# Elastic IP

# FAQs

| | |
|---|---|
| **Issue** | 02 |
| **Date** | 2022-10-30 |

# 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 What Is a Quota?

### 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.

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.

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

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

Different types of IP addresses have different functions.

**Figure 1-1** IP address architecture
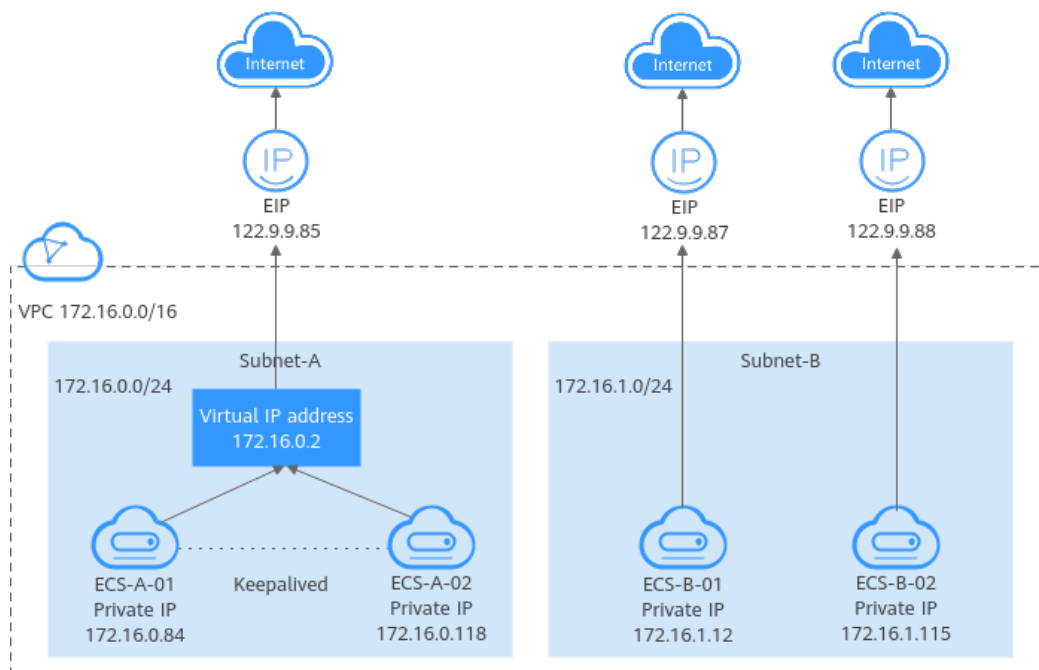
**Table 1-1** Functions of different IP address types

| 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. | • Private IP address of ECS-A-01: 172.16.0.84<br>• Private IP address of ECS-B-01: 172.16.1.12 |
| Virtual IP address | A virtual IP address can be shared among multiple ECSs. Two ECSs can work as an active and standby pair to achieve high availability by using a virtual IP address and Keepalived. If the active ECS is faulty, the virtual IP address can be dynamically switched to the standby ECS to continue providing services.<br><br>For more information about virtual IP addresses, see **Virtual IP Address Overview**. | 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. |
| EIP | EIPs allow cloud resources to access the Internet. They can be flexibly bound to or unbound from instances.<br>• You can bind an EIP to a virtual IP address to enable the ECSs with the virtual IP address bound to access the Internet.<br>• You can also bind an EIP to the ECSs to enable them to access the Internet.<br>For more information, see **EIP Overview**. | • 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.<br>• Bind EIP (122.9.9.87) to ECS-B-01 to enable ECS-B-01 to access the Internet. |

# 1.5 Can an EIP That Uses Dedicated Bandwidth Be Changed to Use Shared Bandwidth?

Yes. An EIP that uses a dedicated bandwidth can be changed to use a shared bandwidth.

# 1.6 Can I Bind an EIP to Multiple ECSs?

Each EIP can be bound to only one ECS at a time.

