Virtual Private Cloud

FAQs

Date 2019-12-23
1 General.......................................................................................................................................1
1.1 What Is a Quota?.................................................................................................................................................................... 1
1.2 How Do I Change the Billing Mode?................................................................................................................................2
1.3 How Do I Change the Bandwidth Billing Option from Bandwidth to Traffic or from Traffic to Bandwidth?..................................................................................................................................................................................... 4
2 VPC and Subnet....................................................................................................................... 5
2.1 What Is Virtual Private Cloud?............................................................................................................................................5
2.2 Will I Be Charged for Using the VPC Service?............................................................................................................... 6
2.3 Which CIDR Blocks Are Available to the VPC Service?...............................................................................................6
2.4 How Many VPCs Can I Create?...........................................................................................................................................6
2.5 Can Subnets Communicate with Each Other?.............................................................................................................. 6
2.6 What Subnet CIDR Blocks Are Available?.......................................................................................................................6
2.7 Can I Modify the CIDR Block of a Subnet?.....................................................................................................................6
2.8 How Many Subnets Can I Create?.....................................................................................................................................6
2.9 What Do I Do If a Subnet Cannot Be Deleted Because It Is Being Used by Other Resources?................... 7
3 EIP................................................................................................................................................8
3.1 How Do I Assign or Retrieve a Specific EIP?.................................................................................................................. 8
3.2 What Are the Differences Between an EIP, a Private IP Address, a Floating IP Address, and a Virtual IP Address?............................................................................................................................................................................................. 8
3.3 How Do I Access the Internet Using the EIP Bound to the Extension NIC?........................................................................9
3.4 What Are the Differences Between the Primary and Extension NICs of ECSs?.................................................................10
3.5 What Are EIPs?...................................................................................................................................................................... 10
3.6 Can an EIP That Uses Dedicated Bandwidth Be Changed to Use Shared Bandwidth?............................................ 11
3.7 How Many ECSSs Can One EIP Be Assigned to?.............................................................................................................11
3.8 How Can I Access an ECS from Another Security Group After an EIP Is Bound to the ECS?...............................11
3.9 What Is the EIP Assignment Policy?............................................................................................................................... 12
3.10 Can I Change the ECS Bound to an EIP?.............................................................................................................................12
3.11 Will the EIP Bound to an ECS Be Changed After the ECS Is Stopped and Then Started?.....................................12
4 Bandwidth...............................................................................................................................................13
4.1 What Is the Inbound Bandwidth and Outbound Bandwidth?.......................................................................................13
4.2 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?.................................................................................................................................14
4.3 How Do I Check Whether the Bandwidth Exceeds the Limit?.....................................................................................14
5 Connectivity ............................................................................................................................ 19
4.10 What Are the

4.9 What Is the Relationship Between Bandwidth and Upload/Download Rate?.................................................17
4.8 Can I Increase My Yearly/Monthly Bandwidth Size and Then Decrease It?..................................................... 17
4.7 How Many EIPs Can Use the Same Shared Bandwidth?........................................................................................ 17
4.6 How Can I Use Shared Bandwidth?................................................................................................................................17
4.5 What Bandwidth Types Does the VPC Service Support?.........................................................................................16
4.4 What Is the Bandwidth Size Range?.................................................................................................................................................. 16
4.3 Can I Check My Bandwidth Use in the Console?......................................................................................................................... 16
4.2 What Are the Bandwidth Resource Types?............................................................................................................................... 16
4.1 How Do I Check My Bandwidth Use?.................................................................................................................................15
3.9 What Are the Limitations of VPC Peering?.............................................................................................................................. 20
3.8 How Many Routes Can Be Added in a VPC?............................................................................................................................. 51
3.7 Are There

