

Elastic IP

FAQs

Issue 01
Date 2024-08-12



Copyright © Huawei Technologies Co., Ltd. 2024. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

Trademarks and Permissions



HUAWEI and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: <https://www.huawei.com>

Email: support@huawei.com

Security Declaration

Vulnerability

Huawei's regulations on product vulnerability management are subject to the *Vul. Response Process*. For details about this process, visit the following web page:

<https://www.huawei.com/en/psirt/vul-response-process>

For vulnerability information, enterprise customers can visit the following web page:

<https://securitybulletin.huawei.com/enterprise/en/security-advisory>

Contents

1 Product Consultation	1
1.1 Managing Quotas	1
1.2 How Do I Assign or Retrieve a Specific EIP?	2
1.3 Why Is an EIP Newly Assigned the Same as the One I Released?	3
1.4 Can I Buy a Specific EIP?	3
1.5 Does an EIP Change Over Time?	3
1.6 Why Can't I Find My Purchased EIP on the Management Console?	3
1.7 What Is the EIP Assignment Policy?	4
1.8 How Do I Query the Region of My EIPs?	5
1.9 Can a Bandwidth Be Used by Multiple Accounts?	5
1.10 How Do I Query the Traffic Usage of My EIP?	5
1.11 Do I Need to Configure a Shared Data Package for Use After It Is Purchased?	6
1.12 Can I Change the Dedicated Bandwidth Used by an EIP to a Shared Bandwidth?	6
1.13 How Many ECSs Can I Bind an EIP To?	6
1.14 What Are the Differences Between EIP, Private IP Address, and Virtual IP Address?	6
1.15 What Are the Differences Among a Bandwidth Add-On Package, Shared Data Package, and Shared Bandwidth?	9
1.16 What Are the Differences Between the Primary and Extension NICs of ECSs?	9
1.17 When Should I Use Premium BGP and Are There Any Limitations on Using Premium BGP?	10
1.18 Why My EIPs Are Frozen? How Do I Unfreeze My EIPs?	10
2 Billing and Payments	12
2.1 How Is an EIP Billed?	12
2.2 How Do I Change My EIP Billing Mode Between Pay-per-Use and Yearly/Monthly?	13
2.3 How Do I Change the Billing Option of a Pay-per-Use EIP Between By Bandwidth and By Traffic?	15
2.4 Why Am I Still Being Billed After My EIP Has Been Unbound or Released?	15
2.5 When Will I Be Billed for Reservation Price?	17
3 EIP Binding and Unbinding	18
3.1 How Do I Access an ECS with an EIP Bound from the Internet?	18
3.2 How Can I Unbind an Existing EIP from an Instance and Bind Another EIP to the Instance?	18
3.3 Can I Bind an EIP of an ECS to Another ECS?	20
3.4 Can I Bind an EIP to a Cloud Resource in Another Region?	21
3.5 Can Multiple EIPs Be Bound to an ECS?	21
3.6 What Are the Differences Between Unbinding and Releasing an EIP?	21

4 Bandwidth	23
4.1 What Bandwidth Types Are Available?	23
4.2 How Many EIPs Can I Add to Each Shared Bandwidth?	23
4.3 What Are the Differences Between a Dedicated Bandwidth and a Shared Bandwidth?	23
4.4 What Are Inbound Bandwidth and Outbound Bandwidth?	24
4.5 How Do I Know If My EIP Bandwidth Limit Has Been Exceeded?	25
4.6 What Are the Differences Between Public Bandwidth and Private Bandwidth?	28
4.7 Can I Increase Then Decrease a Yearly/Monthly Bandwidth?	29
4.8 What Is the Relationship Between Bandwidth and Upload/Download Rate?	29
4.9 What Are the Differences Among Static BGP, Dynamic BGP, and Premium BGP?	29
5 Connectivity	32
5.1 What Are the Priorities of the Custom Route and EIP If Both Are Configured for an ECS to Enable the ECS to Access the Internet?	32
5.2 Why Can't My ECS Access the Internet Even After an EIP Is Bound?	32
5.3 What Should I Do If an EIP Cannot Be Pinged?	36
5.4 How Do I Unblock an EIP?	44
5.5 Why Is There Network Jitter or Packet Loss During Cross-Border Communications?	44
5.6 Why Does the Download Speed of My ECS Is Slow?	44

1 Product Consultation

1.1 Managing Quotas

What Is a Quota?

A quota limits the quantity of a resource available to users, thereby preventing spikes in the usage of the resource. For example, a VPC quota limits the number of VPCs that can be created.

You can also request for an increased quota if your existing quota cannot meet your service requirements.

How Do I View My Quotas?


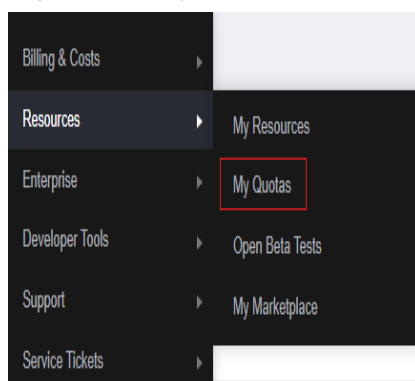
1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. In the upper right corner of the page, choose **Resources > My Quotas**.
The **Service Quota** page is displayed.

Figure 1-1 My Quotas

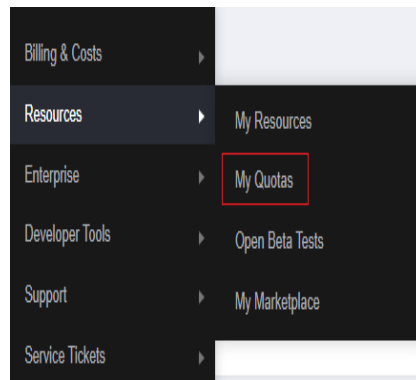


4. View the used and total quota of each type of resources on the displayed page.
If a quota cannot meet service requirements, apply for a higher quota.

How Do I Apply for a Higher Quota?

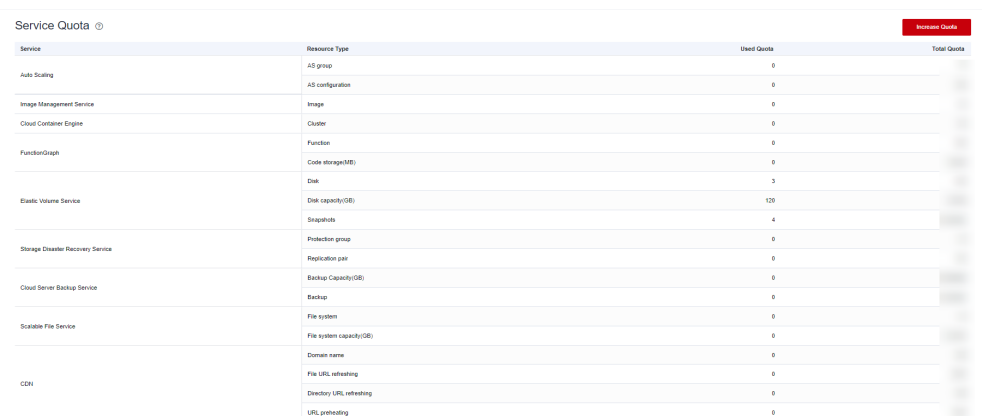
1. Log in to the management console.
2. In the upper right corner of the page, choose **Resources > My Quotas**. The **Service Quota** page is displayed.

Figure 1-2 My Quotas



3. Click **Increase Quota** in the upper right corner of the page.

Figure 1-3 Increasing quota



Service	Resource Type	Used Quota	Total Quota
Auto Scaling	AS group	0	
	AS configuration	0	
Image Management Service	Image	0	
Cloud Container Engine	Cluster	0	
FunctionGraph	Function	0	
	Code storage(MD)	0	
Elastic Volume Service	Disk	3	
	Disk capacity(OB)	120	
Storage Disaster Recovery Service	Snapshots	4	
	Protection group	0	
Cloud Server Backup Service	Replication pair	0	
	Backup Capacity(OB)	0	
Scalable File Service	Backup	0	
	File system	0	
CDN	File system capacity(OB)	0	
	Domain name	0	
	File URL refreshing	0	
	Director URL refreshing	0	
	URL prewarming	0	

4. On the **Create Service Ticket** page, configure parameters as required. In the **Problem Description** area, fill in the content and reason for adjustment.
5. After all necessary parameters are configured, select **I have read and agree to the Ticket Service Protocol and Privacy Statement** and click **Submit**.

1.2 How Do I Assign or Retrieve a Specific EIP?

If you want to retrieve an EIP that you have released or assign a specific EIP, you can use APIs by setting the value of **ip_address** to the one that you want to assign. For details, see [Elastic IP API Reference](#).

 NOTE

- If the EIP has been assigned to another user, you will fail to assign your required EIP.
- You cannot use the management console to assign a specific EIP.

1.3 Why Is an EIP Newly Assigned the Same as the One I Released?

If you have released EIPs in a region, the system preferentially assigns EIPs from the ones you released in the last 24 hours.

If you do not want an EIP that you have released, assign an EIP first and then release the one that you do not want.

You can assign a specific EIP by calling APIs. For details, see [Elastic IP API Reference](#).

1.4 Can I Buy a Specific EIP?

By default, EIPs are assigned randomly.

- If you assign a new EIP within 24 hours after an EIP is released, the released EIP will be assigned first.
- Other users can call APIs to assign the released EIP 24 hours after it is released.

You can assign a specific EIP only by calling an API. For details, see [Assigning an EIP](#).

1.5 Does an EIP Change Over Time?

EIPs will not be changed after they are assigned.

- Stopping and starting an ECSs does not change its EIP.
- Billing mode change does not change EIPs.

An EIP will be released if it expires or if the EIP owner's account is in arrears.

1.6 Why Can't I Find My Purchased EIP on the Management Console?

Symptom

After I logged in to the management console, I could not find my purchased EIP.

Possible Cause

- Your EIP is not in the current region. For details, see [EIP Not in the Current Region](#).

- Your EIP has been released because it has expired but has not been renewed. For details, see [EIP Was Released](#).

EIP Not in the Current Region

Step 1 Log in to the management console.

Step 2 Locate the EIP.

- Method 1:
 - a. In the upper left corner of the console, select the region to which the EIP to be queried belongs.
 - b. Under **Networking**, click **Elastic IP**.
 - c. In the EIP list, view your EIPs.
- Method 2:
 - a. In the upper right corner of the console, choose **Resources > My Resources**.
 - b. On the **My Resources** page, set search criteria to quickly find the target EIP.
 - **Service: Virtual Private Cloud (VPC)**
 - **Resource Type: EIPs**
 - **Region:** Retain the default value **All** or select the region to which the EIP to be queried belongs.
For example, if you select **All** for **Region**, all of your EIPs will be displayed.
 - c. In the EIP list, view your EIPs.