Multiple ECSs cannot share the same EIP. An ECS and its bound EIP must be in the same region. If you want multiple ECSs in the same VPC to share an EIP, you have to use a NAT gateway. For more information, see **NAT Gateway User Guide**.

# 1.7 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.

# 1.8 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.

# 1.9 Can I Buy a Specific EIP?

By default, EIPs are assigned randomly. If you have released EIPs, the system preferentially assigns EIPs from the ones you released.

You can assign a specific EIP only by calling an API. For details, see **Assigning an EIP**.

# 1.10 Does an EIP Change Over Time?

EIPs will not be changed after they are assigned.

- Stopping and starting an ECS 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.

# 1.11 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**.

# 1.12 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.

# 1.13 How Do I Unbind an EIP from an Instance and Bind a New EIP to the Instance?

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

1. Unbind an EIP.

   a. Log in to the management console.

   b. Click  in the upper left corner and select the desired region and project.

   c. Click  in the upper left corner and choose **Networking** > **Elastic IP**.

   d. On the displayed page, locate the row that contains the target EIP, and click **Unbind**.

   e. 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.

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.

## 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.

# 1.14 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**.

## EIP Not in the Current Region

**Step 1** Log in to the management console.

**Step 2** Locate the EIP.

**----End**

# 1.15 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.

You can change an EIP for an instance by referring to **How Do I Unbind an EIP from an Instance and Bind a New 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 Do I Unbind an EIP from an Instance and Bind a New 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

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 | • An EIP billed on a yearly/monthly basis can be directly changed to be billed on a pay-per-use basis (billed by bandwidth).<br><br>• 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:<br><br>  1. Change the yearly/monthly EIP to be billed by bandwidth on a pay-per-use basis.<br><br>  2. Change the EIP billed by bandwidth on a pay-per-use basis to be billed by traffic on a pay-per-use basis.<br><br>The new billing mode takes effect only after the yearly/monthly subscription expires. |
| From pay-per-use to yearly/monthly | • 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.<br><br>• 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:<br><br>  1. Change the EIP billed by traffic on a pay-per-use basis to be billed by bandwidth on a pay-per-use basis.<br><br>  2. Change the EIP billed by bandwidth on a pay-per-use basis to be billed on a yearly/monthly basis.<br><br>After the change is successful, the new billing mode takes effect immediately. |

**Figure 2-1** EIP billing change
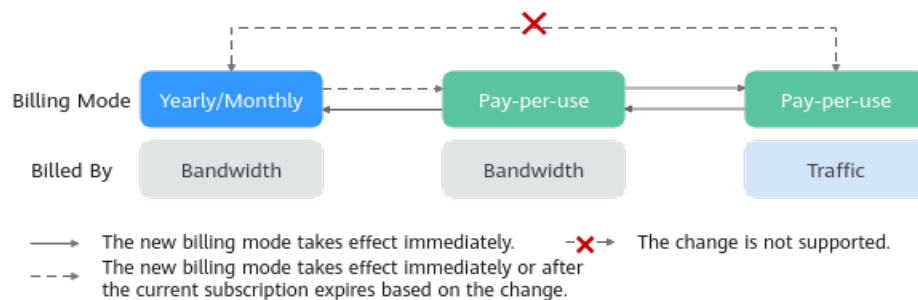


## From Yearly/Monthly to Pay-Per-Use upon Expiration (Billed by Bandwidth)

1. Log in to the management console.

2. In the upper right corner of the page, choose > **Renewal**.

3. In the resource list, search for the EIP whose billing mode needs to be changed.

4. Locate the row that contains the EIP and choose **More** > **Change to Pay-per-Use After Expiration** in the **Operation** column.

5. Confirm the information and click **Change to Pay-per-Use**.

   After the operation is complete, the yearly/monthly EIP is changed to be billed by bandwidth on a pay-per-use basis.

