Elastic IP

Best Practices

Issue	01
Date	2024-05-10

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions

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 Public Network Access

Products

Cloud services, such as EIP, NAT Gateway, and ELB can be used to connect to the Internet.

- EIP

  The EIP service provides independent public IP addresses and bandwidth for Internet access. EIPs can be bound to or unbound from ECSs, BMSs, virtual IP addresses, NAT gateways, or load balancers. Various billing modes are provided to meet diverse service requirements.

- ELB

  ELB distributes access traffic among multiple ECSs to balance the application load, improving fault tolerance and expanding service capabilities of applications. You can create a load balancer, configure a listening protocol and port, and add backend servers to a load balancer. You can also check the running state of backend servers to ensure that requests are sent only to healthy servers.

- NAT Gateway

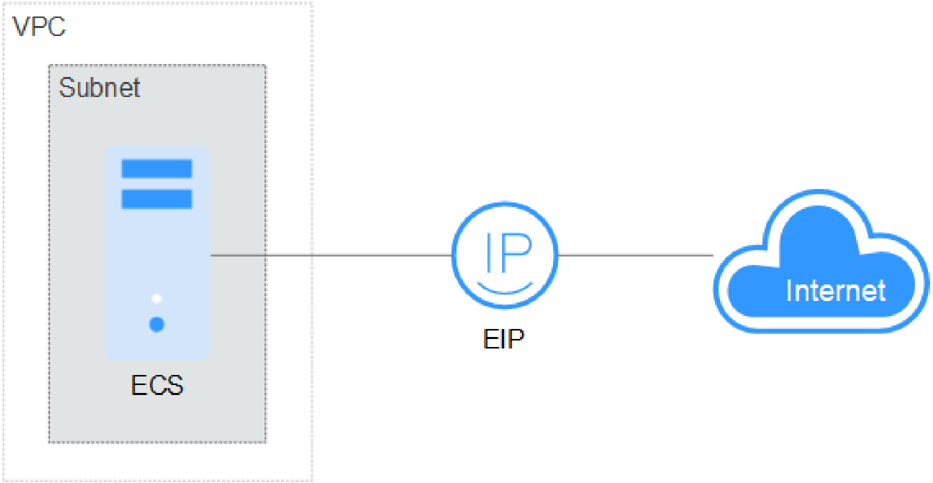
  NAT Gateway provides both SNAT and DNAT for your servers in a VPC and allows servers in your VPC to access or provide services accessible from the Internet.

Providing Services Accessible from the Internet

- Single ECS provides services accessible from the Internet.

  If you have only one application and the service traffic is small, you can assign an EIP and bind it to the ECS so that the ECS can provide services accessible from the Internet.

