the CIDR block of the classic network is 10.0.0.0/8.

- Plan vSwitch CIDR blocks

The CIDR block of a vSwitch must be a subset of the CIDR block of the VPC to which the vSwitch belongs. For example, if the CIDR block of a VPC is 192.168.0.0/16, the CIDR block of a vSwitch that belongs to the VPC can range from 192.168.0.0/17 to 192.168.0.0/29.

When you specify CIDR blocks for vSwitches, take note of the following limits:

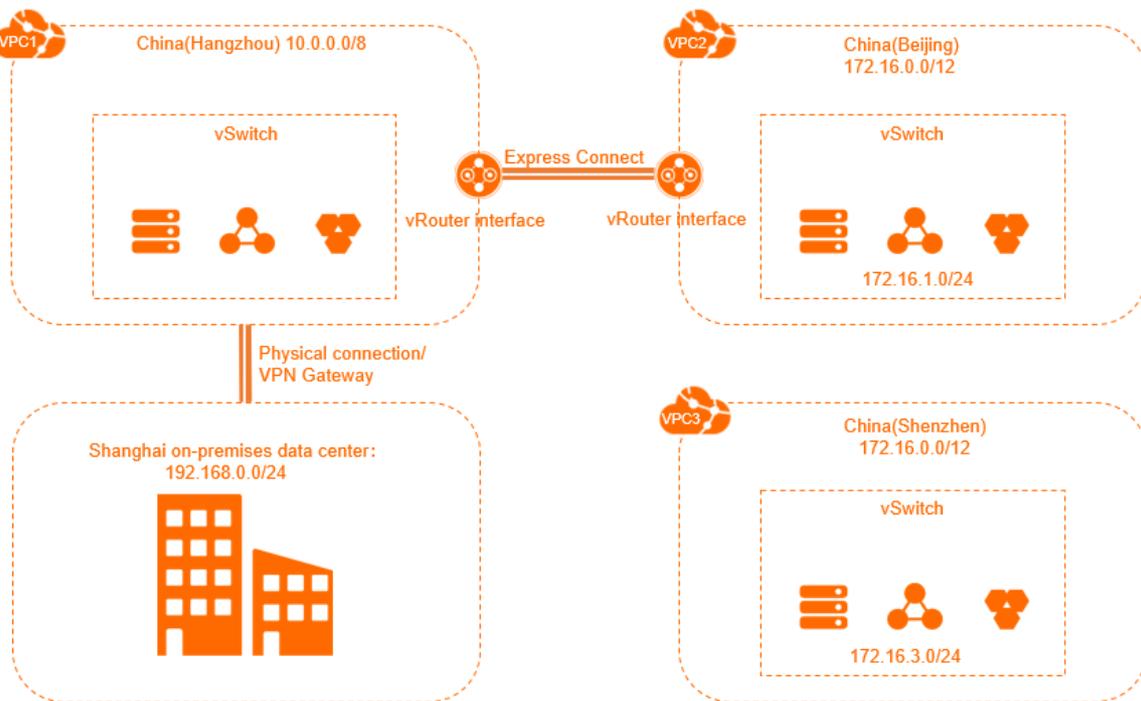
- The subnet mask of a vSwitch must be 16 to 29 bits in length, which provides 8 to 65,536 IP addresses.
- The first IP address and last three IP addresses of each vSwitch CIDR block are reserved. For example, if the CIDR block of a vSwitch is 192.168.1.0/24, IP addresses 192.168.1.0, 192.168.1.253, 192.168.1.254, and 192.168.1.255 are reserved.
- The ClassicLink feature allows ECS instances in a classic network to communicate with ECS instances in a VPC whose CIDR block is 10.0.0.0/8, 172.16.0.0/12, or 192.168.0.0/16. If the CIDR block of the VPC to communicate with the classic network is 10.0.0.0/8, the CIDR block of the vSwitch that belongs to the VPC must be 10.111.0.0/16. For more information, see [Overview](#).
- Consider the number of ECS instances that you want to deploy in a vSwitch before you specify a CIDR block for the vSwitch.

How do I specify CIDR blocks if I want to connect a VPC to another VPC or a data center?

If you want to connect a VPC to another VPC or a data center, make sure that the CIDR blocks do not overlap with each other. Take note of the following rules:

- We recommend that you specify subsets of the RFC CIDR blocks as VPC CIDR blocks to increase the number of VPC subnets. In addition, we recommend that you specify different CIDR blocks for different VPCs.
- If you cannot specify different CIDR blocks for different VPCs, try to specify different CIDR blocks for vSwitches that belong to different VPCs.
- If neither of the preceding requirements is met, make sure that the CIDR blocks of vSwitches that need to communicate with each other are different.

The following figure describes a scenario where VPC 1, VPC 2, and VPC 3 are deployed in the China (Hangzhou), China (Beijing), and China (Shenzhen) regions. VPC 1 and VPC 2 communicate with each other through Express Connect. Currently, VPC 3 does not need to communicate with other VPCs. However, VPC 3 may need to communicate with VPC 2 in the future. In addition, you have a data center in Shanghai, and you want to connect VPC 1 in the China (Hangzhou) region to the data center through Express Connect circuits.



