Elastic IP

FAQs

Issue 02

Date 2025-10-27

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


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.

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 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 assign another EIP first and then release the one that you do not need.

1.2 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***.

2 Billing and Payments

2.1 How Is an EIP Billed?

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 price
  - 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

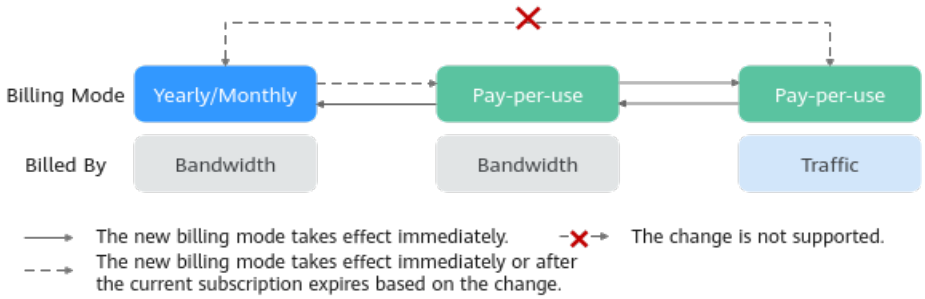
For details, see **EIP Billing**.

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). • 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: 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. 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. 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.
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. • 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: 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. 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 (Billed by Bandwidth) upon Expiration

Step 1 Go to the **EIP list** page.

Step 2 In the EIP list, change billing mode of a single EIP or multiple EIPs from yearly/monthly to pay-per-use (billed by bandwidth):

- Single EIP:

  Locate the row that contains the EIP, click **More** in the **Operation** column, and click **Change to Pay-per-Use upon Expiration**.

- Multiple EIPs:

  Select the EIPs in the EIP list, click **More** in the upper left corner of the list, and click **Change to Pay-per-Use upon Expiration**.

You are switched to a page of the Billing Center.

Step 3 Confirm the information and click **Change to Pay-per-Use upon Expiration**.

----End

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

Step 1 Go to the **EIP list** page.

Step 2 In the EIP list, change billing mode of a single EIP or multiple EIPs from yearly/monthly to pay-per-use (billed by bandwidth):

- Single EIP:

  Locate the row that contains the EIP, click **More** in the **Operation** column, and click **Change to Pay-per-Use Immediately**.

- Multiple EIPs:

  Select the EIPs in the EIP list, click **More** in the upper left corner of the list, and click **Change to Pay-per-Use Immediately**.

Step 3 In the displayed dialog box, confirm the information and click **OK**.

Step 4 Confirm the information and click **Change to Pay-per-Use**.

----End

NOTE

When the change is complete, the pay-per-use billing will be applied immediately, and the remaining fees will be refunded. For details about the billing rules, see **From Yearly/Monthly to Pay-per-Use Immediately**.

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

Step 1 Go to the **EIP list** page.

Step 2 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 click **Change Billing Mode** in the upper left corner of the EIP list.

Step 3 In the displayed dialog box, confirm the information and click **Change**.

Step 4 On the **Change Subscription** page, set parameters such as **Usage Duration**.

Step 5 Click **Pay**.

----End

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. **CAUTION** The pay-per-use (billed by bandwidth) billing mode is based on the fixed bandwidth you purchased. If the **actual bandwidth used exceeds the purchased one**, **no extra charges will apply**, but the **network quality may be affected**. You are advised to plan the bandwidth based on actual service requirements.
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.

Procedure

Step 1 Go to the **EIP list** page.

Step 2 In the EIP list, locate the row that contains the EIP, click **More** in the **Operation** column, and click **Modify Bandwidth**.

Step 3 On the **Modify Bandwidth** page, change the billing option as prompted.

You can also change the bandwidth name and size.

Step 4 Click **Next**.

Step 5 On the displayed page, confirm the configurations and click **Submit**.

----End

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?**

3 EIP

3.1 What Are the Differences Between EIPs, Private IP Addresses, and Virtual IP Addresses?

Different types of IP addresses have different functions.