3.6 Will a Route Table be Billed?............................................................................................................................................ 50
3.5 How Many Routes Can Exist in a Route Table?.................................................................................................................... 50
3.4 Can a Route Table Span Multiple VPCs?................................................................................................................................. 50
3.3 How Do I Configure Policy-Based Routing for ECSs with Multiple NICs?................................................................. 48
3.2 Can a Route Table Span Multiple VPCs?................................................................................................................................. 48
3.1 How Do I Configure Policy-Based Routing for ECSs with Multiple NICs?................................................................. 48
2.10 How Do I Set Up a VPC Peering Connection with a Private Network?.................................................................................. 2
2.9 How Do I Set Up a VPC Peering Connection with a Public Network?..................................................................................... 2
2.8 How Do I Set Up a VPC Peering Connection with an External Network?.................................................................................. 2
2.7 How Do I Set Up a VPC Peering Connection?.......................................................................................................................... 2
2.6 How Do I Create a VPC Peering Connection?.......................................................................................................................... 2
2.5 How Do I Create a VPC Peering Connection?.......................................................................................................................... 2
2.4 Does a VPC Allow for Communication Between Two VPCs?......................................................................................... 19
2.3 Why Cannot I Access Public Websites Through Domain Names or Access Internal Domain Names in the Cloud When My ECS Has Multiple NICs?.................................................................................................................. 19
2.2 What Are the Limitations of VPC Peering?............................................................................................................................ 19
2.1 Why Cannot I Access Public Websites Through Domain Names or Access Internal Domain Names in the Cloud When My ECS Has Multiple NICs?.................................................................................................................. 19
1.10 How Many Cloud-init Connections Can Be Configured for an ECS?...................................................................................... 29
1.9 What Do I Do If a Virtual IP Address Cannot Be Pinged After Being Bound to an ECS NIC?..................25
1.8 What Do I Do If ECSs Using Private IP Addresses in the Same Subnet Only Support One-Way Communication?.......................................................................................................................................................................... 22
1.7 What Do I Do If Two ECSs in the Same VPC Cannot Communicate with Each Other or Packet Loss Occurs During the Communication Between the Two ECSs?.................................................................................... 23
1.6 What Do I Do If Two ECSs in the Same VPC Cannot Communicate with Each Other or Packet Loss Occurs During the Communication Between the Two ECSs?.................................................................................... 23
1.5 What Do I Do If a Virtual IP Address Cannot Be Pinged After Being Bound to an ECS NIC?..............25
1.4 What Do I Do If Two ECSs in the Same VPC Cannot Communicate with Each Other or Packet Loss Occurs During the Communication Between the Two ECSs?.................................................................................... 23
1.3 What Do I Do If Two ECSs in the Same VPC Cannot Communicate with Each Other or Packet Loss Occurs During the Communication Between the Two ECSs?.................................................................................... 23
1.2 What Do I Do If Two ECSs in the Same VPC Cannot Communicate with Each Other or Packet Loss Occurs During the Communication Between the Two ECSs?.................................................................................... 23
1.1 What Do I Do If Two ECSs in the Same VPC Cannot Communicate with Each Other or Packet Loss Occurs During the Communication Between the Two ECSs?.................................................................................... 23

1.1 What Is a Quota?

Quotas prevent unforeseen spikes in resource usage. Quotas can limit the number or amount of resources available to users. For example, a VPC quota limits the number of VPCs that you can create.

You can also request more quotas if the existing resource quotas 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, click Increase Quota to adjust it.
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.
4. On the Create Service Ticket page, configure parameters as required. In 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 Tenant Authorization Letter and Privacy Statement and click Submit.

1.2 How Do I Change the Billing Mode?

Changing the Billing Mode from Pay-per-Use to Yearly/Monthly

You can change the billing mode of pay-per-use EIPs and shared bandwidth billed by bandwidth to yearly/monthly. After the change is successful, the new billing mode takes effect immediately.

You can change the billing mode on the related service page or in the billing center. The following operations describe how to change the billing mode of EIPs from pay-per-use to yearly/monthly.

NOTE

The billing mode of a pay-per-use EIP billed by traffic cannot be directly changed to yearly/monthly. You must first change the pay-per-use EIP to be billed by bandwidth and then change its billing mode to yearly/monthly.

1. Log in to the management console.
2. Under Network, click Elastic IP.
3. On the displayed page, search for the pay-per-use EIP whose billing mode is to be changed.
4. Locate the row that contains the target EIP and click Change Billing Mode in the Operation column.
Figure 1-3 Changing the billing mode on the service page

5. Click Yes.

Figure 1-4 Setting specifications

7. Click Submit and Pay.
   You can also select multiple EIPs and click Change Billing Mode above the EIP list to change their billing modes at one time.