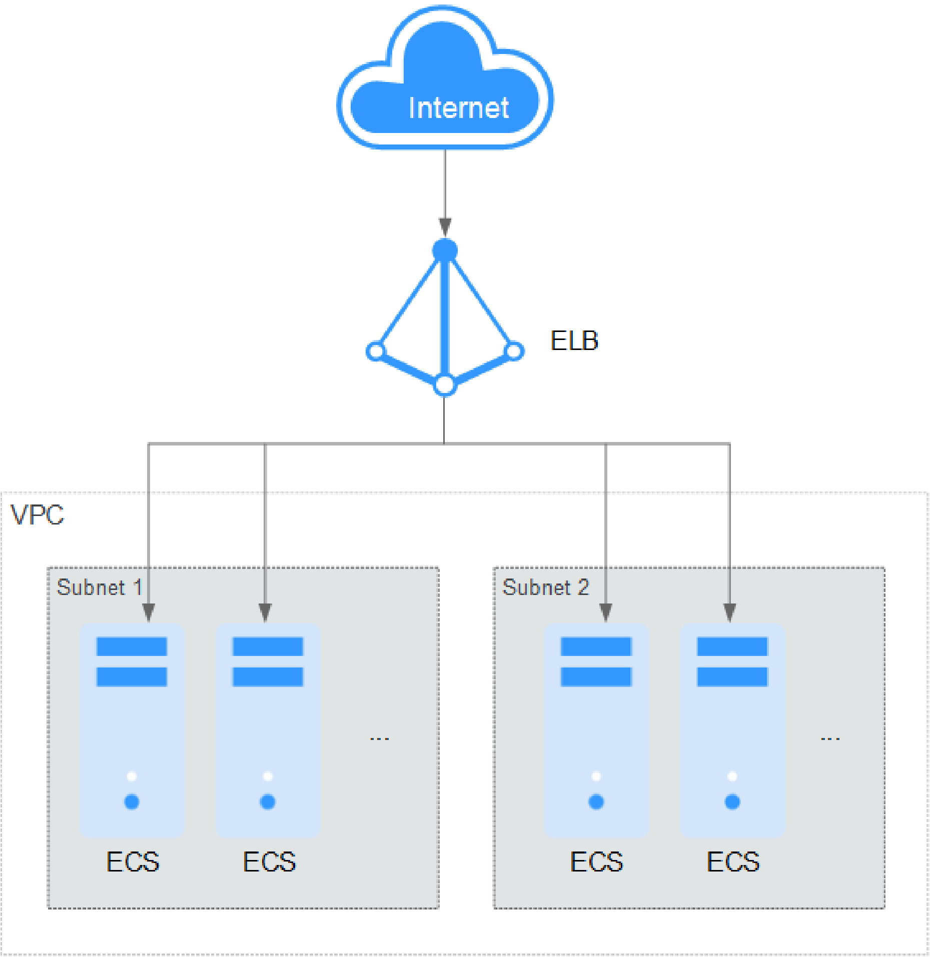
Figure 1-1 EIP



- Multiple ECSs balance workloads.

  In high-concurrency scenarios, such as e-commerce, you can use load balancers provided by the ELB service to evenly distribute incoming traffic across multiple ECSs, allowing a large number of users to concurrently access your business system or application. ELB deeply integrates with the Auto Scaling (AS) service, which enables automatic scaling based on service traffic and ensures service stability and reliability.

Figure 1-2 ELB

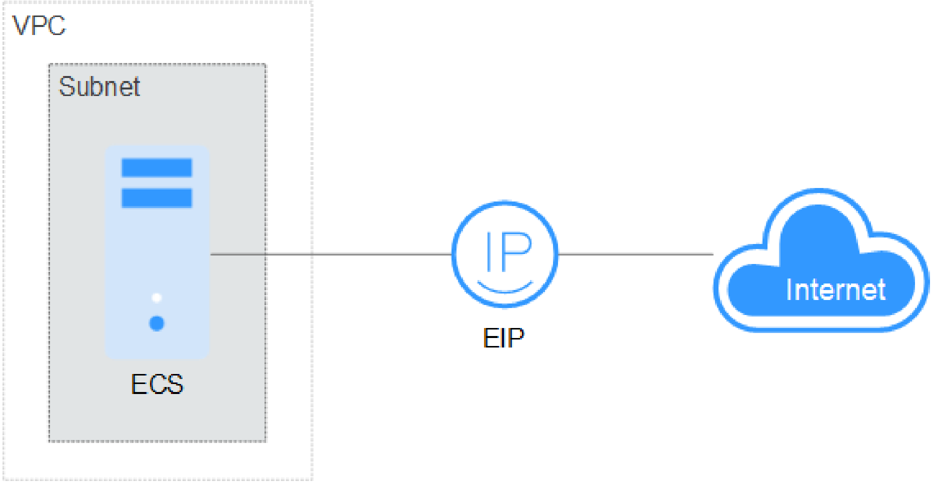


Accessing the Internet

- Single ECS accesses the Internet.

  When an ECS needs to access the Internet, you can bind an EIP to the ECS so that the ECS can access the Internet. Huawei Cloud allows your EIP to be billed on a pay-per-use basis. If you do not need to use the EIP, you can flexibly unbind it.