Figure 3-1 IP address architecture

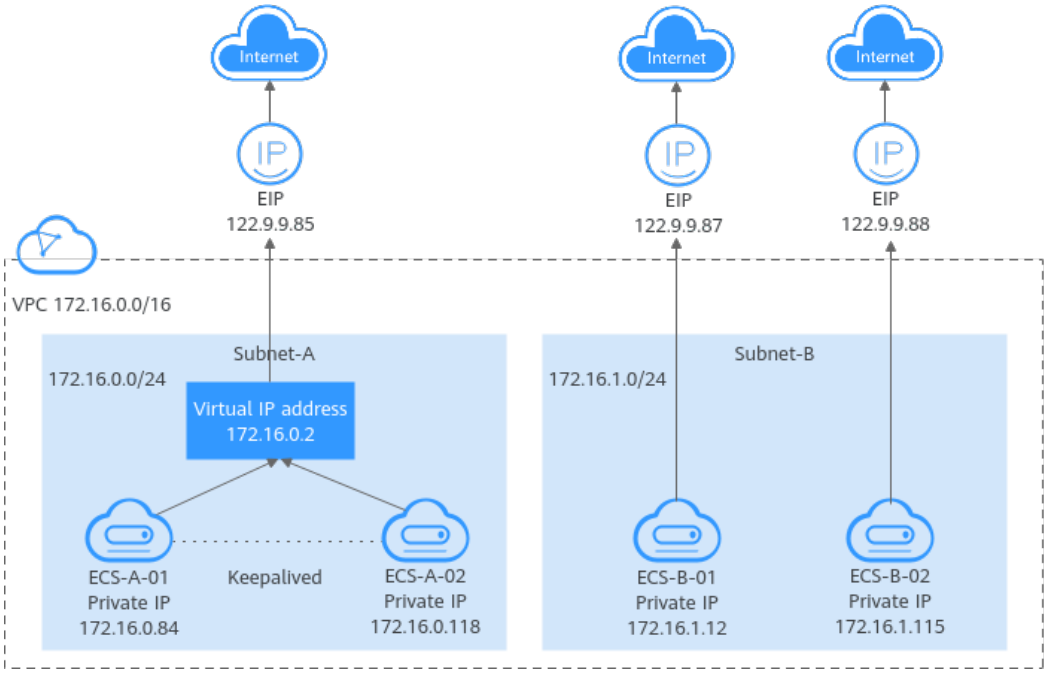


Table 3-1 Functions of different IP address types

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 • Private IP address of ECS-B-01: 172.16.1.12
Virtual IP address	A virtual IP address is a private IP address independently assigned from a VPC subnet. It can be released when no longer needed. You can: • Bind one or more virtual IP addresses to a cloud server so that you can use either the virtual or private IP address to access the server. If you have multiple services running on a cloud server, you can use different virtual IP addresses to access them. • Bind a virtual IP address to multiple cloud servers. 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 avoid single points of failure, you can deploy cloud servers in the active/standby mode or deploy one active cloud server and multiple standby cloud servers. In this arrangement, the cloud servers all use the same virtual IP address. If the active cloud server goes down, the standby cloud server becomes the active server and continues to provide services. 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.

IP Address Type	Description	Example Value
EIP	EIPs allow cloud resources to access the Internet. They can be flexibly bound to or unbound from instances. • 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. 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. • Bind EIP (122.9.9.87) to ECS-B-01 to enable ECS-B-01 to access the Internet.

3.2 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 because of untimely data update.
- 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**.

3.3 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.

3.4 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**.

3.5 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 network interfaces attached and you want to bind multiple EIPs to this ECS, you need to configure policy-based routes for these network interfaces so that these extension network interfaces can communicate with external networks. For details, see **Configuration Example**.

Configuration Example

Table 3-2 lists ECS configurations.

Table 3-2 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**.

3.6 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.

4 Bandwidth

4.1 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 about the outbound bandwidth and inbound bandwidth, see **Table 4-1**.

- **Outbound Bandwidth** means the same thing as **Upstream Bandwidth** or **Upstream Traffic** on the Cloud Eye console.
- **Inbound Bandwidth** means the same thing as **Downstream Bandwidth** and **Downstream Traffic** on the Cloud Eye console.