----End

EIP Was Released

Yearly/monthly EIPs will be released when they expire and have not been renewed.

- If you need to buy an EIP and bind it to a cloud resource, refer to [Assigning an EIP](#).
- If you want to retrieve an EIP that you have released, refer to [How Do I Assign or Retrieve a Specific EIP?](#)

1.7 What Is the EIP Assignment Policy?

By default, EIPs are assigned randomly.

If an EIP is released by mistake, the system will preferentially assign you an EIP that you have released in the last 24 hours.

If you want a specific EIP that you released more than 24 hours ago, see [How Do I Assign or Retrieve a Specific EIP?](#)

If you do not want an EIP that you have released, it is recommended that you buy another EIP first and then release the one that you do not need.

1.8 How Do I Query the Region of My EIPs?

You can visit <https://en.ipip.net/ip.html> to query the region of your EIPs.

- The region of an EIP identified using a third-party website may be different from the region that the EIP belongs to.
- If the region identified using another third-party website is different from the one identified using <https://en.ipip.net/ip.html>, use the region identified using <https://en.ipip.net/ip.html>.
- If the region identified using <https://en.ipip.net/ip.html> is different from the one you selected when purchasing the EIP, use the region you had selected during EIP purchase.

NOTE

The geographical location of an EIP purchased in CN North-Ulanqab1 is Beijing.

- If your service is adversely affected because the region of your EIP cannot be determined, [submit a service ticket](#).

To know more about the region of EIPs, [submit a service ticket](#).

1.9 Can a Bandwidth Be Used by Multiple Accounts?

A bandwidth cannot be shared between different accounts. Each account can use and manage only its own EIP bandwidths.

1.10 How Do I Query the Traffic Usage of My EIP?

Description

I want to view the amount of traffic consumed by my EIP.

Notes and Constraints

Only the usage of pay-per-use EIPs billed by traffic can be queried.

Procedure

1. Log in to the management console.
2. On the top menu bar, choose **Billing** > **Bills**.
The **Dashboard** page is displayed.
3. Choose **Billing** > **Expenditure Details** and sort by usage.
4. View the traffic usage on the displayed page.

1.11 Do I Need to Configure a Shared Data Package for Use After It Is Purchased?

No.

A shared data package takes effect immediately after being purchased and no additional operations are required. If you have subscribed to pay-per-use EIPs billed by traffic in a region and buy a shared data package in the same region, the EIPs will use the shared data package.

1.12 Can I Change the Dedicated Bandwidth Used by an EIP to a Shared Bandwidth?

Yes.

You can change the dedicated bandwidth used by a pay-per-use EIP to a shared bandwidth.

You cannot change the dedicated bandwidth used by a yearly/monthly EIP to a shared bandwidth.

1.13 How Many ECSs Can I Bind an EIP To?

An EIP can be bound to only one ECS.

An EIP cannot be shared by multiple ECSs, and the EIP and ECS must be in the same region. You can use public NAT gateways to enable the ECSs in the VPC to share an EIP to access or be accessed by the Internet.

For more information, see the [NAT Gateway User Guide](#).

1.14 What Are the Differences Between EIP, Private IP Address, and Virtual IP Address?

Different types of IP addresses have different functions.

Figure 1-4 IP address architecture

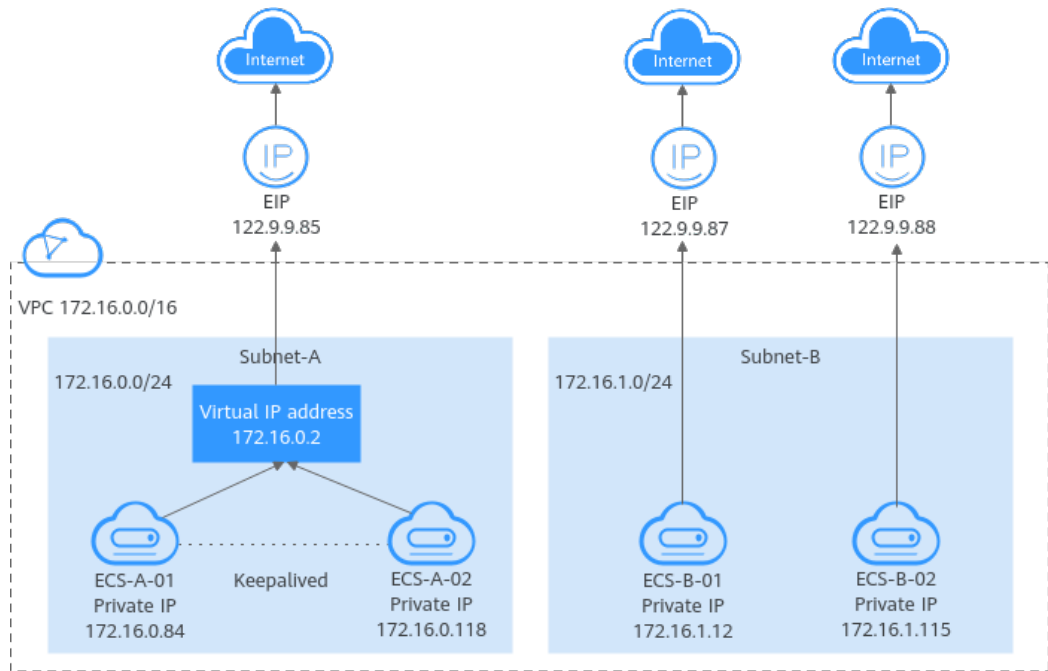


Table 1-1 Functions of different IP address types

IP Address Type	Description	Example Value
Private IP address	Private IP addresses come with your ECSs and belong to the VPC subnets of the ECSs. They are used for private communication on the cloud.	<ul style="list-style-type: none"> Private IP address of ECS-A-01: 172.16.0.84 Private IP address of ECS-B-01: 172.16.1.12

IP Address Type	Description	Example Value
Virtual IP address	<p>A virtual IP address is a private IP address that can be independently assigned from and released to a VPC subnet. You can:</p> <ul style="list-style-type: none">• Bind one or more virtual IP addresses to an ECS so that you can use either the virtual IP address or private IP address to access the ECS. If you have multiple services running on an ECS, you can use different virtual IP addresses to access them.• Bind a virtual IP address to multiple ECSs. You can use a virtual IP address and an HA software (such as Keepalived) to set up a high-availability active/standby cluster. If you want to improve service availability and eliminate single points of failure, you can deploy ECSs in the active/standby pair or deploy one active ECS and multiple standby ECSs. In this case, the ECSs can use the same virtual IP address. If the active ECS goes down, the standby ECS becomes the active ECS and continues to provide services. <p>For more information about virtual IP addresses, see Virtual IP Address Overview. For details about how to set up a high availability cluster, see Using a Virtual IP Address and Keepalived to Set Up a High-Availability Web Cluster.</p>	<p>Bind virtual IP address (172.16.0.2) both ECS-A-01 and ECS-A-02. The active/standby switchover of ECS-A-01 and ECS-A-02 can be implemented by using Keepalived.</p>
EIP	<p>EIPs allow cloud resources to access the Internet. They can be flexibly bound to or unbound from instances.</p> <ul style="list-style-type: none">• You can bind an EIP to a virtual IP address to enable the ECSs with the virtual IP address bound to access the Internet.• You can also bind an EIP to the ECSs to enable them to access the Internet. <p>For more information, see EIP Overview.</p>	<ul style="list-style-type: none">• Bind EIP (122.9.9.85) to virtual IP address (172.16.0.2) to enable ECS-A-01 and ECS-A-02 to access the Internet.• Bind EIP (122.9.9.87) to ECS-B-01 to enable ECS-B-01 to access the Internet.

1.15 What Are the Differences Among a Bandwidth Add-On Package, Shared Data Package, and Shared Bandwidth?

Bandwidth add-on packages, shared data packages, and shared bandwidths are different products.

Table 1-2 Differences among a bandwidth add-on package, shared data package, and shared bandwidth

Aspect	Bandwidth Add-On Package	Shared Data Package	Shared Bandwidth
Customer	All customers	All customers	Medium- and large-scale customers
Feature	A bandwidth add-on package is used to temporarily increase the maximum shared or dedicated bandwidth of a yearly/monthly EIP. If you need to temporarily increase your bandwidth, you can purchase a bandwidth add-on package with a specific validity period.	After a shared data package takes effect, EIPs billed by traffic will use the shared data package first. After the shared data package is used up, the EIPs will be billed by traffic on a pay-per-use basis. Shared data packages are cost-effective than billing by traffic on a pay-per-use basis.	Multiple pay-per-use EIPs can share the same bandwidth. Shared bandwidth can be billed by bandwidth or by 95th percentile bandwidth (enhanced).
Usage method	The validity period of a bandwidth add-on package must be within that of the bandwidth you want to add the package to.	A shared data package takes effect immediately after being purchased and you do not need to perform any configurations.	After purchasing a shared bandwidth, you need to add EIPs to the shared bandwidth.

1.16 What Are the Differences Between the Primary and Extension NICs of ECSs?

The differences are as follows:

- Generally, the OS default routes preferentially use the primary NICs. If the OS default routes use the extension NICs, network communication will be interrupted. Then, you can check the route configuration to rectify the network communication error.
- Primary NICs can communicate with the public service zone (zone where PaaS and DNS services are deployed). Extension NICs cannot communicate this zone.

1.17 When Should I Use Premium BGP and Are There Any Limitations on Using Premium BGP?

Scenario: Premium BGP chooses the optimal path and ensures low-latency and high-quality networks. BGP is used to interconnect with lines of multiple mainstream carriers. Public network connections that feature low latency and high quality are directly established between Chinese mainland and Hong Kong (China).

Limitations

- Bandwidths of the premium BGP type are available only in **CN-Hong Kong**.
- Premium EIPs can be billed on a yearly/monthly or pay-per-use basis.
- Only premium BGP EIPs can be added to shared bandwidths of the premium BGP type.
- Premium BGP does not support shared data packages and bandwidth add-on packages.