## 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 click **Change Billing Mode** in the **Operation** column.

   – Multiple EIPs:

     Select EIPs and click **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.<br>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.<br>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 What Is Enhanced 95th Percentile Bandwidth Billing?

The enhanced 95th percentile bandwidth billing allows you to use more bandwidth after you pay for the baseline bandwidth. You are billed based on the required duration and the average bandwidth size obtained after discarding some

top bandwidth usages in a billing period. The following uses the shared bandwidth as an example to describe the enhanced 95th percentile bandwidth billing.

## Prerequisite

To use the enhanced 95th percentile billing, the following requirements must be met:

- Your level is greater than or equal to V4.
- The minimum bandwidth you can purchase is 300 Mbit/s.

## Billed Items

The enhanced 95th percentile bandwidth billing allows you to be billed based on the required duration and the average bandwidth size obtained after discarding some top bandwidth usages in a billing period.

## Billed Usage Period

An enhanced 95th percentile bandwidth billing resource is billed for the purchased duration and is settled by month.

## Pricing Details

**Billing formula**: Monthly peak bandwidth x Monthly peak bandwidth price x Shared bandwidth in-use days/Calendar days of the month

**Billing cycle**: Bills are generated for each calendar month.

**Billing mode**: The enhanced 95th percentile bandwidth billing is pay-per-use and does not require prepayment. The monthly fee is settled at the end of each calendar month.

**Table 2-3** Enhanced 95th percentile billing

| Item | Description | Example Value |
|---|---|---|
| Monthly peak bandwidth | The larger value between **the monthly baseline bandwidth** and **the average monthly peak bandwidth** is used as the monthly peak bandwidth. If the monthly baseline bandwidth of a month is greater than the average monthly peak bandwidth, the monthly peak bandwidth is the monthly baseline bandwidth. Otherwise, the monthly peak bandwidth is the average monthly peak bandwidth. | 300 Mbit/s |
| Monthly peak bandwidth price | The price is fixed for each calendar month and is irrelevant to the actual number of days of a month. | ¥120 CNY |

| Item | Description | Example Value |
|------|-------------|---------------|
| Shared bandwidth in-use days | The actual days that the shared bandwidth is used in the current month | 16 days |
| Calendar days of the month | The number of days in the current calendar month | 30 days |
| Billing formula | Monthly peak bandwidth x Monthly peak bandwidth price x Shared bandwidth in-use days/Calendar days of the month | |

📖 **NOTE**

**Table 2-3** is for reference only. The final price may differ.

**Monthly baseline bandwidth**

- Daily baseline bandwidth

    - Daily baseline bandwidth = Baseline percentage x Shared bandwidth. The baseline percentage is 20%.

    - The size of a shared bandwidth with the enhanced 95 percentile billing can be changed and the change takes effect immediately. After the shared bandwidth is changed, its baseline bandwidth changes accordingly.

    - The daily baseline bandwidth is calculated based on the maximum baseline bandwidth set for a day. For example, if the bandwidth is adjusted from 100 Mbit/s to 300 Mbit/s and then to 200 Mbit/s during a day, the daily baseline bandwidth is 60 Mbit/s (300 Mbit/s x 20%).

- Monthly baseline bandwidth

    - A bandwidth can be adjusted frequently to suit the traffic requirements during a month.

    - The monthly baseline bandwidth is calculated based on the following formula (only the integer is retained in the calculated result): **Monthly baseline bandwidth = (Baseline bandwidth 1 x Number of days using baseline bandwidth 1 + Baseline bandwidth 2 x Number of days using baseline bandwidth 2 + ... + Baseline bandwidth n x Number of days using baseline bandwidth n)/Number of days using all baseline bandwidths in a month**.

**Average monthly peak bandwidth**

- Daily peak bandwidth

    - Inbound and outbound traffic data is collected every five minutes.