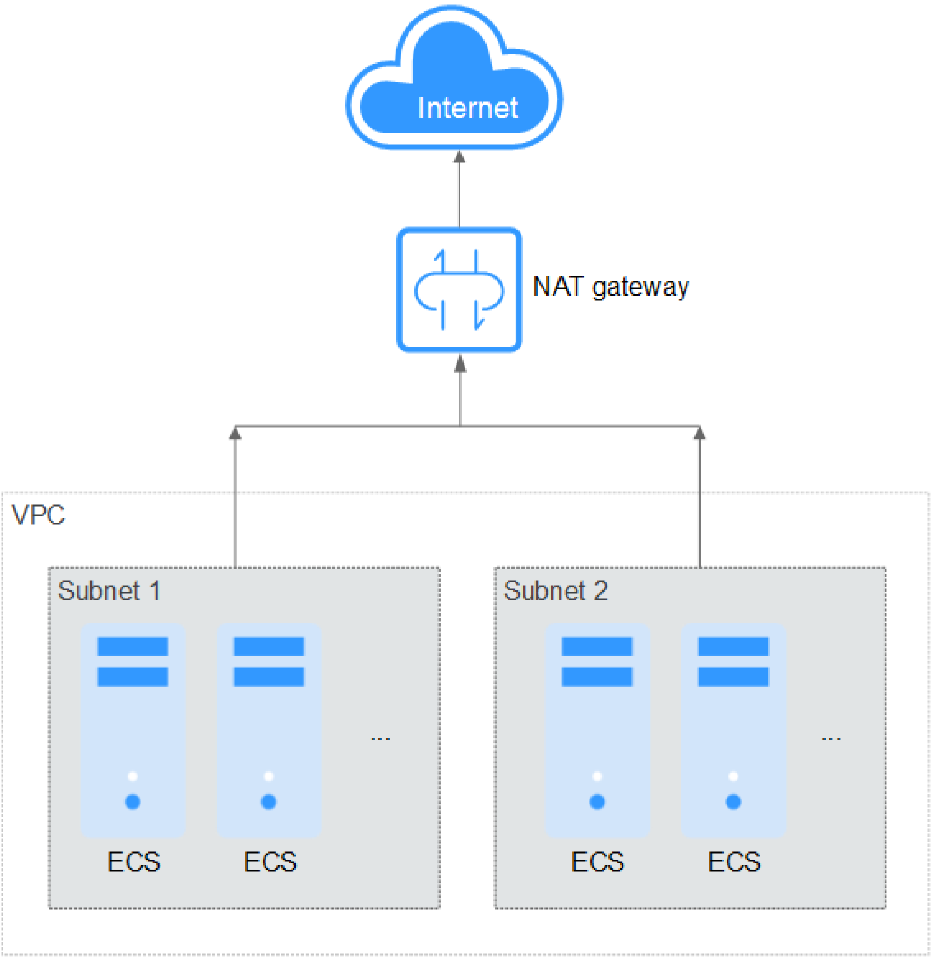
Figure 1-3 EIP



- Multiple ECSs access the Internet.

  If multiple ECSs in your VPC need to access the Internet, you can use a NAT gateway and configure SNAT rules by subnet to allow ECSs in the VPC to access the Internet. If you access to the Internet using an EIP but with no DNAT rules configured, external users cannot directly access the public network address of the NAT gateway through the Internet, ensuring ECS security.

Figure 1-4 NAT gateway



2 Lower Network Costs

You can select a proper product and billing mode based on your service requirements.

Dedicated Bandwidth

If you want to ensure the bandwidth available for a particular EIP, you are advised to purchase dedicated bandwidth. Dedicated bandwidth can only be used for a single, specific EIP. Dedicated bandwidth is not affected by other services.

An EIP can be billed by bandwidth or by traffic:

- Bandwidth: If your services use a large amount of traffic but are stable, an EIP billed by bandwidth is recommended.
- Traffic: If your services only use a relatively small amount of traffic, an EIP billed by traffic combined with a shared data package is recommended for a more favorable price.

If your traffic is stable, the yearly/monthly billing based on the bandwidth is more cost effective.

Shared Bandwidth

When you host a large number of applications on the cloud, if each EIP uses dedicated bandwidth, a lot of bandwidths are required, which incurs high costs. If all EIPs share the same bandwidth, your network operation costs will be lowered and your system O&M as well as resource statistics will be simplified. Multiple EIPs whose billing mode is pay-per-use can be added to a shared bandwidth. You can bind EIPs to products such as ECSs, NAT gateways, and load balancers so that these products can use the shared bandwidth.

Shared Data Package

A shared data package is a prepaid package for public network traffic. The price of the package is lower than that for the postpaid billing by traffic. Shared data packages greatly reduce the cost of traffic on a public network. A shared data package takes effect immediately after being purchased and no additional operations are required. If you have subscribed to pay-per-use EIPs billed by traffic in a region and buy a shared data package in the same region, the EIPs will use the shared data package.

- When to use a shared data package

  After a shared data package takes effect for a bandwidth billed by traffic, the traffic used by the bandwidth is deducted from the shared data package first. After the shared data package is used up, the bandwidth is billed by the amount of traffic used. A shared data package saves more if your amount of traffic used is huge.