1.18 Why My EIPs Are Frozen? How Do I Unfreeze My EIPs?

- **In arrears**
 - Yearly/Monthly EIPs
If you do not renew yearly/monthly EIPs after the grace period ends, the EIPs enter a retention period and are frozen. Frozen EIPs cannot be used, modified, or released. If you still do not renew your EIPs before the retention period ends, they will be released and cannot be restored. To ensure the availability of your EIPs, renew them before they expire.
 - Pay-per-use EIPs
If your pay-per-use EIPs are still in arrears after the grace period ends, the EIPs enter the retention period and are frozen. Frozen EIPs cannot be used, modified, or released. If you still do not top up and pay off the arrears before the retention period ends, the EIPs will be released and cannot be restored. To ensure the availability of your EIPs, top up your account and pay off the arrears before they expire.
 - Frozen EIPs will be available after you renew them or top up your account. You can renew your resources on the management console. For more details, see [Renewal Management](#).
- **Attacks**

EIPs will be frozen if their associated instances have security violations, such as attacks. Frozen EIPs are unavailable and cannot be modified or released. To unfreeze EIPs, [create a service ticket](#). You can change an EIP for an instance by referring to [How Can I Unbind an Existing EIP from an Instance and Bind Another EIP to the Instance?](#)

- **Violations**

The server bound to the EIP is suspected of violations and the EIP is frozen by the national supervision department. If you have confirmed that you have not been involved in any violation, contact the national supervision department to file an appeal. If the appeal is successful, Huawei Cloud will receive an unsealing instruction to unfreeze your resources. You can change an EIP for an instance by referring to [How Can I Unbind an Existing EIP from an Instance and Bind Another EIP to the Instance?](#)

2 Billing and Payments

2.1 How Is an EIP Billed?

There are yearly/monthly and pay-per-use billing modes. Each one has different advantages and disadvantages. Yearly/Monthly: You pay upfront for the amount of time you expect to use the EIP for. You will need to make sure your account has a sufficient balance or you have a valid payment method configured first. Pay-per-use: You can start using the EIP first and then pay as you go. You are billed based on the EIP usage duration (by bandwidth) or used traffic (by traffic).

You will be billed for the EIP and fixed bandwidth.

- EIP reservation price
If your pay-per-use EIP has no instance bound, you will be billed for the EIP reservation price.
- Fixed bandwidth
 - EIP bandwidth prices: bandwidth prices of yearly/monthly EIPs and pay-per-use EIPs (by bandwidth); traffic price of pay-per-use EIPs (by traffic)
 - Shared bandwidth price
 - Shared data package price

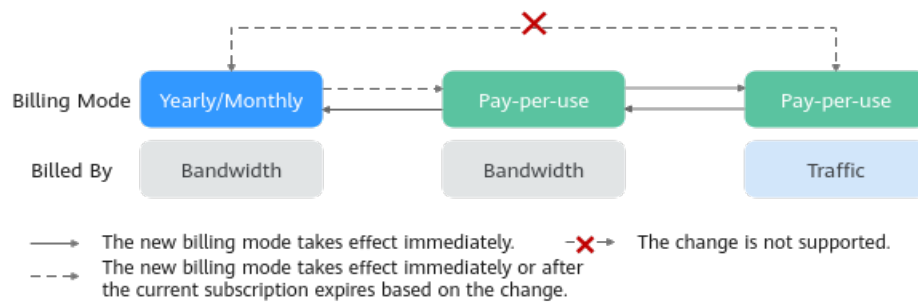
For details, see [EIP Billing](#).

2.2 How Do I Change My EIP Billing Mode Between Pay-per-Use and Yearly/Monthly?



Table 2-1 Billing mode change description

Change	Description
From yearly/monthly to pay-per-use	<ul style="list-style-type: none">• An EIP billed on a yearly/monthly basis can be directly changed to be billed on a pay-per-use basis (billed by bandwidth).• An EIP billed on a yearly/monthly basis cannot be directly changed to be billed on a pay-per-use basis (billed by traffic). To change this:<ol style="list-style-type: none">1. Change the yearly/monthly EIP to be billed by bandwidth on a pay-per-use basis.2. Change the EIP billed by bandwidth on a pay-per-use basis to be billed by traffic on a pay-per-use basis. <p>The new billing mode takes effect only after the yearly/monthly subscription expires, if you want to change the EIP to be billed by bandwidth on a pay-per-use basis upon expiration.</p> <p>The new billing mode takes effect immediately, if you want to change the EIP to be billed by bandwidth on a pay-per-use basis immediately.</p>
From pay-per-use to yearly/monthly	<ul style="list-style-type: none">• An EIP that is billed by bandwidth on a pay-per-use basis can be directly changed to be billed on a yearly/monthly basis.• An EIP that is billed by traffic on a pay-per-use basis cannot be directly changed to be billed on a yearly/monthly basis. To change this:<ol style="list-style-type: none">1. Change the EIP billed by traffic on a pay-per-use basis to be billed by bandwidth on a pay-per-use basis.2. Change the EIP billed by bandwidth on a pay-per-use basis to be billed on a yearly/monthly basis. <p>After the change is successful, the new billing mode takes effect immediately.</p>



Figure 2-1 EIP billing change



From Yearly/Monthly to Pay-Per-Use upon Expiration (Billed by Bandwidth)

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click  in the upper left corner and choose **Networking > Elastic IP**.
4. In the displayed dialog box, confirm the information and click **Yes**.
You are switched to a page of the Billing Center.
5. Confirm the information and click **Change to Pay-per-Use**.

From Pay-per-Use (Billed by Bandwidth) to Yearly/Monthly



1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click  in the upper left corner and choose **Networking > Elastic IP**.
4. In the EIP list, change the billing mode of a single EIP or multiple EIPs from pay-per-use (billed by bandwidth) to yearly/monthly.
 - Single EIP:
Locate the row that contains the EIP and choose **More > Change Billing Mode** in the **Operation** column.
 - Multiple EIPs:
Select EIPs and choose **More > Change Billing Mode** in the upper left corner of the EIP list.
5. In the displayed dialog box, confirm the information and click **Yes**.
6. On the **Change Subscriptions** page, set parameters such as **Renewal Duration**.
7. Click **Pay**.

2.3 How Do I Change the Billing Option of a Pay-per-Use EIP Between By Bandwidth and By Traffic?

Table 2-2 EIP billing mode change description

Change	Description
From billing by traffic (pay-per-use) to billing by bandwidth (pay-per-use)	A pay-per-use EIP billed by traffic can be directly changed to be billed by bandwidth. After the change is successful, the new billing mode takes effect immediately.
From billing by bandwidth (pay-per-use) to billing by traffic (pay-per-use)	A pay-per-use EIP billed by bandwidth can be directly changed to be billed by traffic. After the change is successful, the new billing mode takes effect immediately.

Pay-per-Use EIPs: From Billing By Traffic to By Bandwidth

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click  in the upper left corner and choose **Networking** > **Elastic IP**.
4. In the EIP list, locate the row that contains the EIP, click **More** in the **Operation** column, and click **Modify Bandwidth**.
5. On the **Modify Bandwidth** page, change the billing option as prompted.
You can also change the bandwidth name and size.
6. Click **Next**.
7. On the displayed page, confirm the configurations and click **Submit**.

NOTE

- Changing the billing options does not change EIPs or interrupt their use.
- The preceding change scenarios apply only to **pay-per-use** EIPs.
- **Yearly/monthly** EIPs cannot be directly changed to **pay-per-use EIPs billed by traffic**. If the change is required, refer to [How Do I Change My EIP Billing Mode Between Pay-per-Use and Yearly/Monthly?](#)

2.4 Why Am I Still Being Billed After My EIP Has Been Unbound or Released?

Symptom

After my EIP is unbound from an instance or is released, the EIP is still being billed.

Yearly/monthly EIPs are prepaid and you have already paid for the EIPs during the validity period. Unbinding an EIP or modifying its bandwidth does not affect the fees. This section describes the possible causes only for pay-per-use EIPs.

Possible Causes

Table 2-3 Possible causes that pay-per-use EIPs are billed

EIP Status	Billed By	Possible Cause
EIP is unbound from an instance.	Pay-per-use EIP billed by traffic	<ul style="list-style-type: none"> EIP reservation price: If a pay-per-use EIP is unbound from an instance, the reservation price will be billed. If your EIP is no longer required, release it to stop the billing. Traffic: will not be billed.
	Pay-per-use EIP billed by bandwidth	<ul style="list-style-type: none"> EIP reservation price: If a pay-per-use EIP is unbound from an instance, the reservation price will be billed. If your EIP is no longer required, release it to stop the billing. Bandwidth: will continue to be billed. If you do not want to pay for the bandwidth, change the EIP from billing by bandwidth to by traffic.
	Pay-per-use EIP added to a shared bandwidth	<ul style="list-style-type: none"> EIP reservation price: If a pay-per-use EIP is unbound from an instance, the reservation price will be billed. If your EIP is no longer required, release it to stop the billing. Shared bandwidth: will continue to be billed. A shared bandwidth and an EIP are billed separately. Unbinding and releasing an EIP will not affect the billing of the shared bandwidth. If you do not need the shared bandwidth anymore, delete it.
EIP is released.	<ul style="list-style-type: none"> Pay-per-use EIP billed by traffic Pay-per-use EIP billed by bandwidth 	The EIP, traffic, and bandwidth will stop being billed. If you find that you are still being billed, check whether your account has a shared bandwidth.
	Pay-per-use EIP added to a shared bandwidth	A shared bandwidth and an EIP are billed separately. Unbinding and releasing an EIP will not affect the billing of the shared bandwidth. If you do not need the shared bandwidth anymore, delete it .

2.5 When Will I Be Billed for Reservation Price?

If your pay-per-use EIP has no instance bound, you will be billed for the EIP reservation price.

You will not be billed for pay-per-use EIPs bound to instances and yearly/monthly EIPs.

3 EIP Binding and Unbinding

3.1 How Do I Access an ECS with an EIP Bound from the Internet?

Each ECS is automatically added to a security group after being created to ensure its security. The security group denies access traffic from the Internet by default (except TCP traffic from port 22 through SSH to a Linux ECS and TCP traffic from port 3389 through RDP to a Windows ECS). To allow external access to ECSs in the security group, add an inbound rule to the security group.

You can set **Protocol** to **TCP**, **UDP**, **ICMP**, or **All** as required on the page for creating a security group rule.

- If your ECS needs to be accessible over the Internet and you know the IP address used to access the ECS, set **Source** to the IP address range containing the IP address.
- If your ECS needs to be accessible over the Internet but you do not know the IP address used to access the ECS, retain the default setting 0.0.0.0/0 for **Source**, and then set allowed ports to improve network security.


The default source **0.0.0.0/0** indicates that all IP addresses can access ECSs in the security group.