In this example, VPC 1 and VPC 2 use different CIDR blocks. Currently, VPC 3 does not need to communicate with other VPCs. Therefore, the CIDR block of VPC 3 can be the same as that of VPC 2. However, VPC 3 may need to communicate with VPC 2 in the future. Therefore, the CIDR blocks of vSwitches in VPC 2 are different from the CIDR blocks of vSwitches in VPC 3. When a VPC communicates with another one, their CIDR blocks can be the same. However, the CIDR blocks of the vSwitches that need to communicate with each other must be different.

2. Create an IPv4 VPC

This topic describes how to create a virtual private cloud (VPC) with an IPv4 CIDR block. After you create the VPC, you can associate elastic IP addresses (EIPs) with the Elastic Compute Service (ECS) instances in the VPC. This allows the ECS instances to access the Internet.

Prerequisites

Before you deploy cloud resources in a VPC, you must first plan CIDR blocks for the VPC. For more information, see [Plan networks](#).

Step 1: Create a VPC and a vSwitch

Perform the following steps to create a VPC and a vSwitch:

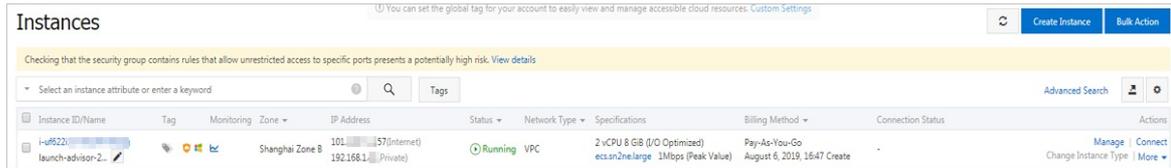
- 1.
2. In the top navigation bar, select the region where you want to deploy the VPC.
The VPC and the cloud resources that you want to deploy must belong to the same region. **China (Qingdao)** is selected in this example.
3. On the **VPCs** page, click **Create VPC**.
4. On the **Create VPC** page, set the following parameters and click **OK**.

 **Note** Allocate is selected in the IPv6 CIDR Block section in this example.

Step 2: Create an ECS instance

To create an ECS instance in the VPC, perform the following operations:

1. Log on to the [VPC console](#).
2. In the left-side navigation pane, click **vSwitch**.
3. In the top navigation bar, select the region where the vSwitch is deployed. **China (Qingdao)** is selected in this example.
4. On the **vSwitch** page, find the vSwitch that you want to manage, and choose **Create > ECS Instance** in the **Actions** column.
5. On the **Custom Launch** tab, set the following parameters:
For more information about how to configure an ECS instance, see [Create an instance by using the wizard](#).
 - **Network Type**: Select the VPC and the vSwitch that you created.
 - **Public IP Address**: Clear the check box.
 - **Security Group**: Use the default security group.
6. Click **Create Order** and complete the payment.
7. Log on to the ECS console. In the left-side navigation pane, click **Instances**. On the **Instances** page, view the details of the ECS instance.



Step 3: Create an EIP and associate the EIP with the ECS instance

An EIP is a public IP address that you can purchase and use as an independent resource. You can associate EIPs with ECS instances in a VPC to enable the ECS instances to access the Internet.

To create an EIP and associate the EIP with the ECS instance, perform the following operations:

- 1.
2. On the **Elastic IP Addresses** page, click **Create EIP**.
3. On the **Elastic IP** page, set the parameters, click **Buy Now**, and then complete the payment.
For more information, see [Apply for an EIP](#).
4. On the **Elastic IP Addresses** page, find the EIP that you created and click **Bind Resource** in the **Actions** column.
5. In the **Associate EIP with Resource** dialog box, set the following parameters and click **OK**.

Parameter	Description
Instance Type	Select ECS Instance.
Resource Group	Select the resource group to which the ECS instance belongs.
Mode	Select the mode in which the EIP is associated with the ECS instance. You can select only NAT Mode.
Select an instance to associate.	Select the ECS instance that is created in Step 2: Create an ECS instance .

Step 4: Test Internet connectivity

To test the connectivity between the ECS instance and the Internet, perform the following operations:

1. Log on to the ECS instance with which the EIP is associated. For more information, see [Connection methods](#).
2. Run the `ping` command to test the connectivity between the ECS instance and the Internet.

The test result shows that the ECS instance can communicate with the Internet.

```
[root@izbp h9icmaZ ~]# ping www.aliyun.com
PING na61-na61-wugb.idg.aliyuncdn.com (203.206.111.14) 56(84) bytes of data:
64 bytes from 203.206.111.14: icmp_seq=1 ttl=93 time=28.5 ms
64 bytes from 203.206.111.14: icmp_seq=2 ttl=93 time=28.3 ms
64 bytes from 203.206.111.14: icmp_seq=3 ttl=93 time=28.3 ms
64 bytes from 203.206.111.14: icmp_seq=4 ttl=93 time=28.3 ms
64 bytes from 203.206.111.14: icmp_seq=5 ttl=93 time=28.3 ms
64 bytes from 203.206.111.14: icmp_seq=6 ttl=93 time=28.3 ms
64 bytes from 203.206.111.14: icmp_seq=7 ttl=93 time=28.3 ms
^C
--- na61-na61-wugb.idg.aliyuncdn.com ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 7ms
rtt min/avg/max/mdev = 28.306/28.342/28.473/0.105 ms
```

3. Create a VPC with an IPv6 CIDR block

This topic describes how to create a virtual private cloud (VPC) with an IPv6 CIDR block and then create an Elastic Compute Service (ECS) instance that uses an IPv6 address. Then, the ECS instance can access other services over IPv6.