Changing the Billing Mode from Yearly/Monthly to Pay-per-Use

The billing mode of yearly/monthly EIPs and shared bandwidth can be changed to pay-per-use. The new billing mode takes effect only when the yearly/monthly mode expires.

You can change the billing mode from yearly/monthly to pay-per-use in the billing center. The following operations describe how to change the billing mode of EIPs from yearly/monthly to pay-per-use:

1. Log in to the management console.
2. Choose Fees > Renewal.
3. In the search box on the right, search for the EIP whose billing mode needs to be changed.

4. Locate the row that contains the target EIP and click **Change to Pay-per-Use** in the **Operation** column.

5. Click **Change to Pay-per-Use**.

### NOTE

Changing the EIP billing mode does not change the EIP.

#### 1.3 How Do I Change the Bandwidth Billing Option from Bandwidth to Traffic or from Traffic to Bandwidth?

- The billing option can be changed only when the billing mode is **Yearly/Monthly**. For details, see **Modifying EIP Bandwidth**.
- A yearly/monthly resource can only be billed by bandwidth.
2.1 What Is Virtual Private Cloud?

The Virtual Private Cloud (VPC) service enables you to provision logically isolated, configurable, and manageable virtual networks for cloud servers, cloud containers, and cloud databases, improving cloud service security and simplifying network deployment.

You can create security groups and VPNs, configure IP address ranges, and specify bandwidth sizes in your VPC. With a VPC, you can configure and manage the networks within the VPC, making changes to these networks as needed, quickly and securely. You can also define rules for communication between ECSs in the same security group or in different security groups.

Figure 2-1 Product Architecture
2.2 Will I Be Charged for Using the VPC Service?

The VPC service is free of charge itself. However, you are charged for the bandwidth or VPN used in the VPC.

2.3 Which CIDR Blocks Are Available to the VPC Service?

The VPC service supports the following CIDR blocks:

- 10.0.0.0 – 10.255.255.255
- 172.16.0.0 – 172.31.255.255
- 192.168.0.0 – 192.168.255.255

2.4 How Many VPCs Can I Create?

By default, a user can create a maximum of five VPCs. If your quota cannot fulfill your service requirements, submit a work order for capacity expansion.

2.5 Can Subnets Communicate with Each Other?

Subnets belong to VPCs. Subnets in the same VPC can communicate with each other. Subnets in different VPCs cannot communicate with each other by default. However, you can create VPC peering connections to enable subnets in different VPCs to communicate with each other.

2.6 What Subnet CIDR Blocks Are Available?

The subnet CIDR blocks must be included in the VPC CIDR blocks. The VPC CIDR blocks are 10.0.0.0/8–24, 172.16.0.0/12–24, and 192.168.0.0/16–24. The subnet CIDR blocks must be within these CIDR blocks, and the allowed block size of a subnet is between the netmask of its VPC CIDR block and /28 netmask.

2.7 Can I Modify the CIDR Block of a Subnet?

The subnet CIDR block cannot be modified after a subnet is created.

2.8 How Many Subnets Can I Create?

By default, one tenant can create a maximum of 100 subnets. If the number of subnets does not meet your service requirements, submit a service ticket to increase the quota.
2.9 What Do I Do If a Subnet Cannot Be Deleted Because It Is Being Used by Other Resources?

The VPC service allows you to create private, isolated virtual networks. In a VPC, you can manage private IP address ranges, subnets, and network gateways. ECSs, BMSs, databases, and some other applications use secure networks created in VPCs.

Subnets in a VPC cannot be deleted if the subnets are used by the following resources:

- ECS
- CCI instance
- Elastic load balancer
- VPN
- Private IP address
- Custom route
- NAT gateway

Check whether the subnet is used by the preceding resources. If yes, delete all resources in the subnet and delete the subnet.
3.1 How Do I Assign or Retrieve a Specific EIP?

If you want to retrieve a released EIP or assign a specific EIP, you can use APIs. When assigning an EIP, set the value of `ip_address` to the IP address that you want to retrieve or assign. For details, see Elastic IP API Reference. For details, see Elastic IP API Reference.

**NOTE**
- If the EIP has been assigned to another user, the application fails.
- The management console does not support retrieving or assigning a specific EIP.