Figure 4-1 Inbound bandwidth and outbound bandwidth

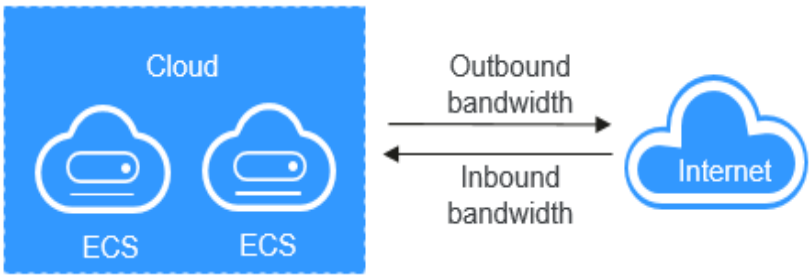


Table 4-1 Inbound bandwidth and outbound bandwidth

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. Outbound bandwidth means the same thing as upstream bandwidth on the Cloud Eye console.
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. Inbound bandwidth means the same thing as downstream bandwidth on the Cloud Eye console.

4.2 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.

4.3 How Do I Know If My EIP Bandwidth 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.

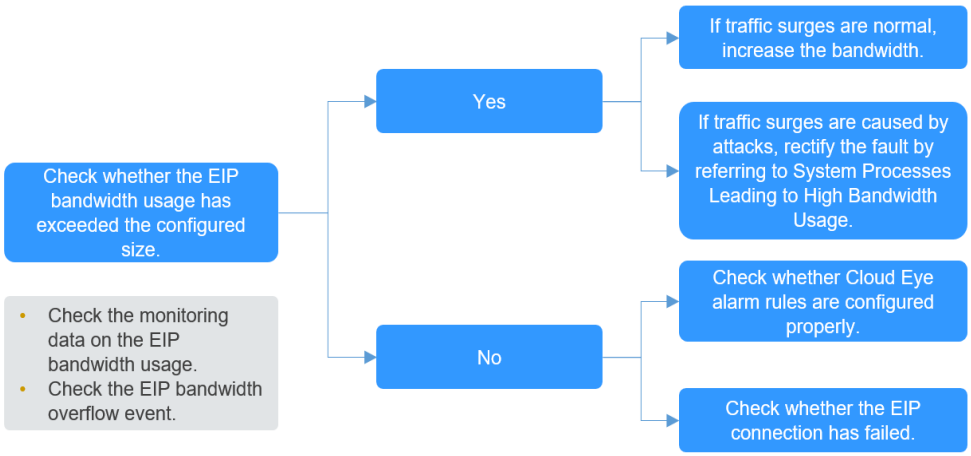
NOTE

If the bandwidth exceeds the configured bandwidth size, there may be packet loss or remote login failure to an ECS. 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.

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 traffic surge is normal.

1. If the traffic surge is normal, increase the bandwidth. For details, see **Modifying an EIP Bandwidth**.

2. If the traffic surge is not normal, for example, the surge was caused by attacks, refer 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 locate processes that have led to excessively high bandwidth or CPU usage, and optimize or stop the processes.

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.

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. You can also **increase your bandwidth**. To create an alarm rule:

1. In the left navigation pane of 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 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. In the left navigation pane of 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**.

4.4 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.

4.5 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.

4.6 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).

4.7 What Are the Differences Between a Dedicated Bandwidth and a Shared Bandwidth? Can a Dedicated Bandwidth Be Changed to a Shared Bandwidth or the Other Way Around?

You can select a dedicated or shared bandwidth based on your requirements by referring to **Table 4-2**.

Table 4-2 Differences between dedicated and shared bandwidths

Item	Dedicated Bandwidth	Shared Bandwidth
Concepts	If you assign an EIP and do not add it to a shared bandwidth, the EIP uses a dedicated bandwidth by default no matter how the EIP is billed. A dedicated bandwidth can only be used by one EIP. Each EIP can only be bound to one cloud resource, such as an ECS, a NAT gateway, or a load balancer.	A shared bandwidth can be used by multiple pay-per-use EIPs. • The shared bandwidth is dynamically allocated to the EIPs based on the actual usage conditions. • Adding an EIP to or removing an EIP from a shared bandwidth does not affect your services.
Features	• Stable performance: The bandwidth is dedicated, so your use of the bandwidth is not affected by other resources. This type of bandwidth is ideal for applications requiring high-performance networks. • Quality of service (QoS): Guaranteed stable bandwidths and low latency are suitable for real-time applications.	• Cost-effectiveness: Multiple EIPs sharing the same bandwidth can effectively reduce the overall costs. This type of bandwidth is suitable for users with limited budgets. • Flexibility: You can dynamically adjust the size of a shared bandwidth based on your requirements. • Performance fluctuation: When the bandwidth is used by multiple EIPs at the same time, the bandwidth allocated to each EIP is limited.