Step 1: Create a VPC and a vSwitch

Before you deploy cloud resources in a VPC, you must plan your networks. For more information, see [Plan networks](#).

1. Log on to the [VPC console](#).
2. In the top navigation bar, select the region where you want to create the VPC.

The VPC and the cloud resources that you want to deploy must be in the same region. In this example, **China (Hohhot)** is selected.

Note

3. On the **VPCs** page, click **Create VPC**.
4. On the **Create VPC** page, set the following parameters and click **OK**.

 **Note** In this example, **Assign** is selected in the **IPv6 CIDR Block** section. After you create the VPC, the system automatically assigns an IPv6 CIDR block whose prefix is **/56** to the VPC and creates a free IPv6 gateway. You can use the IPv6 gateway to process IPv6 traffic.

Step 2: Create an ECS instance

After you create a VPC with an IPv6 CIDR block and a vSwitch, create an ECS instance and assign an IPv6 address to the ECS instance. You must allocate the IPv6 address to the network interface controller (NIC) of the ECS instance.

1. Log on to the [VPC console](#).
2. In the left-side navigation pane, click **vSwitch**.
3. In the top navigation bar, select the region where the vSwitch is deployed. In this example, **China (Hohhot)** is selected.
4. On the **vSwitch** page, find the vSwitch that you want to manage, and choose **Create > ECS Instance** in the **Actions** column.
5. On the **Custom Launch** tab, set the parameters of the ECS instance.

In this example, the following parameters are set for Networking:

- **Public IP Address: Assign Public IPv4 Address and Pay-By-Bandwidth** are selected and the bandwidth limit is set to 1 Mbit/s. You can also use an elastic IP address (EIP) instead of assigning a public IP address to the ECS instance.
 - **IPv6: Assign IPv6 Address Free of Charge** is selected.
6. Return to the **Instances** page and click the ID of the ECS instance that you created to view the

IPv6 address that is assigned to the ECS instance.

7. Assign a static IPv6 address to the ECS instance.

Step 3: Purchase an IPv6 public bandwidth plan

By default, IPv6 addresses are used only for communication within private networks. If you want to allow an ECS instance that is assigned an IPv6 address to access the Internet or receive requests from IPv6 clients over the Internet, you must purchase a public bandwidth plan.

- 1.
2. In the top navigation bar, select the region of the IPv6 gateway. In this topic, **China (Hohhot)** is selected.
3. On the **IPv6 Gateway** page, find the IPv6 gateway that you want to manage and click **Manage** in the **Actions** column.
4. On the **IPv6 Internet Bandwidth** tab, find the IPv6 address that you want to manage and click **Enable IPv6 Internet Bandwidth** in the **Actions** column.
5. Specify the billing method and a bandwidth limit, click **Buy Now**, and then complete the payment.

Step 4: Configure security group rules

Services that are assigned IPv4 addresses and services that are assigned IPv6 addresses cannot communicate with each other. If the current security group rules do not support your IPv6 services, you must configure IPv6 security group rules for the ECS instance.

For more information, see [Add security group rules](#).

Step 5: Verify network connectivity

Log on to the ECS instance and run the `ping` command to `ping` an IPv6 service over the Internet to verify network connectivity. If the ECS instance can receive echo reply packets, it indicates that the connection is reachable.

The test result shows that the ECS instance can access the Internet over IPv6.

```
[root@izbp1-73damf1fZ ~]# ping6 aliyun.com
PING aliyun.com(2401:b000:1000::6 (2401:b000:1000::6)) 56 data bytes
64 bytes from 2401:b000:1000::6: icmp_seq=1 ttl=94 time=5.54 ms
64 bytes from 2401:b000:1000::6: icmp_seq=2 ttl=94 time=5.51 ms
64 bytes from 2401:b000:1000::6: icmp_seq=3 ttl=94 time=5.50 ms
64 bytes from 2401:b000:1000::6: icmp_seq=4 ttl=94 time=5.51 ms
64 bytes from 2401:b000:1000::6: icmp_seq=5 ttl=94 time=5.53 ms
64 bytes from 2401:b000:1000::6: icmp_seq=6 ttl=94 time=5.50 ms
64 bytes from 2401:b000:1000::6: icmp_seq=7 ttl=94 time=5.51 ms
64 bytes from 2401:b000:1000::6: icmp_seq=8 ttl=94 time=5.50 ms
^C
--- aliyun.com ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7011ms
rtt min/avg/max/mdev = 5.496/5.512/5.538/0.014 ms
```