3.2 What Are the Differences Between an EIP, a Private IP Address, a Floating IP Address, and a Virtual IP Address?

An EIP is an IP address that can be directly accessed over the Internet. Each EIP can be used by only one ECS at a time.

A private IP address is used by the internal network of the public cloud for internal communications. It cannot be accessed over the Internet.

A floating IP address functions similar to an EIP. They are both public IP addresses that are used to connect to the Internet, but a floating IP address API cannot be used to configure bandwidth parameters. For details, see Floating IP Address.

A virtual IP address is not allocated to an actual ECS NIC. A virtual IP address is used for active/standby switchover of ECSs to for higher availability. If the active ECS becomes faulty and cannot provide services, the virtual IP address is dynamically re-assigned to the standby ECS so services can continue uninterrupted. For details, see Virtual IP Address Overview.
3.3 How Do I Access the Internet Using the EIP Bound to the Extension NIC?

1. After an EIP is bound to an extension NIC, log in to the ECS and run the `route` command to query the route. You can run `route --help` to learn more about the `route` command.

   ![Viewing route information](image1)

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

   ![Viewing NIC information](image2)

3. Configure the NIC to 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 0.0.0.0 192.168.11.1 dev eth0
      ```
This operation will interrupt ECS communication. Exercise caution when performing this operation. 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 network segment (for example, xx.xx.0.0/16) through the extension NIC:

You can configure the network segment as required.

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

### 3.4 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.
- By default, only the primary NICs can communicate with the public service zone (zone where PaaS and DNS services are deployed). The extension NICs cannot communicate this zone.

### 3.5 What Are EIPs?

An EIP is a public IP address that can be accessed directly over the Internet. An EIP consists of a public IP address and some amount of public network egress bandwidth. EIPs can be bound to or unbound from ECSs, BMSs, virtual IP addresses, NAT gateways, and load balancers.

Each EIP can be used by only one cloud resource at a time.
3.6 Can an EIP That Uses Dedicated Bandwidth Be Changed to Use Shared Bandwidth?

No. An EIP that uses the dedicated bandwidth cannot be changed to use shared bandwidth.

In addition, an EIP that uses the shared bandwidth cannot be changed to use the dedicated bandwidth.

3.7 How Many ECSs Can One EIP Be Assigned to?

Each EIP can be used by only one ECS at a time.

3.8 How Can I Access an ECS from Another Security Group After an EIP Is Bound to the ECS?

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 the Linux OS and TCP traffic from port 3389 through RDP to the Windows OS). 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 the ECS needs to be accessible over the Internet and the IP address used to access the ECS over the Internet has been configured on the ECS, or the ECS does not need to be accessible over the Internet, set Source to the IP address range containing the IP address that is allowed to access the ECS over the Internet.
If the ECS needs to be accessible over the Internet and the IP address used to access the ECS over the Internet has not been configured on the ECS, it is recommended that you retain the default setting 0.0.0.0/0 for Source, and then set Port Range to improve network security.

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

### NOTE

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

### 3.9 What Is the EIP Assignment Policy?

By default, an EIP is assigned randomly. If you used to release EIPs, the system preferentially assigns an EIP from what you used.

### 3.10 Can I Change the ECS Bound to an EIP?

Yes.

You can unbind the EIP from the original ECS. For details, see [Binding or Releasing an EIP](#).

Then, bind the EIP to the target ECS. For details, see [Binding an EIP to Cloud Resources](#).

### 3.11 Will the EIP Bound to an ECS Be Changed After the ECS Is Stopped and Then Started?

The EIP will not be changed.

Stopping and starting an ECS does not affect its EIP.
4.1 What Is the Inbound Bandwidth and Outbound Bandwidth?

Inbound bandwidth: specifies the bandwidth from the Internet to the HUAWEI CLOUD. For example, download resources from the Internet to ECSs in the cloud.

Outbound bandwidth: specifies the bandwidth from the HUAWEI CLOUD to the Internet. For example, the ECSs in the cloud provide services accessible from the Internet and external users can download resources from the ECSs in the cloud.