- Allocate ECSs that have different Internet access requirements to different security groups.

3.2 How Can I Unbind an Existing EIP from an Instance and Bind Another EIP to the Instance?



Scenario 1: Unbinding an EIP from an ECSs and Binding a New EIP to the ECSs

1. Unbind an EIP.
 - a. Log in to the management console.

- b. Click  in the upper left corner and choose **Networking > Elastic IP**.
 - c. On the displayed page, locate the row that contains the target EIP, and click **Unbind**.
 - d. Click **Yes**.
2. Assign an EIP.


 **NOTE**

If you already have an EIP that you require, skip this step.

- a. Log in to the management console.
 - b. Click  in the upper left corner and choose **Networking > Elastic IP**.
 - c. On the displayed page, click **Buy EIP**.
 - d. Set the parameters as prompted.
 - e. Click **Next**.
3. Bind the new EIP to the ECS.
 - a. Log in to the management console.
 - b. Click  in the upper left corner and choose **Networking > Elastic IP**.
 - c. On the **EIPs** page, locate the row that contains the target EIP, and click **Bind**.
 - d. Select the desired ECS.
 - e. Click **OK**.
 4. Release the EIP that is unbound.

 **NOTE**

If an unbound EIP is no longer required, you can release it. If you do not release an unbound EIP, it will continue to be billed.

- a. Log in to the management console.
- b. Click  in the upper left corner and choose **Networking > Elastic IP**.
- c. In the EIP list, locate the row that contains the EIP, and choose **More > Release** in the **Operation** column.
- d. Click **Yes**.

Scenario 2: Unbinding an EIP from a Load Balancer and Binding a New EIP to the Load Balancer

1. Unbind an EIP.
 - a. Log in to the management console.
 - b. Click **Service List**. Under **Networking**, click **Elastic Load Balance**.
 - c. In the load balancer list, locate the target load balancer and choose **More > Unbind EIP** in the **Operation** column.
 - d. Click **Yes**.
2. Assign an EIP by referring to [2](#).

 NOTE

If you already have an EIP that you require, skip this step.

3. Bind the new EIP to the load balancer.
 - a. Log in to the management console.
 - b. Click **Service List**. Under **Networking**, click **Elastic Load Balance**.
 - c. In the load balancer list, locate the target load balancer and choose **More > Bind EIP** in the **Operation** column.
 - d. In the **Bind EIP** dialog box, select the EIP to be bound and click **OK**.
4. Release the EIP that was replaced. For details, see [4](#).

 NOTE

If an unbound EIP is no longer required, you can release it. If you do not release an unbound EIP, it will continue to be billed.

Scenario 3: Unbinding an EIP from a NAT Gateway and Binding a New EIP to the NAT Gateway

1. Assign an EIP by referring to [2](#).

 NOTE

If you already have an EIP that you require, skip this step.

2. Modify an SNAT rule.

For details, see [Modifying an SNAT Rule](#). In the EIP list, select the new EIP and deselect the existing EIP.
3. Modify a DNAT rule.

For details, see [Modifying a DNAT Rule](#).
4. Release the EIP that was replaced. For details, see [4](#).

 NOTE

If an unbound EIP is no longer required, you can release it. If you do not release an unbound EIP, it will continue to be billed.

3.3 Can I Bind an EIP of an ECS to Another ECS?

Yes.

You can unbind the EIP from the original ECS. For details, see [Unbinding an EIP from an Instance](#).

Then, bind the EIP to the target ECS. For details, see [Binding an EIP to an Instance](#) section "Assigning an EIP and Binding It to an ECS" in *Elastic IP User Guide*.

If you want to change an EIP for your ECS, refer to [Changing an EIP](#).

3.4 Can I Bind an EIP to a Cloud Resource in Another Region?

An EIP cannot be bound to a cloud resource in another region.

The EIP and the cloud resource must be in the same region.

For example, EIPs in CN-Hong Kong cannot be bound to the cloud resources in AP-Singapore.

3.5 Can Multiple EIPs Be Bound to an ECS?

Scenarios

Multiple EIPs can be bound to an ECS, but this operation is not recommended.

If an ECS has multiple NICs attached and you want to bind multiple EIPs to this ECS, you need to configure policy-based routes for these NICs so that these extension NICs can communicate with external works.

Operation Guide

This document describes how to configure policy-based routes for Linux and Windows ECSs. For details, see [Table 3-1](#).

Table 3-1 Operation instructions

OS Type	IP Address Version	Procedure
Linux	IPv4	Take an ECS running CentOS 8.0 (64-bit) as an example. Configuring Policy-based Routes for a Linux ECS with Multiple NICs (IPv4/IPv6)
	IPv6	
Windows	IPv4	Take an ECS running Windows Server 2012 (64-bit) as an example. Configuring Policy-based Routes for a Windows ECS with Multiple NICs (IPv4/IPv6)
	IPv6	

3.6 What Are the Differences Between Unbinding and Releasing an EIP?

[Table 3-2](#) lists the differences between unbinding and releasing an EIP.

Table 3-2 Differences

Item	Unbinding an EIP	Release an EIP
Application scenarios	<ul style="list-style-type: none">Your instance no longer requires the EIP.You want to bind the EIP to another instance.	If an EIP is no longer required, you can unbind it from your instance and then release it.
Pay-per-use EIP billing	<ul style="list-style-type: none">Billed by bandwidth: Both the EIP and its bandwidth will be billed.Billed by traffic: Only the EIP will be billed.Billed by shared bandwidth: Both the EIP and shared bandwidth will be billed.	<ul style="list-style-type: none">Billed by bandwidth: Both the EIP and its bandwidth will not be billed.Billed by traffic: Both the EIP and traffic will not be billed.Billed by shared bandwidth: The EIP will not be billed. After the shared bandwidth is deleted, it will no longer be billed.

 **NOTE**

Yearly/Monthly EIPs are billed based on your required duration. No operations on the EIP will affect its billing.

4 Bandwidth

4.1 What Bandwidth Types Are Available?

There are dedicated or shared bandwidths.

If an EIP is not added to a shared bandwidth, the EIP uses the dedicated bandwidth no matter how it is billed.

- Dedicated bandwidths can be used by only one EIP.
- Shared bandwidths can be used by multiple EIPs.

4.2 How Many EIPs Can I Add to Each Shared Bandwidth?

A shared bandwidth can be used by multiple EIPs.

By default, you can add a maximum of 20 EIPs to a shared bandwidth.

If the current quota cannot meet service requirements, [submit a service ticket](#) to increase the quota.

4.3 What Are the Differences Between a Dedicated Bandwidth and a Shared Bandwidth?

A dedicated bandwidth can only be used by one EIP that is bound to one cloud resource, such as an ECS, a NAT gateway, or a load balancer.

A shared bandwidth can be shared by multiple pay-per-use EIPs. Adding an EIP to or removing an EIP from a shared bandwidth does not affect your services.

A dedicated bandwidth cannot be changed to a shared bandwidth or the other way around. You can purchase a shared bandwidth for your pay-per-use EIPs.

- After you add an EIP to a shared bandwidth, the EIP will use the shared bandwidth.

- After you remove an EIP from a shared bandwidth, the EIP will use the dedicated bandwidth.

4.4 What Are Inbound Bandwidth and Outbound Bandwidth?

Bandwidth refers to the maximum amount of data that can be transmitted in a given amount of time (generally one second). A larger bandwidth value indicates a stronger transmission capability. Bandwidth is classified into public bandwidth and private bandwidth.

Public bandwidth is the bandwidth consumed when data is transferred between Huawei Cloud instances and the Internet. Public bandwidth is classified into inbound bandwidth and outbound bandwidth. For details the outbound bandwidth and inbound bandwidth, see [Table 4-1](#).

Figure 4-1 Inbound bandwidth and outbound bandwidth

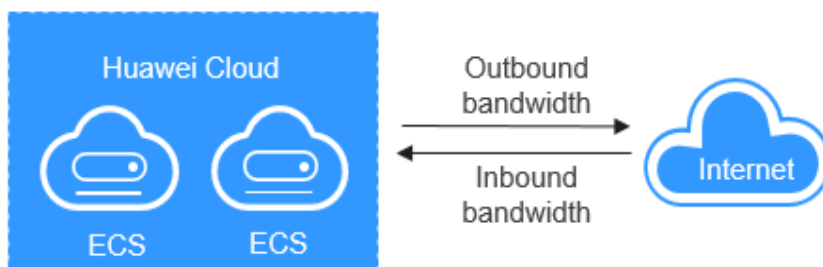


Table 4-1 Inbound bandwidth and outbound bandwidth

Type	Description
Outbound bandwidth	<p>Bandwidth consumed when data is transferred from Huawei Cloud to the Internet. For example, the outbound bandwidth is used when ECSs provide services accessible from the Internet and FTP clients download resources from the ECSs. Outbound bandwidth means the same thing as upstream bandwidth on the Cloud Eye console.</p> <p>Huawei Cloud only charges for the outbound bandwidth.</p> <p>NOTE</p> <ul style="list-style-type: none">• To view the bandwidth usage, see Viewing Metrics.• To view bandwidth billing details, see Bills.

Type	Description
Inbound bandwidth	<p>Bandwidth consumed when data is transferred from the Internet to Huawei Cloud. For example, the inbound bandwidth is used when resources are downloaded from the Internet to ECSs and FTP clients upload resources to the ECSs. Inbound bandwidth means the same thing as downstream bandwidth on the Cloud Eye console.</p> <p>The maximum inbound bandwidth depends on the size of the outbound bandwidth.</p> <ul style="list-style-type: none">• If your purchased bandwidth is less than or equal to 10 Mbit/s, the inbound bandwidth will be 10 Mbit/s, and the outbound bandwidth will be the same as the purchased bandwidth.• If your purchased bandwidth is greater than 10 Mbit/s, the outbound and inbound bandwidth will be the same as the purchased bandwidth. <p>The preceding bandwidth limit is not applicable in CN North-Beijing1 and CN East-Shanghai2.</p>

4.5 How Do I Know If My EIP Bandwidth Limit Has Been Exceeded?

Symptom

The bandwidth size configured when you buy a dedicated or shared bandwidth defines the maximum amount of outbound bandwidth supported. If an ECS running your web applications cannot be accessed smoothly from the Internet, check whether the bandwidth of the EIP bound to the ECS is greater than the configured bandwidth size.