    - The averages of both inbound bandwidth and outbound bandwidth within five minutes are calculated, and the larger one is used as the bandwidth for that collection.

    - After all meter readings within a day are obtained, they are sequenced in descending order. The top four peak bandwidths are discarded, and the fifth peak bandwidth is used as the daily peak bandwidth.

**Figure 2-2** Daily peak bandwidth



- Inbound and outbound traffic data is collected every five minutes.
- The fifth peak bandwidth value is used as the daily peak bandwidth.

288
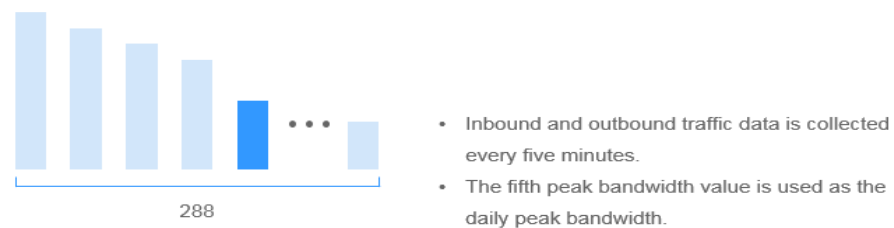
☐ NOTE

> If less than five peak bandwidths are obtained in a day, the smallest one is used as the daily peak bandwidth. A daily peak bandwidth is an integer (any fractional parts are discarded).

- Average monthly peak bandwidth

  At the end of each month, the daily peak bandwidths are sequenced in descending order. The average of the top five daily peak bandwidths is the average monthly peak bandwidth (only the integer is retained and fractional parts are discarded).

  ☐ NOTE

  > If less than five daily peak bandwidth values are obtained, the average of all the daily peak bandwidths in the month is the average monthly peak bandwidth. A monthly peak bandwidth is an integer (any fractional parts are discarded).

## Price Change After Specification Change

If you change the specifications of a shared bandwidth billed by 95th percentile bandwidth (enhanced), the original order will become invalid and a new order will be placed. You will be billed based on the new specifications.

If you change specifications within a given hour, multiple records will be generated. Different records record the billing for different specifications.

For example, if you purchased a shared bandwidth (500 Mbit/s) billed by 95th percentile bandwidth (enhanced) at 09:00:00 and increased the bandwidth to 1,000 Mbit/s at 09:30:00, the following items will be billed:

- Bandwidth of 500 Mbit/s from 09:00:00 to 09:30:00
- Bandwidth of 1,000 Mbit/s from 09:30:00 to 10:00:00

## Arrears Impact

**Figure 2-3** shows the statuses an enhanced 95th percentile billing resource can have throughout its lifecycle. After an enhanced 95th percentile billing resource is purchased, it enters the valid period and runs normally during this period. If your account goes into arrears, the resource enters a grace period and then a retention period.

**Figure 2-3** Life cycle of enhanced 95th percentile billing resources
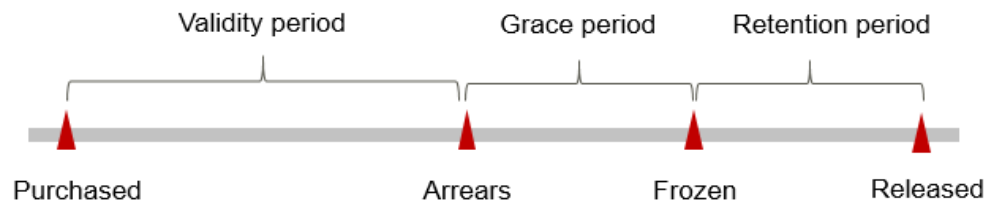


**Arrears Reminder**

The system will bill you for pay-per-use resources after each billing cycle ends. If your account goes into arrears, we will notify you by email, SMS, or in-app message.