- Additional notes on shared data packages
  - Only the traffic generated in the region selected when the shared data package is purchased can be deducted.
  - Dynamic and static shared data packages are used to deduct the traffic generated by dynamic BGP and static BGP EIPs, respectively.
  - A shared data package has a validity period of one calendar month or one calendar year from the date of purchase. After this period expires, the unused traffic expires as well and cannot be used. You are advised to evaluate the size of a shared data package required based on the historical usage.
  - If you enable the auto-renew function for a shared data package, the system automatically attempts to renew the subscription within seven days before the shared data package expires. After the renewal is successful, the remaining traffic in the shared data package can be used within the new validity period.
  - After a shared data package is used up, your service will not automatically stop. The system automatically bills you based on traffic, ensuring service system availability.

3 On-premises Data Centers Providing Internet-Accessible Services Using IPv6 EIPs

Application Scenarios

You can use the IPv6 function of the EIP service to map existing IPv4 EIPs into IPv6 EIPs. After the IPv6 EIP function is enabled, you will obtain both an IPv4 EIP and its corresponding IPv6 EIP. External IPv6 addresses can access cloud resources through this IPv6 EIP.

If existing services in an on-premises data center (IDC) cannot be migrated to the cloud because they use IPv4 addresses and also the IPv4/IPv6 dual-stack reconstruction cannot be completed for these services in a short period, IPv6 EIPs can be used to connect to the on-premises data center. Then, the data center can provide internet-accessible services using IPv6 EIPs without the need to reconstruct the existing IPv4 network.

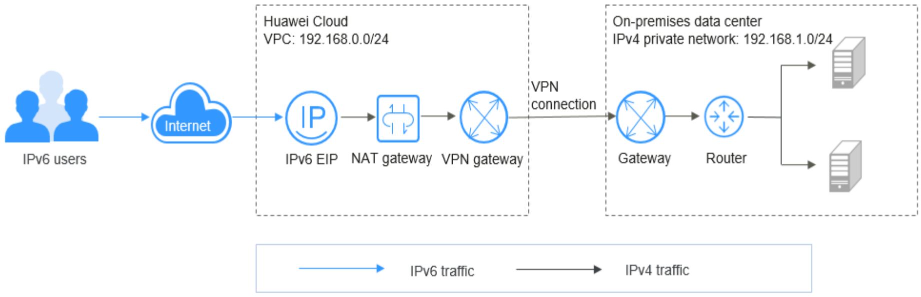
Architecture

1. A virtual private network (VPN) connects an on-premises data center to a VPC.
2. A NAT gateway in the VPC uses an IPv6 EIP to provide internet-accessible services.

NOTE

- IPv6 EIP can only be used to provide internet-accessible services and cannot access IPv6 addresses.
- The CIDR block of an on-premises data center cannot overlap with the CIDR block of the VPC subnet. Otherwise, the communication between them will fail.

Figure 3-1 Networking diagram



Advantages

On-premises data centers can provide internet-accessible services using IPv6 EIPs without the need to reconstruct their existing IPv4 networks, meeting different requirements of IPv4 and IPv6 users.

Notes and Constraints

After IPv6 EIP is enabled, inbound and outbound security group rules need to be added to allow packets to and from the IP address range 198.19.0.0/16. IPv6 EIP uses NAT64 to convert the source IPv6 address in the inbound direction to an IPv4 address in the IP address range 198.19.0.0/16. The source port can be a random one, the destination IP address is the private IPv4 address of your local server, and the destination port remains unchanged.

Table 3-1 Security group rules

Direction	Protocol	Source and Destination
Inbound	All	Source: 198.19.0.0/16
Outbound	All	Destination: 198.19.0.0/16

Resource Planning

Table 3-2 Resources

Resource	Resource Name	Description	Quantity
VPC	VPC-Test01	This VPC (192.168.0.0/24) will have an EIP and a NAT gateway deployed.	1
EIP	EIP-IPv4&IPv6	When you create this IPv4 EIP, enable the IPv6 EIP function.	1
NAT gateway	NAT-Test	This public NAT gateway will have an EIP bound.	1

Resource	Resource Name	Description	Quantity
VPN gateway	VPN-GW-Test	This VPN gateway is an egress gateway in a VPC and allows reliable and encrypted communications between a VPC and an on-premises data center.	1
VPN connection	VPN-Test	This VPN connection quickly builds a reliable and encrypted communications channel between a VPN gateway and a remote gateway.	1
On-premises data center	IDC-Test	This on-premises data center (192.168.1.0/24) includes remote gateways, routers, and backend servers.	1

Operation Process

1. **1**
2. **2**
3. **3**

Procedure

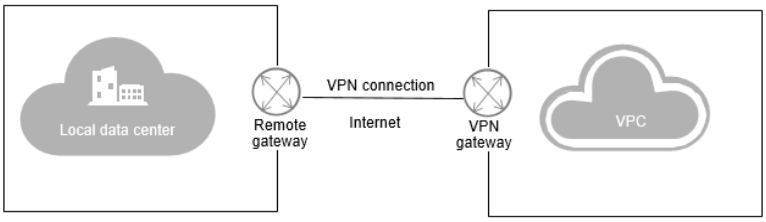
1. **Buy an EIP and enable the IPv6 EIP function.**

   Buy an EIP with the required bandwidth and select the **IPv6 EIP** option.