Figure 4-1 Inbound bandwidth and outbound bandwidth

HUAWEI CLOUD only bills for the outbound bandwidth. If the bandwidth in the outbound direction is less than 100 Mbit/s, the bandwidth in the inbound direction is 100 Mbit/s. If the bandwidth in the outbound direction is greater than 100 Mbit/s, the bandwidth in the inbound direction is the same as that in the outbound direction.

NOTE

If the enhanced 95th percentile bandwidth billing is used, the bandwidth is billed based on the average bandwidth in the inbound and outbound directions.
4.2 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?

Dedicated bandwidth: The bandwidth will be used by one EIP only and the EIP can be used by only one cloud resource, such as ECS and NAT gateway.

Shared bandwidth: The bandwidth will be shared by multiple EIPs. You can add multiple pay-per-use EIPs to the bandwidth. Adding an EIP to or removing an EIP from a shared bandwidth does not affect service running.

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

- After an EIP is added to a shared bandwidth, the EIP uses the shared bandwidth.
- After an EIP is removed from the shared bandwidth, the EIP uses the dedicated bandwidth.

4.3 How Do I Check Whether the Bandwidth Exceeds the Limit?

Symptom

The bandwidth size configured when buying a dedicated or shared bandwidth is the upper limit of the outbound bandwidth. If the web applications that depend on the Internet freeze, check whether the dedicated bandwidth of the EIP bound to the ECS is greater than the configured bandwidth size.

- **NOTE**
  
  If the bandwidth exceeds the configured bandwidth size, packet loss may occur. To ensure normal service running, you are advised to monitor the bandwidth.

Troubleshooting Method 1

Query the historical dedicated bandwidth usage of an EIP.

1. Log in to the management console and view the EIP bound to the ECS.

*Figure 4-2 Viewing the EIP*
2. On the **Cloud Eye** console, click **Event Monitoring**.

![Event Monitoring](image1)

3. Click **View Event**.

![View Event](image2)

If the event **EIP bandwidth overflow** is not displayed, the dedicated bandwidth of the EIP does not exceed the limit. In this case, check other causes.

If the event **EIP bandwidth overflow** is displayed, the dedicated bandwidth of the EIP has exceeded the limit. To ensure stable service running, increase the bandwidth. For details, see [Modifying EIP Bandwidth](#).

**NOTE**

Cloud Eye does not support the display of the shared bandwidth limit details on the **Event Monitoring** page.

**Troubleshooting Method 2**

Create an alarm rule to generate alarms when the bandwidth exceeds the limit.

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 limit.

When the actual bandwidth exceeds the limit, an alarm is generated and the system automatically sends a notification.

The basic alarm function is free of charge. Simple Message Notification (SMN) sends you the alarm messages and bills you for that.

### 4.4 What Is the Bandwidth Size Range?

The bandwidth size ranges from 1 Mbit/s to 2000 Mbit/s.

### 4.5 What Bandwidth Types Does the VPC Service Support?

The VPC service supports the dedicated bandwidth and shared bandwidth. The dedicated bandwidth can be used by only one EIP, whereas the shared bandwidth can be shared by multiple EIPs.
4.6 How Can I Use Shared Bandwidth?

1. Log in to the management console.
2. On the console homepage, under Network, click Virtual Private Cloud.
3. In the navigation pane on the left, choose Elastic IP and Bandwidth > Shared Bandwidths.
4. In the upper right corner, click Buy Shared Bandwidth. On the displayed page, configure parameters as prompted to buy a shared bandwidth.

4.7 How Many EIPs Can Use the Same Shared Bandwidth?

A shared bandwidth can be used by up to 20 EIPs. If the number of EIPs cannot meet your requirements, you can submit a service ticket to request to increase the quota.

4.8 Can I Increase My Yearly/Monthly Bandwidth Size and Then Decrease It?

The increased bandwidth size takes effect immediately. The decreased bandwidth size takes effect in the subsequent billing cycle after a successful renewal. For details, see Modifying EIP Bandwidth.

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

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

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

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) in consideration of losses, such as computer performance, network device quality, resource usage, and network peak hours.