Item	Dedicated Bandwidth	Shared Bandwidth
Applicable scenarios	• Bandwidth preemption needs to be avoided to ensure Internet access for all EIP at the same time. • High-performance and stable bandwidth is required, such as video streaming, online gaming, and financial transactions.	• Internet access needs to be scheduled at different times to optimize bandwidth usage. • There are no demanding requirements on bandwidth or multiple EIPs need to be used at the same time, such as web servers and test environments.
Changes between dedicated and shared bandwidths	A dedicated bandwidth **cannot be changed** to a shared bandwidth and vice versa. However, you can purchase a shared bandwidth for pay-per-use EIPs. • Add an EIP to a shared bandwidth and then the EIP will use the shared bandwidth. • Remove the EIP from the shared bandwidth and then the EIP will use the dedicated bandwidth.	

Bandwidth Preemption Descriptions

- **Dedicated bandwidth**: Each EIP has a fixed bandwidth and is not affected by other EIPs.

  For example, both EIP-A and EIP-B are allocated 20 Mbit/s of dedicated bandwidth.

  If the bandwidth of EIP-A hits 30 Mbit/s, there will be packet loss due to the bandwidth limit, while the bandwidth of EIP-B remains idle.
- **Shared bandwidth**: If the bandwidth usage of some EIPs is high, the idle bandwidth of other EIPs can be used.

  For example, two EIPs (EIP-A and EIP-B) are added to a shared bandwidth of 40 Mbit/s.
  - If EIP-A uses 30 Mbit/s and EIP-B uses 10 Mbit/s, the total bandwidth is 40 Mbit/s. EIP-A can use the idle bandwidth of EIP-B to increase its bandwidth and prevent packet loss.
  - If EIP-A uses 30 Mbit/s and EIP-B uses 15 Mbit/s, the total bandwidth reaches 45 Mbit/s and exceeds the 40 Mbit/s limit. In this case, the flexibility of the shared bandwidth fails and there will be packet loss on both EIPs.

4.8 What Are the Differences Between Static BGP and Dynamic BGP?

The EIP type cannot be changed. For example, dynamic BGP EIPs cannot be changed to static BGP EIPs because they are in different IP address pools.

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. **NOTE** 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 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

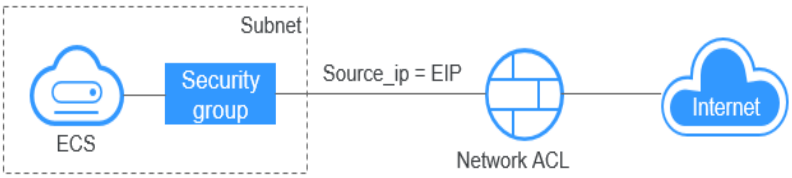
Checking Whether EIPs Are Blocked or Frozen