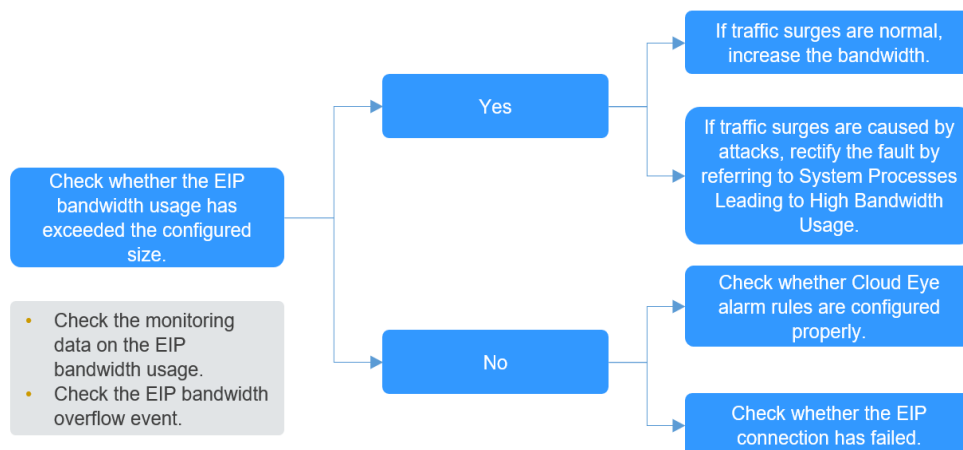
NOTE

If the bandwidth exceeds the configured bandwidth size, there may be packet loss or remote login to an ECS may fail. To prevent data loss, it is recommended that you monitor the bandwidth.

Troubleshooting

Troubleshoot the issue by following the procedure described below. If the problem persists, [submit a service ticket](#).

Figure 4-2 Troubleshooting procedure



Step 1 Check whether the EIP bandwidth usage has exceeded the configured size.

1. Check the monitoring data on the EIP bandwidth usage.
Check whether the inbound bandwidth and outbound bandwidth usage have exceeded the amount purchased. For details, see [Exporting Monitoring Data](#).
2. Check **EIP bandwidth overflow** event.
For details about how to check the event, see [a](#).

If you have not configured EIP bandwidth overflow events, configure one by referring to [solution 2](#). If there is packet loss or access delay, you can view **EIP bandwidth overflow** event on the **Event Monitoring** page.

If the bandwidth usage goes too high for a little while but it does not interrupt your services, ignore the problem. If the bandwidth usage goes too high many times or if the issue lasts for a long time, fix the problem as described in [Step 2](#).

Step 2 Fix the excessive bandwidth usage issue.

Traffic surges may cause the bandwidth to go beyond of the configured limit, causing packet loss.

Check whether the sudden increase in bandwidth is normal.

1. If it is normal, [increase the bandwidth](#).
2. If it is not normal, for example, the sudden increase in bandwidth was caused by online attacks, rectify the fault by referring to [System Processes Leading to High Bandwidth Usage](#).

Step 3 Check the alarm rule settings and EIP connectivity if the bandwidth usage has not exceeded the configured limit.

After doing the checks in [Step 1](#), if the bandwidth usage has not exceeded the configured limit or the purchased bandwidth:

- Check whether Cloud Eye alarm rules are configured properly.
If there are alarm rules for bandwidth usage on the Cloud Eye console, where the outbound bandwidth limit or the alarm period is set too small, the system may generate excessive alarms. You can refer to [Improper Cloud Eye Alarm Rules](#) to fix the problem.

- Check whether the EIP connection has failed.
If an ECS with an EIP bound cannot access the Internet, you can refer to [Why Can't My ECS Access the Internet Even After an EIP Is Bound?](#)

----End

System Processes Leading to High Bandwidth Usage

If some heavy-duty system processes or applications running on your ECS are causing the high bandwidth or CPU usage, your ECS will run slowly or may unexpectedly be inaccessible.

You can refer to the following to locate processes that have led to excessively high bandwidth or CPU usage, and optimize or stop the processes.

- [Why Is My Windows ECS Running Slowly?](#)
- [Why Is My Linux ECS Running Slowly?](#)

Improper Cloud Eye Alarm Rules

If there are alarm rules for bandwidth usage on the Cloud Eye console, where the outbound bandwidth limit or the alarm period is set too small, the system may generate excessive alarms.

- Solution 1: Create a more appropriate bandwidth alarm rule.
If there are alarm rules for bandwidth usage on the Cloud Eye console, where the outbound bandwidth limit or the alarm period is set too small, the system may generate excessive alarms. You need to set an appropriate alarm rule based on your purchased bandwidth. For example, if your purchased bandwidth is 5 Mbit/s, you can create an alarm rule to report an alarm if the outbound bandwidth reaches 4.8 Mbit/s for three consecutive periods. To create an alarm rule:
 - a. Log in to the management console, under **Management & Governance**, click **Cloud Eye**. On the **Cloud Eye** console, choose **Alarm Management > Alarm Rules**.
 - b. Click **Create Alarm Rule** and configure an alarm rule to generate alarms when the bandwidth usage exceeds the configured limit.
- Solution 2: Configure **EIP bandwidth overflow** events.

NOTE

The **Event Monitoring** page only displays EIP status. It does not display the shared bandwidth limit.

To configure **EIP bandwidth overflow** events:

- a. Log in to the management console, under **Management & Governance**, click **Cloud Eye**. On the **Cloud Eye** console, choose **Event Monitoring**.
- b. Click **Create Alarm Rule** and configure an alarm rule to generate alarms when the EIP bandwidth usage exceeds the limit.

After the configuration, you can view the usage details of the EIP dedicated bandwidth on the **Event Monitoring** page when there are packet loss or data transfer delays.

To check the EIP bandwidth overflow history, perform the following steps:

- a. On the **Cloud Eye** console, click **Event Monitoring**.
- b. On the **Event Monitoring** page, locate the target monitoring event and click **View Graph** in the **Operation** column.
- c. On the system event list page, locate the target monitored object and click **View Event** in the **Operation** column to view the bandwidth overflow details.

If the event **EIP bandwidth overflow** is not displayed, the usage of the dedicated EIP bandwidth did not exceed the preset limit.

If the event **EIP bandwidth overflow** is displayed, the usage of the dedicated EIP bandwidth exceeded the limit. To ensure stability and high availability of your workload, **you can increase your bandwidth**.

You will not be billed for Cloud Eye alarms, but if you enable SMN to send out alarm notifications, this will incur charges. For details, see the [Cloud Eye User Guide](#).

Submitting a Service Ticket

If the problem persists, [submit a service ticket](#).

4.6 What Are the Differences Between Public Bandwidth and Private Bandwidth?

Public Bandwidth

Public bandwidth is the bandwidth consumed when data is transferred between Huawei Cloud instances and the Internet. You can configure the public bandwidth when creating an ECS or bind an EIP to an ECS after the ECS is created.

Public bandwidth is classified into inbound bandwidth and outbound bandwidth.

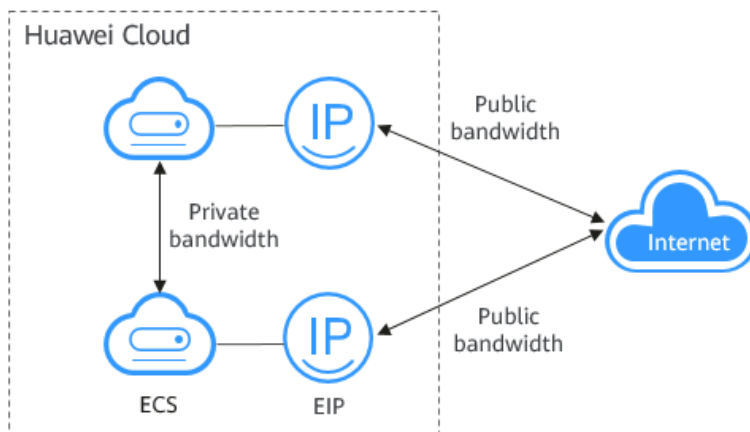
Inbound bandwidth is the bandwidth consumed when data is transferred from the Internet to Huawei Cloud. For example, when resources are downloaded from the Internet to ECSs, that consumes inbound bandwidth.

Outbound bandwidth is the bandwidth consumed when data is transferred from Huawei Cloud to the Internet. For example, when ECSs provide services accessible from the Internet and external users download resources from the ECSs, this consumes outbound bandwidth.

Private Bandwidth

Private bandwidth is the bandwidth consumed when data is transferred between ECSs in the same region and on the same private network. ECSs can also be connected to cloud databases, load balancers, and OBS through private bandwidth. The private bandwidth size depends on the instance specifications.

For details, see [ECS Types](#).

Figure 4-3 Public bandwidth and private bandwidth

4.7 Can I Increase Then Decrease a Yearly/Monthly Bandwidth?

The bandwidth can be decreased after it is increased.

For details about how to adjust the bandwidth, see [Modifying an EIP Bandwidth](#).

- Increasing the bandwidth: The change is applied immediately.
You need to pay the price difference.
- Decreasing the bandwidth: The change is not applied immediately.
You need to select a new bandwidth size and a renewal duration. The change will be applied in the first billing cycle after a successful renewal.

4.8 What Is the Relationship Between Bandwidth and Upload/Download Rate?

The bandwidth is measured in bit/s, indicating the number of binary bits transmitted per second. The download rate is measured in byte/s, indicating the number of bytes transmitted per second.

1 byte = 8 bits, that is, download rate = bandwidth/8

Due to various issues such as computer performance, network device quality, resource usage, and network peak hours, if the bandwidth is 1 Mbit/s, the actual upload or download rate is generally lower than 125 kByte/s (1 Mbit/s = 1,000 Kbit/s, upload or download rate = 1,000/8 = 125 kByte/s).

4.9 What Are the Differences Among Static BGP, Dynamic BGP, and Premium BGP?

Border Gateway Protocol (BGP) is a routing protocol used between autonomous systems (ASs). BGP is the only protocol that can process many connections

between unrelated routing domains. The EIP service connects to networks provided by China Unicom, China Telecom, China Mobile, and other carriers.

When assigning an EIP, you can select from the following EIP types:

- Static BGP routes are manually configured by network carriers.
- Dynamic BGP provides automatic failover and chooses the optimal path when a network connection fails.
- Premium BGP chooses the optimal path and ensures low-latency and high-quality networks. BGP is used to interconnect with lines of multiple mainstream carriers. Public network connections that feature low latency and high quality are directly established between the Chinese mainland and Hong Kong (China). (Premium BGP is available only in **CN-Hong Kong**.)

For details about static BGP, dynamic BGP, and premium BGP and their differences, see [Table 4-2](#).