**Impact of Arrears**

If your account is insufficient to pay your amount due, your account goes into arrears and your resource enters the grace period. Pay-per-use resources are not stopped immediately. You are still responsible for expenditures generated during the grace period. You can view the charges on the **Billing Center** > **Overview** page and pay any past due balance as needed.

If you do not bring your account balance current before the grace period expires, the EIP status turns to **Frozen** and enters a retention period.

If you do not bring your account balance current before the retention period ends, the EIP will be released.

# 2.5 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 2-4** 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 | • EIP reservation price): If a pay-per-use EIP is unbound from an instance, the EIP (reservation price) will be billed.<br>If your EIP is no longer required, **release it** to stop the billing.<br>• Traffic: will not be billed. |
| | Pay-per-use EIP billed by bandwidth | • EIP reservation price): If a pay-per-use EIP is unbound from an instance, the EIP (reservation price) will be billed.<br>If your EIP is no longer required, **release it** to stop the billing.<br>• Bandwidth: will continue to be billed.<br>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 | • EIP reservation price): If a pay-per-use EIP is unbound from an instance, the EIP (reservation price) will be billed.<br>If your EIP is no longer required, **release it** to stop the billing.<br>• Shared bandwidth: will continue to be billed.<br>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. | • Pay-per-use EIP billed by traffic<br>• 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**. |

## 2.6 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). 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 Do I Access the Internet Using an EIP Bound to an Extension NIC?

1. After an EIP is bound to an extension NIC, log in to the ECS and use the **route** command to query the routes.

   You can run **route --help** to learn more about the **route** command.

**Figure 3-1** Viewing route information



2.  Run the **ifconfig** command to view NIC information.

**Figure 3-2** Viewing NIC information



3.  Enable access to the Internet through the extension NIC by default.

    a.  Run the following command to delete the default route of the primary NIC:

        **route del -net 0.0.0.0 gw 192.168.11.1 dev eth0**

        192.168.11.1 is the gateway of the subnet that the NIC works. You can view the gateway on the **Summary** tab page of the subnet on the management console.

        ☐ **NOTE**

        This operation will interrupt ECS communication. It is recommended that you perform the configuration by following step **4**.

    b.  Run the following command to configure the default route for the extension NIC:

        **route add default gw 192.168.17.1**

4.  Configure Internet access from the extension NIC based on your destination address.

    Run the following command to configure access to a specified CIDR block (for example, *xx.xx*.0.0/16) through the extension NIC:

You can configure the CIDR block as required.

**route add -net xx.xx.0.0 netmask 255.255.0.0 gw 192.168.17.1**

# 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**.

If you want to change an EIP for your ECS, refer to **Changing an EIP**.

# 3.4 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. For details, see **Configuration Example**.

## Configuration Example

**Table 3-1** lists ECS configurations.

**Table 3-1** ECS configurations

| Parameter | Configuration |
|---|---|
| Name | ecs_test |
| Image | CentOS 6.5 64bit |
| EIP | 2 |
| Primary NIC | eth0 |
| Secondary NIC | eth1 |

**Example 1:**

If you intend to access public network 11.11.11.0/24 through standby NIC **eth1**, perform the following operations to configure a route:

1. Log in to the ECS.
2. Run the following command to configure a route:

   **ip route add 11.11.11.0/24 dev eth1 via 192.168.2.1**

In the preceding command, **192.168.2.1** is the gateway IP address of standby NIC **eth1**.

**Example 2:**

Based on example 1, if you intend to enable routing for default public network traffic through standby NIC **eth1**, perform the following operations to configure a route:

1. Log in to the ECS.

2. Run the following command to delete the default route:

   **ip route delete default**

---

**NOTICE**

Exercise caution when deleting the default route because this operation will interrupt the network and result in SSH login failures.

---

3. Run the following command to configure a new default route:

   **ip route add 0.0.0.0/0 dev eth1 via 192.168.2.1**

   In the preceding command, **192.168.2.1** is the gateway IP address of standby NIC **eth1**.