   For details, see **Assigning an EIP**.

2. **Configure a VPN.**

   A VPN consists of a VPN gateway and one or more VPN connections. A VPN gateway provides an internet egress for a VPC and works together with the gateway in the on-premises data center.

   a. Create a VPC.

      Set the VPC CIDR block to 192.168.0.0/24. The CIDR block of the on-premises data center is 192.168.1.0/24.

      The CIDR block of an on-premises data center cannot overlap with the CIDR block of the VPC subnet. Otherwise, the communication between them will fail.

For details, see **Creating a VPC**.

b. Create a VPN gateway.

   VPC: Select the VPC created in **2.a**.

   Bandwidth: Select the bandwidth based on your service requirements.

   For details, see **Creating a VPN Gateway**.

c. Create a VPN connection.

   Local Subnet: Select subnets or manually enter CIDR blocks, for example, **192.168.0.0/24,198.19.0.0/16**.

   Remote Gateway: Set it to public IP address of the gateway in the data center.

   Remote Subnet: Set it to the CIDR block 192.168.1.0/24 of the data center.

   For details, see **Creating a VPN Connection**.

   NOTE

   After the IPv6 EIP function is enabled, the source IP address will be translated into one in the IP address range 198.19.0.0/16. Therefore, you need to enter the VPC subnet and then the IP address range 198.19.0.0/16 in sequence in the **Local Subnet** area.

d. Configure the VPN device in the data center.

   After configuring the VPN on the cloud, you need to configure the VPN device in the data center. For details, see **Virtual Private Network Administrator Guide**.

3. **Configure a public NAT gateway.**

   After purchasing a public NAT gateway, you can add DNAT rules to enable your servers in the VPC or servers in your data center that are connected to the VPC to provide internet-accessible services.

   a. Buy a public NAT gateway.

      VPC: Select the VPC created in **2.a**.

      Subnet: Select a subnet in the VPC created in **2.a**.

      For details, see **Buying a Public NAT Gateway**.

   b. Add a DNAT rule.

      Select the EIP purchased in **1** and add a DNAT rule based on the private IP address and port of the data center. For example, you can set **Port Type** to **Specific port**, **Protocol** to **TCP**, **Private IP Address** to **192.168.1.22**, and select the EIP to be associated.

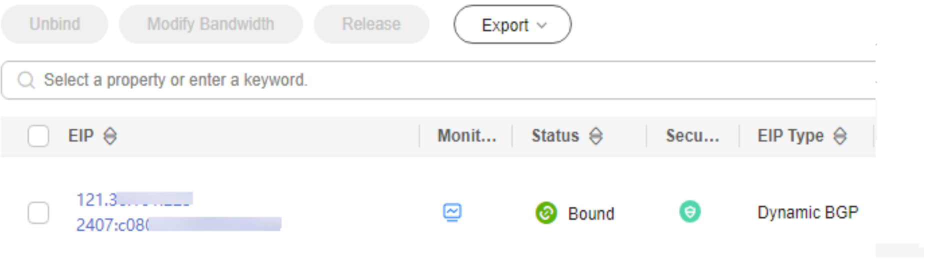
      For details, see **Adding a DNAT Rule**.

Verification

After the preceding operations are complete, the IPv6 EIPs can be used to provide internet-accessible services.

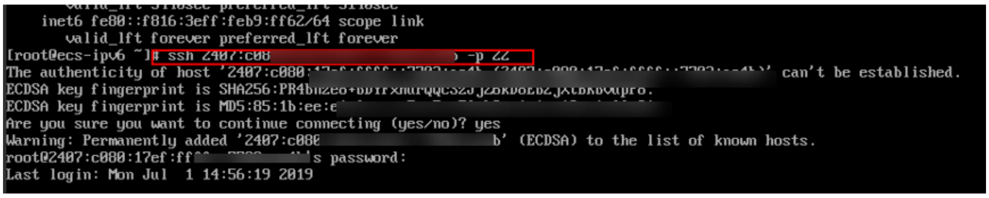
You can query the IPv6 addresses on the **EIPs** page.