Table 4-2 Differences among static BGP, dynamic BGP, and premium BGP

Item	Static BGP	Dynamic BGP	Premium BGP
Definition	Static routes are manually configured and must be manually reconfigured anytime when the network topology or link status changes.	Dynamic BGP provides automatic failover and chooses the optimal path based on the real-time network conditions as well as preset policies.	Premium BGP chooses the optimal path and ensures low-latency and high-quality networks. BGP is used to interconnect with lines of multiple mainstream carriers. Public network connections that feature low latency and high quality are directly established between Chinese mainland and Hong Kong (China).

Item	Static BGP	Dynamic BGP	Premium BGP
Assurance	<p>When changes occur on a network that uses static BGP, the manual configuration takes some time and high availability cannot be guaranteed.</p> <p>If you select static BGP, your application system must have disaster recovery setups in place.</p>	<p>When a fault occurs on a carrier's link, dynamic BGP will quickly select another optimal path to take over services, ensuring service availability.</p> <p>Currently, carriers in China that support dynamic BGP routing include China Telecom, China Mobile, China Unicom, China Education and Research Network (CERNET), National Radio and Television Administration, and Dr. Peng Group.</p>	<p>Premium BGP has the same assurance capability as that of dynamic BGP.</p> <p>In addition, premium BGP ensures higher network quality and lower latency.</p> <p>Currently, mainstream carriers in Hong Kong (China) are supported.</p>
Advantages	<p>This is a more cost-effective option that allows resources to access the Internet over a single carrier network. The routes can be manually configured.</p>	<p>The BGP public network egress supports switchover across domains within seconds, providing your users with high-speed and secure networks.</p>	<ul style="list-style-type: none"> • Premium BGP chooses the optimal path for access from the abroad. • It allows users in the Chinese mainland to access cross-border applications faster.
Service availability	99%	99.95%	99.95%
Billing	<p>Their price from least to most expensive: static BGP, dynamic BGP, and premium BGP. For details, see EIP Pricing Details.</p>		

 **NOTE**

For more information about service availability, see [Huawei Cloud Service Level Agreement](#).

5 Connectivity

5.1 What Are the Priorities of the Custom Route and EIP If Both Are Configured for an ECS to Enable the ECS to Access the Internet?

The priority of an EIP is higher than that of a custom route in a VPC route table. For example:

The VPC route table of an ECS has a custom route with 0.0.0.0/0 as the destination and NAT gateway as the next hop.

If an ECS in the VPC has an EIP bound, the VPC route table will have a policy-based route with 0.0.0.0/0 as the destination, which has a higher priority than its custom route. In this case, traffic is forwarded to the EIP and cannot reach the NAT gateway.

5.2 Why Can't My ECS Access the Internet Even After an EIP Is Bound?

Symptom

An ECS with an EIP bound cannot access the Internet.

Troubleshooting

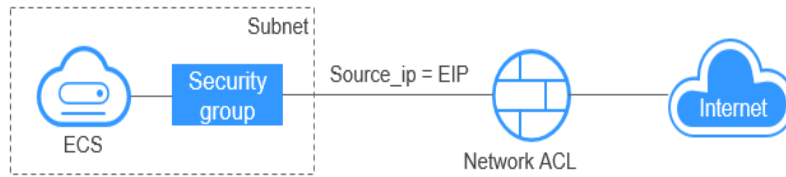
Checking Whether EIPs Are Blocked or Frozen

- Check whether the EIP is blocked. For details, see [How Do I Unblock an EIP?](#)
- Check whether the EIP is frozen. For details, see [Why My EIPs Are Frozen? How Do I Unfreeze My EIPs?](#)

Checking EIP Connectivity

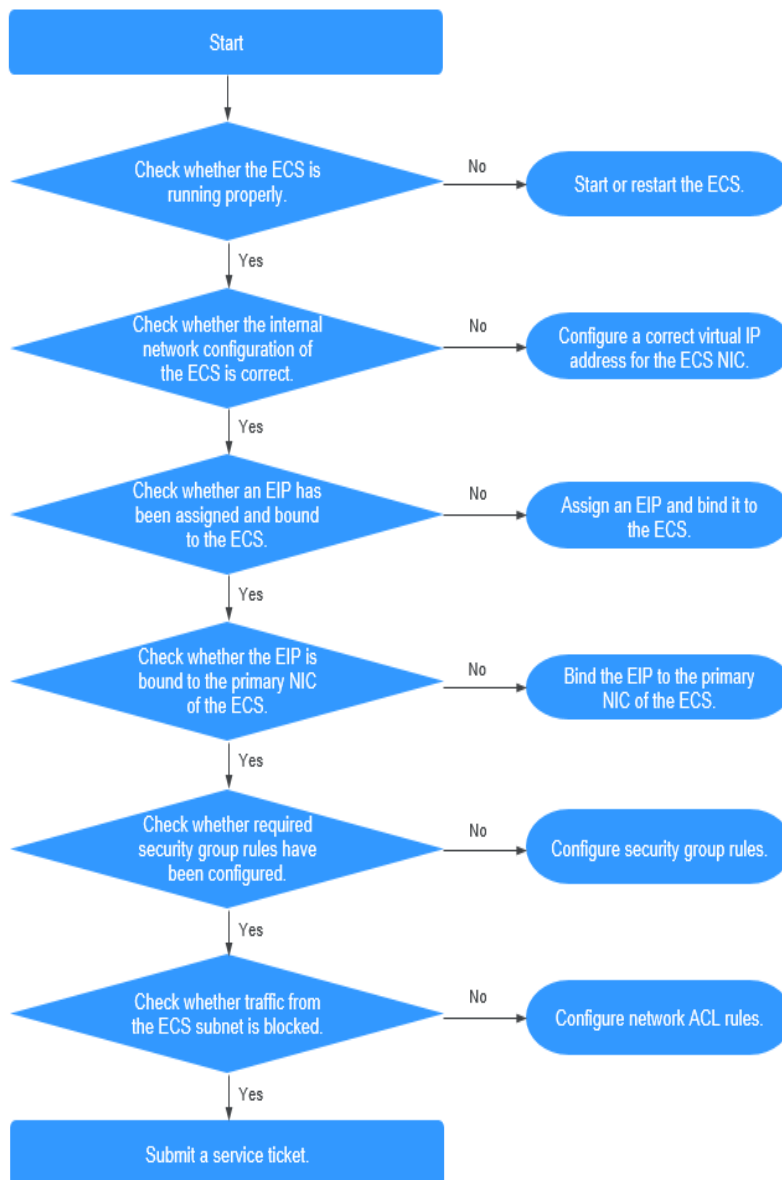
Figure 5-1 shows the networking diagram for an ECS to access the Internet using an EIP.

Figure 5-1 EIP network diagram



Locate the fault based on the following procedure.

Figure 5-2 Troubleshooting procedure



1. **Step 1: Check Whether the ECSs Is Running Properly**
2. **Step 2: Check Whether the Network Configuration of the ECSs Is Correct**
3. **Step 3: Check Whether an EIP Has Been Assigned and Bound to the ECSs**

4. [Step 4: Check Whether an EIP Is Bound to the Primary NIC of the ECSs](#)
5. [Step 5: Check Whether Required Security Group Rules Have Been Configured.](#)
6. [Step 6: Check Whether Traffic from the ECSs Subnet Is Blocked](#)

Step 1: Check Whether the ECSs Is Running Properly

Check the ECSs status.

If the ECSs status is not **Running**, start or restart the ECSs.

Figure 5-3 ECS status

Name/ID	Monit...	Se...	Status	AZ	Specifications/Image	OS Type	IP Address	Billing Mode	Enterprise Pr...
697 49b...			Stopped Locked...	AZ3	2 vCPUs 4 GiB I6.large.2 CCE_Images_HCE20-Node-2...	Linux	99 (Privat...	Pay-per-use Created on Apr 11, 2024...	default
822 4ece-b...			Stopped Locked...	AZ1	2 vCPUs 4 GiB s7.large.2 CCE_Images_HCE20-Node-2...	Linux	30 (Privat...	Pay-per-use Created on Apr 11, 2024...	default
388 496d...			Stopped Locked...	AZ3	4 vCPUs 8 GiB I6.xlarge.2 CCE_Images_HCE20-Node-2...	Linux	46 (EIP)... 8 (Private...	Pay-per-use Created on Apr 10, 2024...	default
c... 42c1...			Running	AZ4	2 vCPUs 4 GiB c7.large.2 CentOS 7.8 64bit	Linux	4 (Private...	Pay-per-use Created on Jan 22, 2024...	default

Step 2: Check Whether the Network Configuration of the ECSs Is Correct

1. Check whether the ECSs NIC has an IP address assigned.

Log in to the ECSs, and run **ifconfig** or **ip address** to check the ECS NIC IP address.

If both the primary and extension NICs of an ECS have an EIP bound, check whether the ECS has policy-based routes configured. If policy-based routes are not configured, refer to [Configuring Policy-based Routes for a Linux ECS with Multiple NICs \(IPv4/IPv6\)](#).

If the ECSs runs Windows, run **ipconfig**.

2. Check whether the ECS NIC has a virtual IP address.

Log in to the ECSs, and run **ifconfig** or **ip address** to check whether the ECSs NIC has a virtual IP address. If the ECSs NIC has no virtual IP address, run the **ip addr add virtual IP address eth0** command to configure an IP address for the ECSs NIC.

Figure 5-4 Virtual IP address of a NIC

```
[root@demoserver ~]# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether fa:16:3e:37:7b:62 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.30/24 brd 192.168.1.255 scope global dynamic eth0
        valid_lft 84950sec preferred_lft 84950sec
    inet 192.168.1.192/24 scope global secondary eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::f816:3eff:fe37:7b62/64 scope link
        valid_lft forever preferred_lft forever
```

Check whether the ECS NIC has a default route. If there is no default route, run **ip route add** to add one.

Figure 5-5 Default route

```
192.168.1.0/24 dev eth0 proto kernel scope link src 192.168.1.200
192.168.1.0/24 dev eth1 proto kernel scope link src 192.168.1.179
169.254.0.0/16 dev eth0 scope link metric 1002
default via 192.168.1.1 dev eth0 proto static
-bash-4.1#
```

Step 3: Check Whether an EIP Has Been Assigned and Bound to the ECSs

Check whether an EIP has been assigned and bound to the ECSs. If no EIP has been assigned, assign an EIP and bind it to the ECSs.

The ECS shown in [Figure 5-6](#) has no EIP bound. It only has a private IP address bound.