# 4 Bandwidth

## 4.1 What Bandwidth Types Are Available?

There are dedicated bandwidths and shared bandwidths. A dedicated bandwidth can only be used by one EIP, but a shared bandwidth can be used by multiple EIPs.

## 4.2 Is There a Limit to the Number of EIPs That Can Be Added to Each Shared Bandwidth?

A maximum of 20 EIPs can be added to each shared bandwidth. If you want to add more EIPs to each shared bandwidth, request a quota increase. For details, see **What Is a 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 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
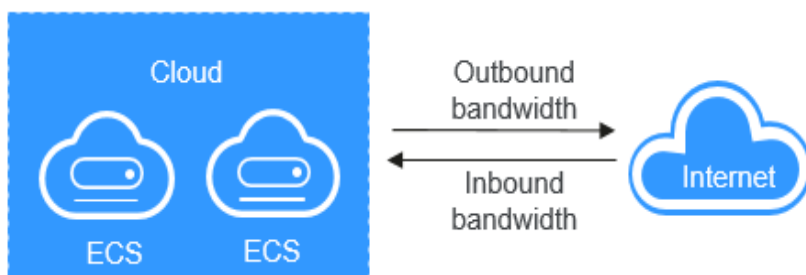


**Table 4-1** Inbound bandwidth and outbound bandwidth

| Type | Description |
|------|-------------|
| Outbound bandwidth | Bandwidth consumed when data is transferred from 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. |
| Inbound bandwidth | Bandwidth consumed when data is transferred from the Internet to 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. |

# 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 is the upper limit of the outbound bandwidth. If an ECS running your web applications cannot be accessed smoothly from the Internet, check whether the outbound bandwidth of the EIP bound to the ECS is greater than the configured bandwidth size.
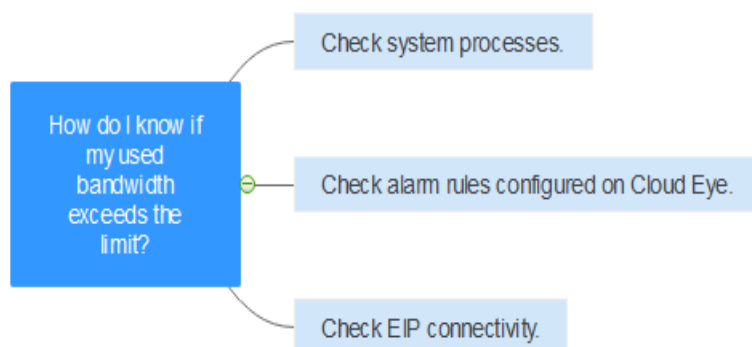
> ◫ **NOTE**
>
> If the outbound bandwidth exceeds the configured bandwidth size, there may be packet loss. To prevent data loss, it is recommended that you monitor the bandwidth.

## Troubleshooting

The issues here are described in order of how likely they are to occur.

Troubleshoot the issue by ruling out the causes described here, one by one.

**Figure 4-2** Troubleshooting



**Table 4-2** Troubleshooting

| Possible Cause | Description | Solution |
|---|---|---|
| System processes leading to high bandwidth | 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. | See **System Processes Leading to High Bandwidth Usage** |
| Improper Cloud Eye alarm rules | If you have created 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. | See **Improper Cloud Eye Alarm Rules** |

| Possible Cause | Description | Solution |
|---|---|---|
| EIP connection failure | An ECS with an EIP bound cannot access the Internet. | See **Why Can't My ECS Access the Internet Even After an EIP Is Bound?** |

### 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 locate the processes that have led to excessively high bandwidth or CPU usage, and optimize or stop the processes.

### Improper Cloud Eye Alarm Rules

If you have created 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 when the maximum outbound bandwidth reaches 4.8 Mbit/s three periods in a row. You can also **increase your bandwidth**.