Figure 3-2 IPv6 addresses



□	EIP	Monit...	Status	Secu...	EIP Type
□	121.3[redacted] 2407:c08[redacted]		Bound		Dynamic BGP

Use an IPv6 client that can access the internet to test the connectivity of the IPv6 EIP.



```
    inet6 fe80::f816:3eff:feb9:ff62/64 scope link
       valid_lft forever preferred_lft forever
[root@ecs-ipv6 ~]# ssh 2407:c08[redacted] -p 22
The authenticity of host '2407:c080:[redacted]' can't be established.
ECDSA key fingerprint is SHA256:PR4[redacted].
ECDSA key fingerprint is MD5:85:1b:ee:e[redacted]
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '2407:c080[redacted]b' (ECDSA) to the list of known hosts.
root@2407:c080:17ef:ff[redacted]'s password:
Last login: Mon Jul  1 14:56:19 2019
```

4 Changing an EIP for an ECS

4.1 Overview

Application Scenarios

You can bind an EIP to an ECS to enable the ECS to access the Internet. If you want to change an EIP for an ECS, you need to unbind the current EIP from the ECS first.

NOTE

- If there is no EIP, assign one.
- If you have released EIPs, 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, it is recommended that you buy another EIP first and then release the one that you do not want.

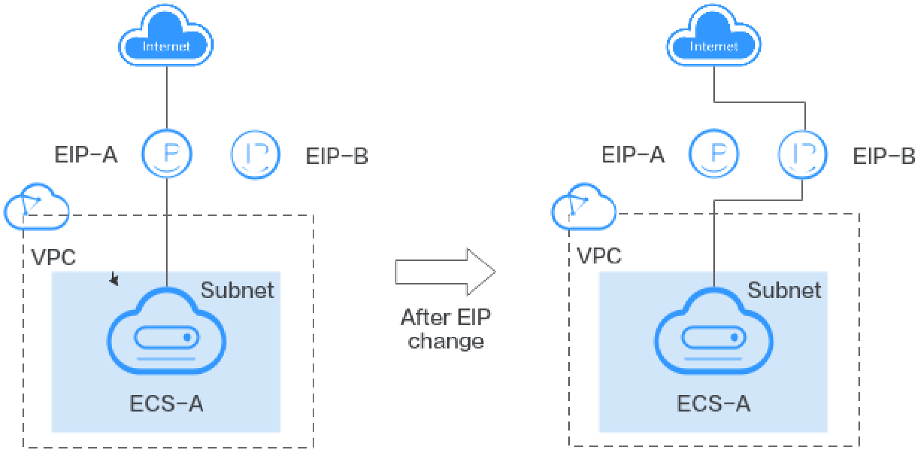
  For details, see **What Is the EIP Assignment Policy?**

Architecture

In this example, ECS-A, EIP-A, and EIP-B are in region A, and EIP-A is bound to ECS-A. To bind EIP-B to ECS-A, you need to:

1. Unbind EIP-A from ECS-A.
2. Bind EIP-B to ECS-A.

Figure 4-1 Changing EIP



Notes and Constraints

- Each EIP can be bound to only one cloud resource and they must be in the same region.
- An EIP and its bound cloud resource can use different billing modes.

  For example, a yearly/monthly EIP can be bound to a pay-per-use ECS.
- If you need to bind or unbind an EIP that is frozen due to account arrears or for security reasons, you need to unfreeze the EIP first. For details, see

4.2 Resource Planning

You need to plan resources before you change an EIP for an ECS. This example describes the resource planning details.

The VPC, EIPs, and ECS must be in the same region.

NOTE

The following resource planning details are only examples for your reference. You can modify them as required.

- One VPC. **Table 4-1** shows details about the required VPC.

Table 4-1 VPC details

VPC Name	VPC CIDR Block	Subnet Name	Subnet CIDR Block	Route Table
VPC	192.168.0.0/16	Subnet	192.168.1.0/24	Default route table

- One ECS. **Table 4-2** shows details about the required ECS.

Table 4-2 ECS details

ECS Name	Image	VPC Name	Subnet Name	Security Group	Private IP Address
ECS-A	Public image: EulerOS 2.5 64bit	VPC	Subnet	sg-demo: General-purpose web server	192.168.1.99

- Two EIPs. **Table 4-3** shows details about the required EIPs.