Figure 5-6 EIP status

Name/ID	Monito...	Sec...	Status	AZ	Specifications/Image	OS Type	IP Address
ecs- b3b97			Running	AZ3	1 vCPU 2 GiB s6.medium.2 CentOS 7.5 64bit	Linux	192.168. (Private IP)

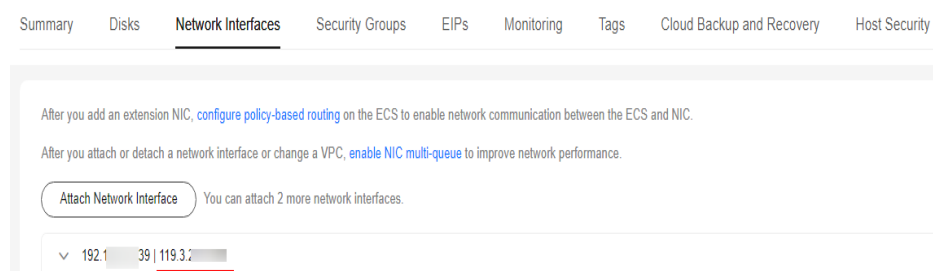
Step 4: Check Whether an EIP Is Bound to the Primary NIC of the ECSs

Check whether an EIP is bound to the primary NIC of the ECSs. If there is no EIP bound to the primary NIC of the ECSs, bind one.

You can view the NIC details by clicking the **NICs** tab on the ECSs details page. By default, the first record in the list is the primary NIC.

As shown in the following figure, the EIP is bound to the primary NIC.

Figure 5-7 Checking whether the EIP is bound to the primary NIC of the ECS



Step 5: Check Whether Required Security Group Rules Have Been Configured.

For details about how to add security group rules, see [Adding a Security Group Rule](#).

If security group rules have not been configured, configure them based on your service requirements. (The remote IP address indicates the allowed IP address, and **0.0.0.0/0** indicates that all IP addresses are allowed.)

Step 6: Check Whether Traffic from the ECSs Subnet Is Blocked

Check whether the network ACL of the NIC subnet blocks certain traffic from the subnet.

You can configure the network ACL on the VPC console. Make sure that the network ACL rules allow the traffic from the ECSs subnet.

Submitting a Service Ticket

If the EIP still cannot communicate with the Internet after you perform all the steps above, [submit a service ticket](#).

Provide the following information to technical support.

Item	Description	Example	Value
VPC CIDR block	Required for gateway configuration	Example: 10.0.0.0/16	N/A
VPC ID	N/A	Example: 120b71c7-94ac-45b8-8e d6-30aafc8fbdba	N/A
CIDR block of subnet 1 (can be the same as the VPC CIDR block)	N/A	Example: 10.0.1.0/24	N/A
ECS ID	N/A	N/A	N/A
ECS IP address	N/A	Example: 192.168.1.192/24	N/A
ECS route information	N/A	N/A	N/A
EIP	Required for the ECS to access the Internet	Example: 10.154.55.175	N/A
EIP bandwidth	Maximum bandwidth size used by the ECS to access the Internet	Example: 1 Mbit/s	N/A
EIP ID	N/A	Example: b556c80e-6345-4003- b512-4e6086abbd48	N/A

5.3 What Should I Do If an EIP Cannot Be Pinged?

Symptom

After you purchase an EIP and bind it to an ECS, the local host or other cloud servers cannot ping the EIP of the ECS.

Fault Locating

Checking EIPs

- Check whether the EIP is blocked. For details, see [How Do I Unblock an EIP?](#)
- Check whether the EIP is frozen. For details, [Why My EIPs Are Frozen? How Do I Unfreeze My EIPs?](#)

Checking EIP Connectivity

The following fault causes are sequenced based on their occurrence probability. If the fault persists after you have ruled out a cause, check other causes.

Figure 5-8 Method of locating the failure to ping an EIP

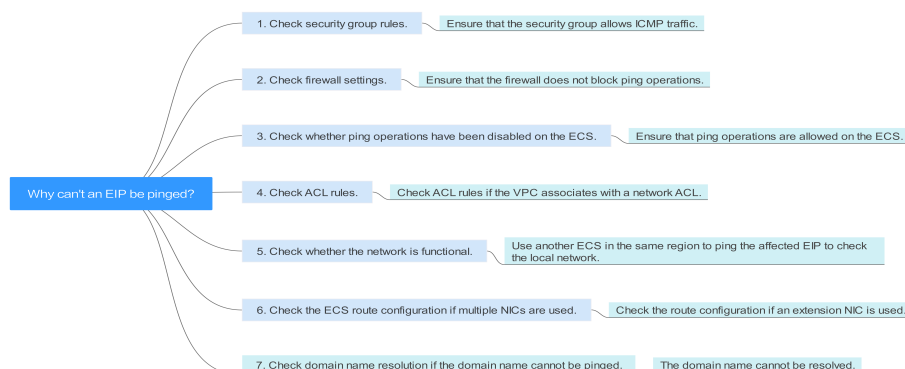


Table 5-1 Method of locating the failure to ping an EIP

Possible Cause	Solution
ICMP access rules are not added to the security group.	Add ICMP access rules to the security group. For details, see Checking Security Group Rules .
Ping operations are prohibited on the firewall.	Allow ping operations on the firewall. For details, see Checking Firewall Settings .
Ping operations are prohibited on the ECS.	Allow ping operations on the ECS. For details, see Checking Whether Ping Operations Have Been Disabled on the ECS .
Network ACL is associated.	If the VPC is associated with a network ACL, check the network ACL rules. For details, see Checking ACL Rules .
A network exception occurred.	Use another ECS in the same region to check whether the local network is functional. For details, see Checking Whether the Network Is Functional .

Possible Cause	Solution
Routes are incorrectly configured if multiple NICs are used.	If the network is inaccessible due to an extension NIC, the fault is generally caused by incorrect route configurations. To resolve this issue, see Checking the ECS Route Configuration If Multiple NICs Are Used .
The domain name is not ICP licensed.	If the domain name cannot be pinged or cannot be resolved, see Checking Domain Name Resolution If the Domain Name Cannot Be Pinged to resolve this issue.

Checking Security Group Rules

ICMP is used for the ping command. Check whether the security group accommodating the ECS allows ICMP traffic.


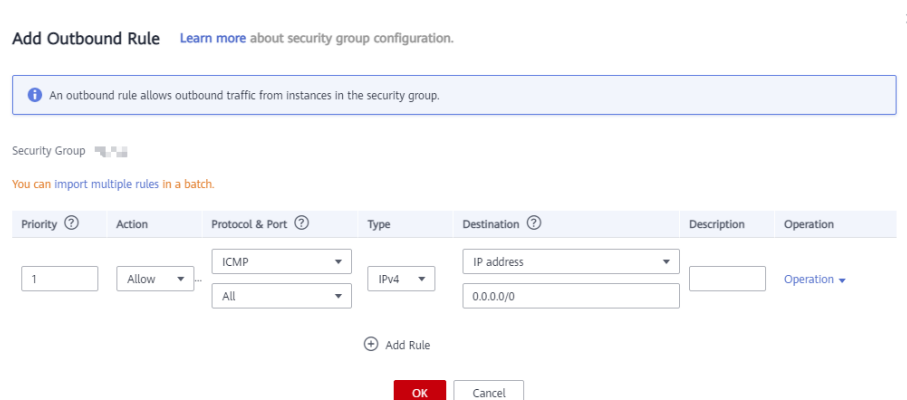

1. Log in to the management console.
2. Click  in the upper left corner and select your region and project.
3. Under **Compute**, click **Elastic Cloud Server**.
4. On the **Elastic Cloud Server** page, click the name of the target ECS.
The page providing details about the ECS is displayed.
5. Click the **Security Groups** tab, expand the information of the security group, and view security group rules.
6. Click the security group ID.
The system automatically switches to the **Security Group** page.
7. On the **Outbound Rules** page, click **Add Rule**. In the displayed dialog box, set required parameters to add an outbound rule.

Figure 5-9 Adding an outbound rule



Add Outbound Rule [Learn more about security group configuration.](#) ×

i An outbound rule allows outbound traffic from instances in the security group.

Security Group 

You can [import multiple rules in a batch.](#)

Priority ?	Action	Protocol & Port ?	Type	Destination ?	Description	Operation
1	Allow	ICMP All	IPv4	IP address 0.0.0.0/0		Operation

+ Add Rule

OK Cancel

Table 5-2 Security group rules

Transfer Direction	Type	Protocol/Port Range	Source
Outbound	IPv4	ICMP/Any	0.0.0.0/0 0.0.0.0/0 indicates all IP addresses.

- On the **Inbound Rules** tab, click **Add Rule**. In the displayed dialog box, set required parameters to add an inbound rule.

Figure 5-10 Adding an inbound rule

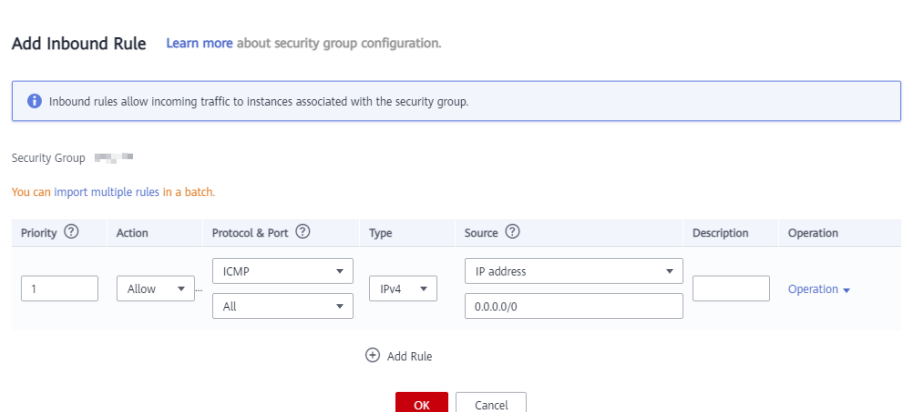


Table 5-3 Security group rules

Transfer Direction	Type	Protocol/Port Range	Source
Inbound	IPv4	ICMP/Any	0.0.0.0/0 0.0.0.0/0 indicates all IP addresses.

- Click **OK** to complete the security rule configuration.

Checking Firewall Settings

If a firewall is enabled on the ECS, check whether the firewall blocks the ping operations.

Linux

- Consider CentOS 7 as an example. Run the following command to check the firewall status:

firewall-cmd --state

If **running** is displayed in the command output, the firewall has been enabled.