1.  Log in to the management console, under **Management & Deployment**, click **Cloud Eye**. On the **Cloud Eye** console, choose **Alarm Management** > **Alarm Rules**.
2.  Click **Create Alarm Rule** and configure an alarm rule to generate alarms when the bandwidth exceeds the configured limit.

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

The bandwidth is measured in bit/s, but the download rate is measured in byte/s.

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).

# 4.7 What Are the Differences Between Static BGP and Dynamic BGP?

The differences between static BGP and dynamic BGP are as follows:

**Table 4-3** Differences between static BGP and dynamic BGP

| Item | Static BGP | Dynamic 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 best path based on the real-time network conditions and preset policies. |
| Assurance | When changes occur on a network that uses static BGP, the manual configuration takes some time and high availability cannot be guaranteed.<br><br>**NOTE**<br>If you select static BGP, your application system must have disaster recovery setups in place. | When a fault occurs on a carrier's link, dynamic BGP will quickly select another optimal path to take over services, ensuring service availability. |
| Service availability | 99% | 99.95% |

**◻ 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.
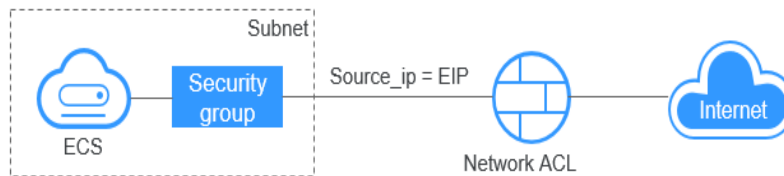
### Troubleshooting

**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?**
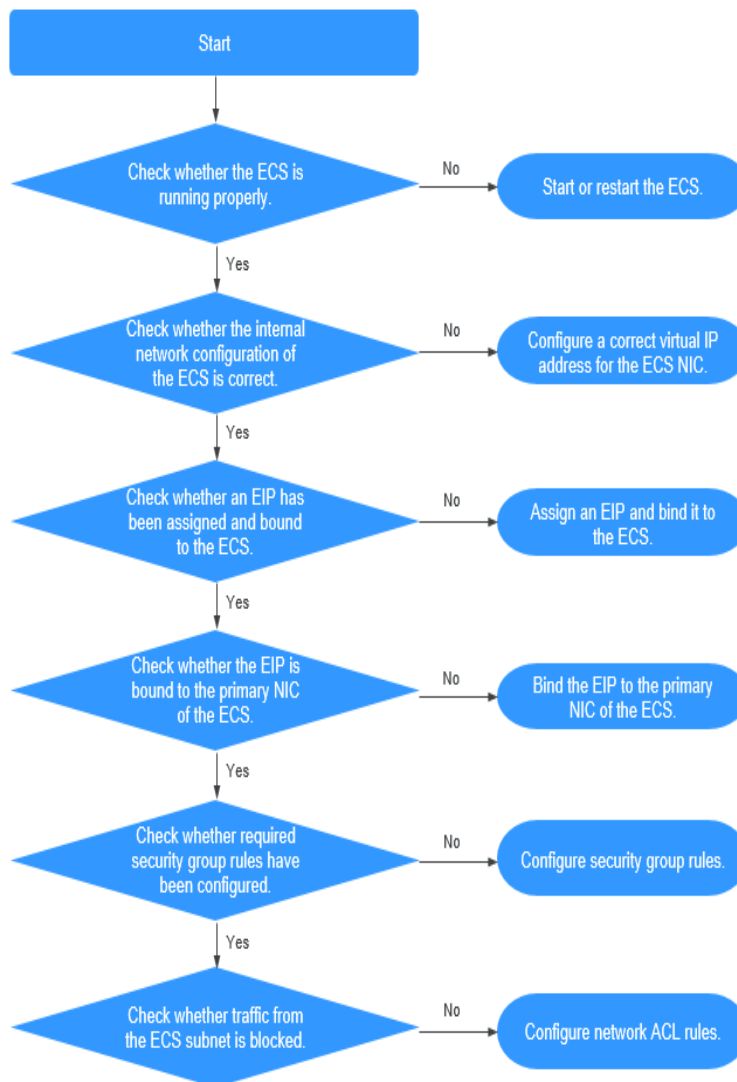
**Checking EIP Connectivity**