Table 4-3 EIP details

EIP Name	EIP Type	Bandwidth	Required Duration: 1 Month	EIP
EIP-A	Dynamic BGP	1 Mbit/s	Subnet-A	122.xx.xx.189
EIP-B	Dynamic BGP	5 Mbit/s	Subnet-A	122.xx.xx.166

4.3 Process Description

This section describes the process of changing an EIP for an ECS. For details, see **Table 4-4**.

Table 4-4 Process description

Procedure	Description
Unbinding an EIP	Unbind EIP-A from ECS-A.
Binding an EIP	On the **Bind EIP** page, bind EIP-B to ECS-A.
Releasing the EIP That Has Been Unbound	Unreleased EIPs will continue to be billed. If you do not need to use EIP-A, release it.

4.4 Procedure

Unbinding an EIP

Step 1 Log in to the management console.

Step 2 Click 📍 in the upper left corner and select your region and project.

Step 3 Locate the row that contains the ECS. Click **More** in the **Operation** column and choose **Manage Network** > **Unbind EIP**.

Step 4 Confirm the EIP information and click **Yes**.

----End

Binding an EIP

Step 1 Log in to the management console.

Step 2 Click 📍 in the upper left corner and select your region and project.

Step 3 Locate the row containing the target ECS. Click **More** in the **Operation** column and select **Manage Network** > **Bind EIP**.

Step 4 Select the desired EIP and click **OK**.

----End

Releasing the EIP That Has Been Unbound

An EIP that is not bound to any instance will continue to be billed. If you do not need the EIP any more, perform the following steps to release it:

Step 1 Log in to the management console.

Step 2 Click 📍 in the upper left corner and select the desired region and project.

Step 3 Click ☰ in the upper left corner and choose **Networking** > **Elastic IP**.

Step 4 In the EIP list, locate the row that contains the EIP to be released and choose **More** > **Release** in the **Operation** column.

A confirmation dialog box is displayed.

Step 5 Click **Yes** in the displayed dialog box.

You can find that the EIP is not in the EIP list.

----End

5 Binding a Premium BGP EIP to an ECS

5.1 Overview

Scenarios

Premium BGP provides fast and high-quality public network lines between Chinese mainland and the rest of the world. BGP is used to interconnect with lines of multiple mainstream carriers. Public network connections that feature low latency and high quality are directly established between Chinese mainland and CN-Hong Kong.

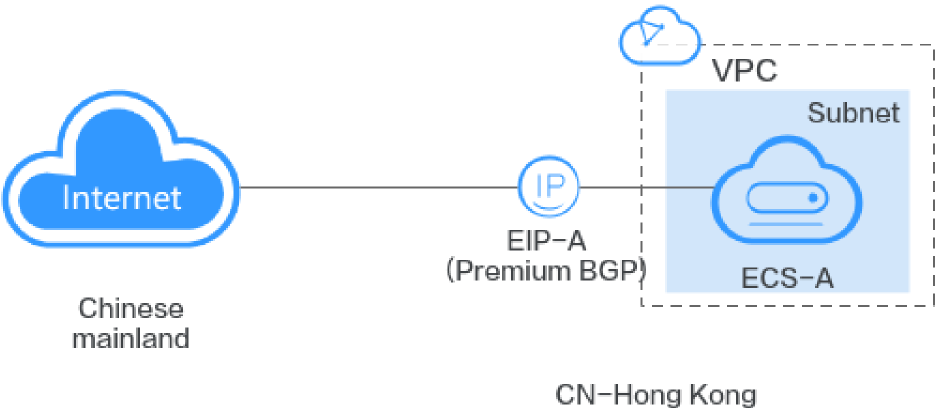
NOTE

- Premium BGP is available only in **CN-Hong Kong**.
- Premium EIPs can be billed on a yearly/monthly or pay-per-use basis.
- Premium BGP does not support shared data packages and bandwidth add-on packages.

Architecture

This document takes **Figure 5-1** as an example. Suppose you deploy your web application on an ECS in CN-Hong Kong and bind a premium BGP EIP to this ECS. And then users from the Chinese mainland can access your application faster through the optimal path.

Figure 5-1 Binding a premium BGP EIP to an ECS



In this example, ECS-A is deployed in CN-Hong Kong, and EIP-A is a premium BGP EIP in CN-Hong Kong. To bind EIP-A to ECS-A, you need to:

1. Assign premium BGP EIP-A.
2. Bind EIP-A to ECS-A.

Notes and Constraints

- Each EIP can be bound to only one cloud resource and they must be in the same region.
- An EIP and its bound cloud resource can use different billing modes.