- 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

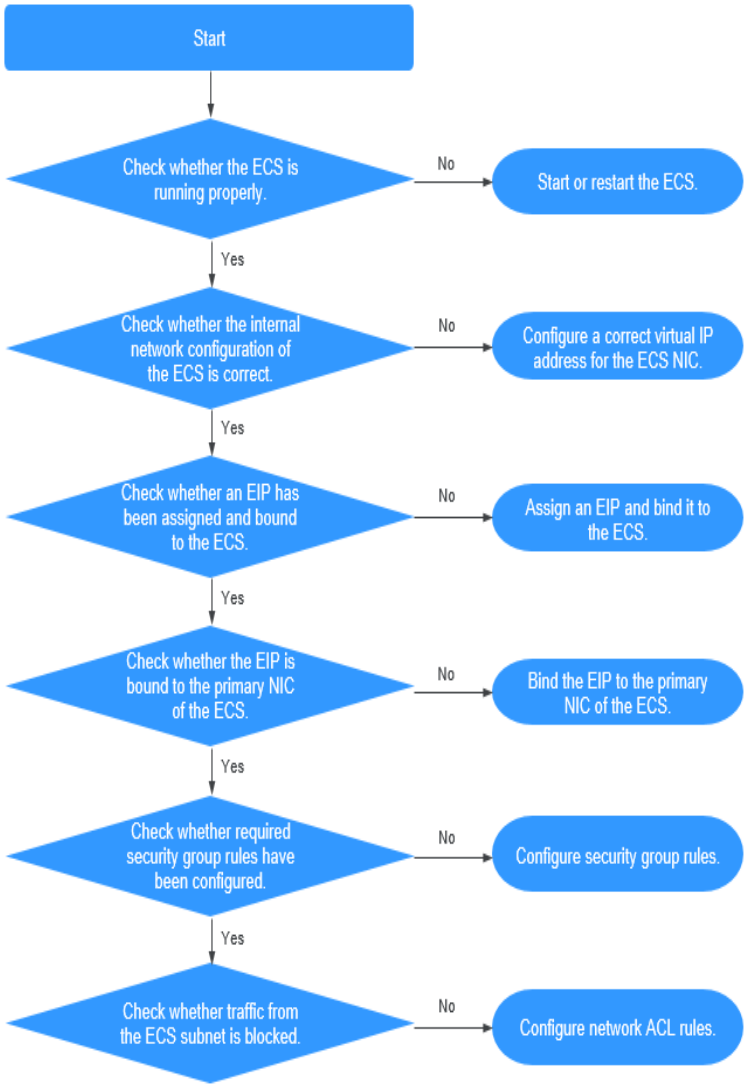
Figure 5-1 shows the networking diagram for an ECS to access the Internet using an EIP.

Figure 5-1 EIP network diagram



Locate the fault based on the following procedure.

Figure 5-2 Troubleshooting procedure



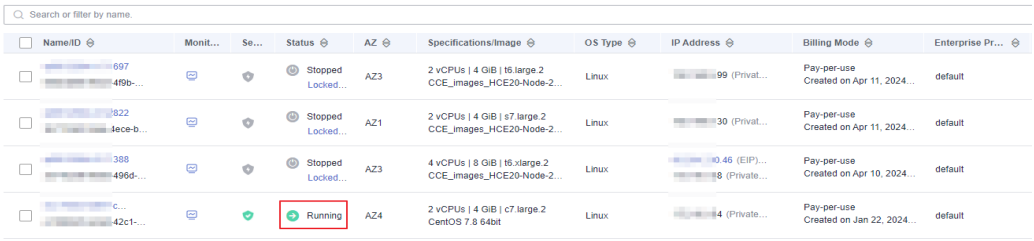
1. **Step 1: Check Whether the ECS Is Running Properly**
2. **Step 2: Check Whether the Network Configuration of the ECS Is Correct**
3. **Step 3: Check Whether an EIP Has Been Assigned and Bound to the ECS**
4. **Step 4: Check Whether an EIP Is Bound to the Primary Network Interface of the ECS**
5. **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

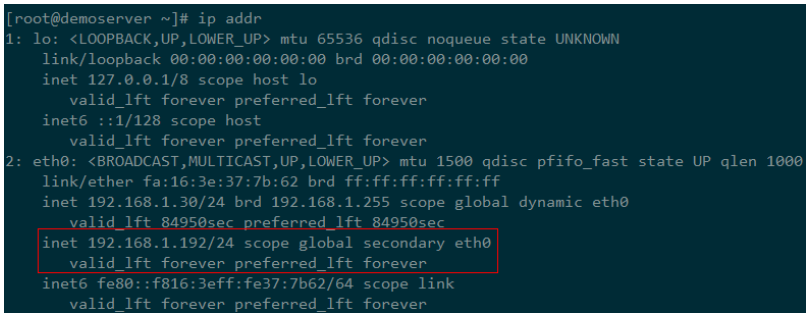
1. Check whether the ECS's network interface has an IP address assigned.

   Log in to the ECS, and run **ifconfig** or **ip address** to check the IP address of the ECS's network interface.