**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 ECS Is Running Properly**
2. **Step 2: Check Whether the Network Configuration of the ECS Is Correct**
3. **Step 3: Check Whether an EIP Has Been Assigned and Bound to the ECS**
4. **Step 4: Check Whether an EIP Is Bound to the Primary NIC of the ECS**
5. **Step 5: Check Whether Required Security Group Rules Have Been Configured.**

6. **Step 6: Check Whether Traffic from the ECS Subnet Is Blocked**

## Step 1: Check Whether the ECS Is Running Properly

Check the ECS status.

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

**Figure 5-3** ECS status



## Step 2: Check Whether the Network Configuration of the ECS Is Correct

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

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

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

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

   **Figure 5-4** Virtual IP address of a NIC

   

   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

   

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

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

The ECS shown in **Figure 5-6** has no EIP bound. It only has a private IP address bound.

**Figure 5-6** EIP status



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

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

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

As shown in **Figure 5-7**, the EIP is bound to the primary NIC.

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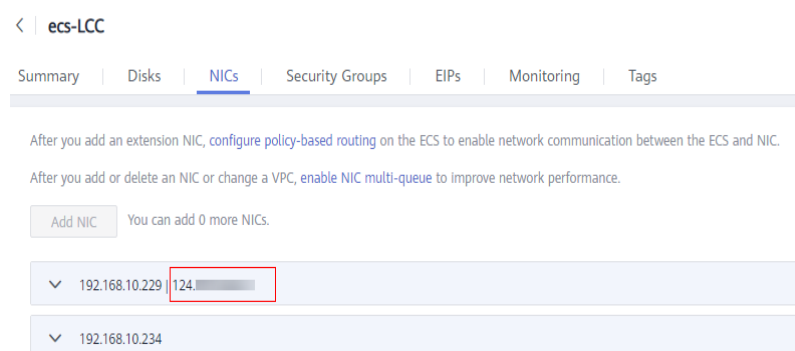


## Step 5: Check Whether Required Security Group Rules Have Been Configured.

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 ECS 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 ECS subnet.

# 5.3 Why Can't an EIP Be Pinged?

## Symptom

After you purchase an EIP and bind it to an ECS, the EIP cannot be pinged on a local server or other cloud servers.

## Fault Locating

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.

**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**. |
| 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 [icon] 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.

    **Table 5-2** Security group rules

| Transfer Direction | Type | Protocol/Port Range | Source |
|---|---|---|---|
| Outbound | IPv4 | ICMP/Any | 0.0.0.0/0 <br><br> 0.0.0.0/0 indicates all IP addresses. |

8. On the **Inbound Rules** tab, click **Add Rule**. In the displayed dialog box, set required parameters to add 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 <br><br> 0.0.0.0/0 indicates all IP addresses. |

9. 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**

1. 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.

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

    **iptables -L**

    If the command output shown in **Figure 5-8** is displayed, there is no ICMP rule blocking the ping operations.

**Figure 5-8** Checking firewall rules



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**

## Checking Whether Ping Operations Have Been Disabled on the ECS

**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.

2. Click the ACL name to view its status.

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

   **□ 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.

## 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 5-9** 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.

# 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 Do I Unbind an EIP from an Instance and Bind a New 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.

# 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%.

- Unstable carrier lines: The network between the local server and the cloud is unstable. Contact the carrier to check the network status.

# 6 Change History

| Released On | Description |
|---|---|
| 2022-10-30 | This release incorporates the following changes:<br><br>Added **Why Does the Download Speed of My ECS Is Slow?** |