  For example, a yearly/monthly EIP can be bound to a pay-per-use ECS.

5.2 Resource Planning

You need to plan resources before you bind a premium BGP EIP to an ECS. This example describes the resource planning details.

The VPC, EIP, and ECS must be in the same region.

NOTE

The following resource planning details are only examples for your reference. You can modify them as required.

- One VPC. **Table 5-1** shows details about the required VPC.

Table 5-1 VPC details

VPC Name	VPC CIDR Block	Subnet Name	Subnet CIDR Block	Route Table
VPC	192.168.0.0/16	Subnet	192.168.1.0/24	Default route table

- One ECS. For details, see **Table 5-2**.

Table 5-2 ECS details

ECS Name	Image	VPC Name	Subnet Name	Security Group	Private IP Address
ECS-A	Public image: EulerOS 2.5 64bit	VPC	Subnet	sg-demo: General-purpose web server	192.168.1.99

- One EIP. **Table 5-3** shows details about the required EIP.

Table 5-3 EIP details

EIP Name	EIP Type	Bandwidth	Required Duration	EIP
EIP-A	Premium BGP	1 Mbit/s	1 Month	122.xx.xx.189

5.3 Process Description

This section describes the process of binding a premium BGP EIP to an ECS. For details, see **Table 5-4**.

Table 5-4 Process description

Procedure	Description
Assigning a premium BGP EIP	Assign premium BGP EIP-A.
Binding EIP-A to ECS-A	Bind EIP-A to ECS-A.

5.4 Procedure

Assigning a premium BGP EIP

Step 1 Log in to the management console.

Step 2 Click 📍 in the upper left corner and select your region and project.

Step 3 Click ☰ in the upper left corner, and choose **Networking** > EIP.

Step 4 On the displayed page, click **Buy EIP**.

Step 5 Configure parameters as prompted.

The values in **Table 5-5** are only examples for your reference. You can modify them as required.

Table 5-5 Parameter descriptions

Parameter	Description	Example Value
Billing Mode	The following billing modes are available: ● Yearly/Monthly ● Pay-per-use	Yearly/Monthly
Region	The region where your EIP is deployed. In this example, select CN-Hong Kong.	CN-Hong Kong
EIP Type	Premium BGP **NOTE** Premium BGP is available only in **CN-Hong Kong**.	Premium BGP
Bandwidth	The bandwidth size in Mbit/s.	1
DDoS Protection	Cloud Native Anti-DDoS Basic Cloud Native Anti-DDoS Basic provides up to 5 Gbit/s of DDoS mitigation capacity. If the attack to an EIP exceeds 5 Gbit/s, the EIP will be blocked.	-
EIP Name	The EIP name.	EIP-A
Enterprise Project	The enterprise project that the EIP belongs to. An enterprise project lets you manage cloud resources and personnel by enterprise project. The default project is **default**. For details about creating and managing enterprise projects, see the **Enterprise Management User Guide**.	default
Advanced Settings	Click the drop-down arrow to configure parameters, including the bandwidth name and tag.	-
Bandwidth Name	The name of the bandwidth.	bandwidth
Tag	The EIP tags. Each tag contains a key and value pair. **NOTE** If your organization has created a tag policy for EIP, you need to add tags for EIP based on the tag policy. If a tag does not comply with the tag rules, the creation may fail. Contact the organization administrator to learn details about the tag policy.	● Key: Ipv4_key1 ● Value: 3005eip

Parameter	Description	Example Value
Monitoring	Used to monitor the EIP and enabled by default. You can use the management console or call APIs provided by Cloud Eye to query the metrics and alarms generated for the EIP and bandwidth.	-
Required Duration	How long you will use your EIP. The duration must be specified if the **Billing Mode** is set to **Yearly/Monthly**.	1 Month

Step 6 Click **Next**.

Step 7 Confirm the information and click **Pay Now**.

Step 8 Confirm the order and click **Pay**.

----End

Binding EIP-A to ECS-A

Step 1 In the EIP list, locate EIP-A, and click **Bind** in the **Operation** column.

Step 2 Select ECS-A and bind EIP-A to it.

NOTE

If ECS-A has an EIP bound to it, unbind the EIP from ECS-A first.

Step 3 Click **OK**.

----End

Related Operations

- **How Do I Assign or Retrieve a Specific EIP?**
- **Can Multiple EIPs Be Bound to an ECS?**
- **How Do I Access an ECS with an EIP Bound from the Internet?**
- **Why Can't My ECS Access the Internet Even After an EIP Is Bound?**