2. Check whether the ECS's network interface has a virtual IP address.

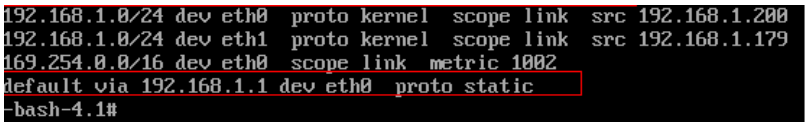
   Log in to the ECS, and run **ifconfig** or **ip address** to check whether the ECS's network interface has a virtual IP address. If the ECS's network interface has no virtual IP address, run the **ip addr add** *<virtual-IP-address>* **eth0** command to configure an IP address for the ECS's network interface.

   Figure 5-4 Virtual IP address of a network interface



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

   Figure 5-5 Default route

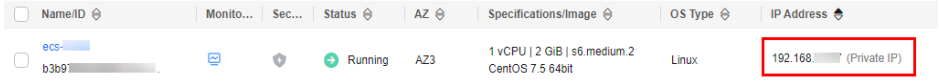


Step 3: Check Whether an EIP Has Been Assigned and Bound to the ECS

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



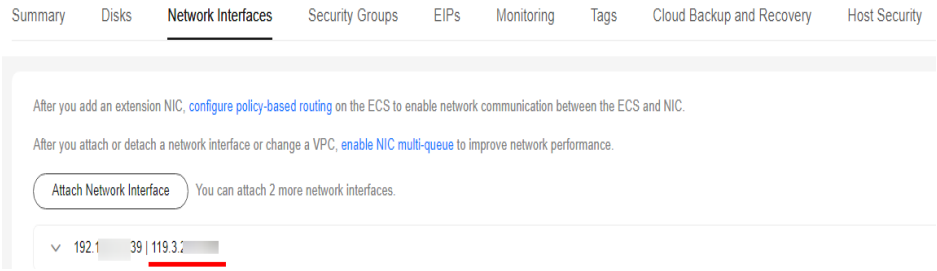
Step 4: Check Whether an EIP Is Bound to the Primary Network Interface of the ECS

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

You can view the network interface details by clicking the **Network Interfaces** tab on the ECS details page. By default, the first record in the list is the primary network interface.

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

Figure 5-7 Checking whether the EIP is bound to the primary network interface 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 associated with the subnet of the ECS's network interface blocks traffic.

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

5.2 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

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 Causes	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 Network 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 Normal**.
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 a region and project.
3. Click  . 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	Destination
Outbound	IPv4	ICMP/Any	0.0.0.0/0 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 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

```
[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

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 Network 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 Normal

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.

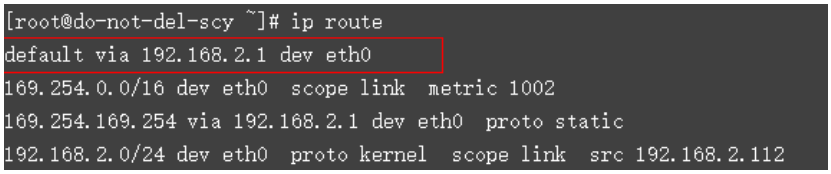
Checking the ECS Route Configuration If Multiple NICs Are Used

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.

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

Troubleshooting Process

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.

Submitting a Service Ticket

If the download speed is still slow after the preceding steps are performed, **submit a service ticket**.

5.4 How Do I Unblock an EIP?

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

Generally, as long as there are no attacks, blocked EIPs will be automatically unblocked 24 hours later. 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 **Changing an EIP for an Instance**.

5.5 Why Are My EIPs 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 an EIP or shared bandwidth is frozen, traffic will be interrupted. 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 an EIP or shared bandwidth is frozen, traffic will be interrupted. 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. To renew the subscription, choose **Renewals** on the management console. For details, see **Renewal Management**.

- **Attacks**

  EIPs will be frozen if their associated instances have security violations, such as attacks. Frozen EIPs cannot be used, modified, or released. If an EIP or shared bandwidth is frozen, traffic will be interrupted.

  You can also **change an EIP for an 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 not committed any violations, contact the regulatory authority to file an appeal. If your appeal is approved, Huawei Cloud will unfreeze your resources.

  You can also **change an EIP for an instance**.

5.6 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 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**.

5.7 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.