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

The differences between static BGP and dynamic BGP are as follows:
### Table 4-1 Differences between static BGP and dynamic BGP

<table>
<thead>
<tr>
<th>Aspect</th>
<th>Static BGP</th>
<th>Dynamic BGP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Definition</td>
<td>Routes are manually configured by carriers. If the network topology or link status changes, carriers must manually modify static routes in the route table.</td>
<td>When changes occur on a network using dynamic BGP, routing protocols provide automatic, real-time optimization of network configurations, ensuring network stability and optimal user experience.</td>
</tr>
</tbody>
</table>
| Assurance    | When changes occur on a network using dynamic BGP, carriers cannot adjust network configurations in real time to ensure optimal user experience.  
**NOTE** If you select static BGP, your application system must have the disaster recovery capability. | The multi-path BGP can detect the status of the access line and carrier's internal networks. When an internal fault occurs on the carrier network, another network will take over services quickly to ensure service availability. |
| Service availability | 99%                                                                 | 99.95%                                                                   |

**NOTE**

For more information about service availability, see [Huawei Cloud Service Level Agreement](#).
5.1 Does a VPN Allow for Communication Between Two VPCs?

If the two VPCs are in the same region, you can use a VPC peering connection to enable communication between them.

If the two VPCs are in different regions, you can use a VPN to enable communication between the VPCs. The CIDR blocks of the two VPCs are the local and remote subnets, respectively.

5.2 Why Cannot I Access Public Websites Through Domain Names or Access Internal Domain Names in the Cloud When My ECS Has Multiple NICs?

When an ECS has more than one NIC, if different DNS server addresses are configured for the subnets used by the NICs, the ECS cannot access public websites or internal domain names in the cloud.

You can rectify this fault by configuring the same DNS server address for the subnets used by the same ECS. You can perform the following steps to modify DNS server addresses of subnets in a VPC:

1. Log in to the management console.
2. On the console homepage, under Network, click Virtual Private Cloud.
3. In the navigation pane on the left, click Virtual Private Cloud.
4. On the Virtual Private Cloud page, locate the VPC for which a subnet is to be modified and click the VPC name.
5. In the subnet list, locate the row that contains the subnet to be modified, click Modify. On the displayed page, change the DNS server address as prompted.
6. Click OK.
5.3 What Are the Limitations of VPC Peering?

- VPC peering connections created between VPCs that have overlapping subnet CIDR blocks may not take effect.
- You cannot have more than one VPC peering connection between the same two VPCs at the same time.
- You cannot create a VPC peering connection between VPCs in different regions.
- You cannot use the EIPs in a VPC of a VPC peering connection to access resources in the other VPC. For example, VPC A is peered with VPC B, VPC B has EIPs that can be used to access the Internet, you cannot use EIPs in VPC B to access the Internet from VPC A.
- To request a VPC peering connection with a VPC of another tenant, the peer tenant must accept the request to activate the connection. If you request a VPC peering connection with a VPC of your own, the system automatically accepts the request to activate the connection.
- After a VPC peering connection is established, the local and peer tenants must add routes in the local and peer VPCs to enable communication between the two VPCs.
- VPC A is peered with both VPC B and VPC C. If VPC B and VPC C have overlapping CIDR blocks, routes with the same destinations cannot be added in VPC A.
- To ensure security, do not accept VPC peering connections from unknown tenants.
- Either owner of a VPC in a peering connection can delete the VPC peering connection at any time. If a VPC peering connection is deleted by one of its owners, all information about this connection will be automatically deleted immediately, including routes added for the VPC peering connection.
- Currently, the route table of a VPC takes effect for all subnets in the VPC. You cannot add a route table dedicated for a specific subnet. The route preference is as follows: direct route > VPC peering connection route > custom route.
- If two VPCs in a VPC peering connection have overlapping CIDR blocks, the peering connection can only enable communication between two subnets in the two VPCs. If subnets in the two VPCs of a VPC peering connection have overlapping CIDR blocks, the peering connection does not take effect. To create a VPC peering connection, ensure that the two VPCs involved do not contain overlapping subnets.
- You cannot delete a VPC for which VPC peering connection routes have been configured.

5.4 What Can I Do If VPCs in a VPC Peering Connection Cannot Communicate with Each Other?

1. Check whether a VPC peering connection has been successfully created for the two VPCs. Confirm the IDs of the VPCs in the VPC peering connection.
2. Check whether routes that point to the CIDR block (or portion of the CIDR block) of the other VPC have been configured.