- Check whether there is any ICMP rule blocking the ping operations.

iptables -L

If the command output shown in [Figure 5-11](#) is displayed, there is no ICMP rule blocking the ping operations.

Figure 5-11 Checking firewall rules

```
[root@ecs-3c4e ~]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination
ACCEPT    icmp -- anywhere             anywhere             icmp echo-request

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
ACCEPT    icmp -- anywhere             anywhere             icmp echo-reply
[root@ecs-3c4e ~]#
```

If the ping operations are blocked by an ICMP rule, run the following commands to modify the rule for unblocking:

```
iptables -A INPUT -p icmp --icmp-type echo-request -j ACCEPT
```

```
iptables -A OUTPUT -p icmp --icmp-type echo-reply -j ACCEPT
```

Windows

1. Log in to the Windows ECS, click the Windows icon in the lower left corner of the desktop, and choose **Control Panel > Windows Firewall**.
2. Click **Turn Windows Firewall on or off**.
View and set the firewall status.
3. If the firewall is **On**, go to [4](#).
4. Check the ICMP rule statuses in the firewall.
 - a. In the navigation pane on the **Windows Firewall** page, click **Advanced settings**.
 - b. Enable the following rules:
Inbound Rules: File and Printer Sharing (Echo Request - ICMPv4-In)
Outbound Rules: File and Printer Sharing (Echo Request - ICMPv4-Out)
If IPv6 is enabled, enable the following rules:
Inbound Rules: File and Printer Sharing (Echo Request - ICMPv6-In)
Outbound Rules: File and Printer Sharing (Echo Request - ICMPv6-Out)

Figure 5-12 Inbound Rules

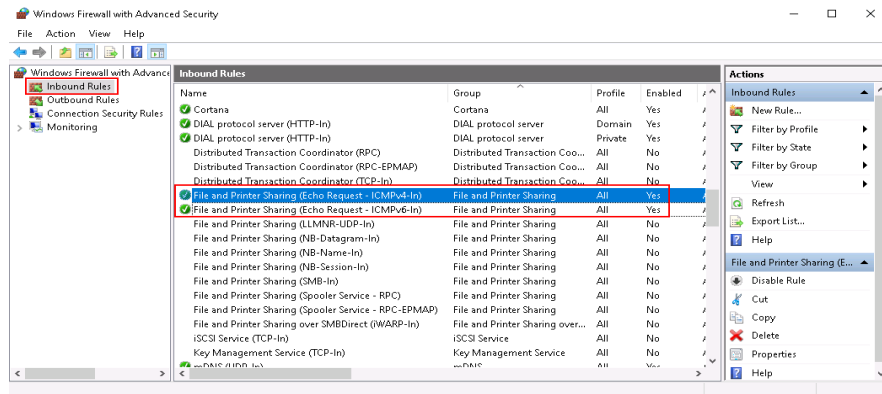
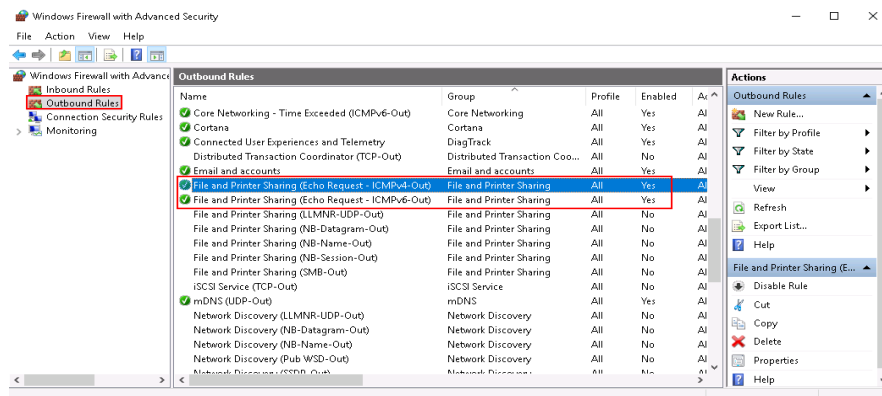


Figure 5-13 Outbound Rules



Checking Whether Ping Operations Have Been Disabled on the ECS

Windows

Enable ping operations using the CLI.

1. Start the **Run** dialog box. Enter **cmd** and press **Enter**.
2. Run the following command to enable ping operations:
netsh firewall set icmpsetting 8

Linux

Check the ECS kernel parameters.

1. Check the **net.ipv4.icmp_echo_ignore_all** value in the **/etc/sysctl.conf** file. Value **0** indicates that ping operations are allowed, and value **1** indicates that ping operations are prohibited.
2. Allow ping operations.
 - Run the following command to temporarily allow the ping operations:
#echo 0 >/proc/sys/net/ipv4/icmp_echo_ignore_all
 - Run the following command to permanently allow the ping operations:
net.ipv4.icmp_echo_ignore_all=0

Checking ACL Rules

By default, no ACL is configured for a VPC. If a network ACL is associated with a VPC, check the ACL rules.

1. Check whether the subnet of the ECS has been associated with a network ACL.

If an ACL name is displayed, the network ACL has been associated with the ECS.

Figure 5-14 Network ACL

Name	VPC	IPv4 CIDR ...	IPv6 CID...	St...	AZ...	Network ACL	Route Table
subnet-b981...	vpc-b945	192.168.0.0/24	-- ...	Av...	AZ1	fw-51ce	rtb-vpc-b945 Default

2. Click the ACL name to view its status.

Figure 5-15 Enabled network ACL

Name	fw-51ce	Status	Enabled
ID	02a3469d-db57-4797-8bea-e2e3e81e4e7e	Description	--

3. If the network ACL is enabled, add an ICMP rule to allow traffic.

Figure 5-16 Adding an ICMP rule

Priority	Status	Type	Action	Protocol	Source	Source Port Range	Destination
1	Enabled	IPv4	Allow	All	0.0.0.0/0	All	0.0.0.0/0
2	Enabled	IPv4	Allow	ICMP	0.0.0.0/0	All	0.0.0.0/0
*	Enabled	--	Deny	All	0.0.0.0/0	All	0.0.0.0/0

NOTE

The default network ACL rule denies all incoming and outgoing packets. If a network ACL is disabled, the default rule is still effective.

Checking Whether the Network Is Functional

1. Use another ECS in the same region to check whether the local network is functional.

Use another ECS in the same region to ping the affected EIP. If the EIP can be pinged, the VPC is functional. In such a case, rectify the local network fault and ping the affected EIP again.

2. Check whether the link is accessible.

A ping failure is caused by packet loss or long delay, which may be caused by link congestion, link node faults, or heavy load on the ECS.

For details, see [How Do I Troubleshoot a Ping Failure or Packet Loss Using a Link Test?](#)

Checking the ECS Route Configuration If Multiple NICs Are Used

Generally, the default route of an OS will preferentially select the primary NIC. If an extension NIC is selected in a route and the network malfunctions, this issue is typically caused by incorrect route configuration.

- If the ECS has multiple NICs, check whether the default route is available.
 - a. Log in to the ECS and run the following command to check whether the default route is available:

ip route

Figure 5-17 Default route

```
[root@do-not-del-scy ~]# ip route
default via 192.168.2.1 dev eth0
169.254.0.0/16 dev eth0 scope link metric 1002
169.254.169.254 via 192.168.2.1 dev eth0 proto static
192.168.2.0/24 dev eth0 proto kernel scope link src 192.168.2.112
```

- b. If the route is unavailable, run the following command to add it:

ip route add default via XXXX dev eth0

NOTE

In the preceding command, *XXXX* specifies a gateway IP address.

- If the ECS has multiple NICs and the EIP is bound to an extension NIC, configure policy routing on the ECS for network communication with the extension NIC.

For details, see [How Do I Configure Policy-Based Routes for an ECS with Multiple NICs?](#)

Checking Domain Name Resolution If the Domain Name Cannot Be Pinged

If you can ping the EIP but not the domain name, the possible cause is that an error occurred in domain name resolution.

1. Check the domain name resolution.

If the domain name records are incorrectly configured, the domain name may fail to be resolved.

Switch to the DNS management console to view details about the domain name resolution.

2. Check the DNS server configuration.

If the system shows no server found after you ping a domain name, this issue may be caused by slow response from the DNS server. In such a case, see [Troubleshooting Slow Access of a Website Outside the Chinese Mainland over an ECS](#).

5.4 How Do I Unblock an EIP?

If the bandwidth of an EIP exceeds the threshold or an attack (usually a DDoS attack) occurs, the EIP will be blocked.

Blocked EIPs will be automatically unblocked 24 hours later if no attack occurs. To unblock the EIPs in advance and prevent attacks, you need to configure [Advanced Anti-DDoS](#).

If the blocked EIP is continuously attacked, assign a new EIP and release the blocked one. For details, see [How Can I Unbind an Existing EIP from an Instance and Bind Another EIP to the Instance?](#)

5.5 Why Is There Network Jitter or Packet Loss During Cross-Border Communications?

If there is network jitter or packet loss during cross-border communications using dynamic BGP EIPs and bandwidths, this is caused by carrier line congestion or switchover and will be restored quickly.

If your communication between Hong Kong (China) and Chinese Mainland requires low-latency and high-quality public networks, buy premium BGP EIPs and bandwidths in CN-Hong Kong.

If the network jitter or packet loss persists after the preceding steps are performed, submit a service ticket. For details about how to submit a service ticket, see [Submitting a Service Ticket](#).

5.6 Why Does the Download Speed of My ECS Is Slow?

If the download speed of an ECS is slow, check the following:

- Bandwidth limit exceeded: Your used bandwidth exceeds its limit and the limiting policy of the bandwidth takes effect, causing packet loss and slowing down the access. You can check the bandwidth usage or increase the bandwidth.

If your service traffic continues to be high, you can increase the bandwidth by referring to [Modifying a Shared Bandwidth](#).

- The memory usage of the ECS is higher than 80%.
For details, see [Why Is My Linux ECS Running Slowly?](#) or [Why Is My Windows ECS Running Slowly?](#)
- Unstable carrier lines: The network between the local server and the cloud is unstable. Contact the carrier to check the network status.

- Unstable cross-border lines: Latency, jitter, or packet loss occasionally occurs due to cross-border line congestion, switchover, or limits on bandwidth going out of China.

For details, see [Why Accessing a Website Outside the Chinese Mainland Is Slow on an ECS?](#) and [Why Is There Network Jitter or Packet Loss During Cross-Border Communications?](#)

You can also use a server outside China to upload files to your mailbox or web disk, and then access your mailbox or web disk in China to download the files to your local server.