3. Check whether routes configured for the VPC peering connection are correct. If VPCs in a VPC peering connections have overlapping CIDR blocks, you can only add routes to enable communication between two subnets in the two VPCs.

4. Check whether the VPCs in the VPC peering connection contain overlapping subnets.

5. Check whether required security group rules have been configured for the ECSs that need to communicate with each other and whether restriction rules have been added to the iptables or firewall used by the ECSs.

6. If a message indicating that this route already exists is displayed when you add routes for a VPC peering connection, check whether the route’s destination IP addresses of the VPN, Direct Connect, and VPC peering connections already exist.

7. If the route’s destination IP addresses of a VPC peering connection overlap with those of a Direct Connect or VPN connection, the route may be invalid.

8. If VPCs in a VPC peering connection cannot communicate with each other after all these possible faults have been rectified, contact customer service.

5.5 How Many VPC Peering Connections Can I Have?

A tenant can have a maximum of 50 VPC peering connections in one region. Accepted VPC peering connections consume the quota of both owners of a VPC peering connection. A VPC peering connection consumes the quota of only the requester (tenant of the local VPC).

5.6 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.

5.7 What Do I Do If Intermittent Interruption Occurs When a Local Host Accesses a Website Built on an ECS?

After a website is built on an ECS, some users occasionally fail to access the website through the local network.

Fault Locating

1. Check the local network of the user.
   If the local host communicates with the ECS using NAT, this problem may occur.

2. Run the following command to check whether `tcp_tw_recycle` is enabled on the ECS:
sysctl -a | grep tcp_tw_recycle
The value of tcp_tw_recycle is 1, indicating the function is enabled.

3. Run the following command to check the number of lost packets of the ECS:
   cat /proc/net/netstat | awk '/TcpExt/ { print $21,$22 }'
   If the value of ListenDrops is not 0, packet loss occurs, that is, the network is faulty.

Troubleshooting Procedure
This problem can be solved by modifying the kernel parameters of the ECS.
- Run the following command to temporarily modifying the parameters (the modification becomes invalid after the ECS is restarted):
  sysctl -w net.ipv4.tcp_tw_recycle=0
- Perform the following operations to permanently modify the parameters:
  a. Run the following command and modify the /etc/sysctl.conf file:
     vi /etc/sysctl.conf
     Add the following content to the file:
     net.ipv4.tcp_tw_recycle=0
  b. Press Esc, enter :wq!, and save the file and exit.
  c. Run the following command to make the modification take effect:
     sysctl -p

5.8 What Do I Do If ECSs Using Private IP Addresses in the Same Subnet Only Support One-Way Communication?

Symptom
Two ECSs (ecs01 and ecs02) are in the same subnet in a VPC. Their IP addresses are 192.168.1.141 and 192.168.1.40, respectively.

The ECS ecs02 private IP address can be pinged from ECS ecs01, but ECS ecs01 private IP address cannot be pinged from ECS ecs02.

Fault Locating
1. Ping ECS ecs01 from ECS ecs02 through the EIP. If ECS ecs01 can be pinged, the NIC of ECS ecs01 is working properly.
2. Run the arp -n command on ECS ecs02 to check whether the command output contains the MAC address of ECS ecs01. If the command output does not contain the MAC address of ECS ecs01, the ECS ecs02 fails to learn the ECS ecs01 MAC address when using the private IP address to ping ECS ecs01.
3. Run the ip a command on ecs01 to check the NIC configuration of ECS ecs01. The following figure shows an example.
The IP address 192.168.1.40/32 should not be configured based on the command output. As a result, ECS ecs01 fails to send packets to ECS ecs02.

Troubleshooting Procedure

Modify the NIC configuration of ECS ecs01. Run the following command to delete the redundant IP address, for example, 192.168.1.40/32, configured on the NIC eth0:

```
ip a del 192.168.1.40/32 dev eth0
```

5.9 What Do I Do If Two ECSs in the Same VPC Cannot Communicate with Each Other or Packet Loss Occurs During the Communication Between the Two ECSs?

Fault Locating

1. Check security group rules.
2. Check network ACLs.
3. Check the NIC information of ECSs.
4. Check the disconnected ports.

Troubleshooting Procedure

1. Check security group rules.
   
   Check whether the ECS NIC security group allows the outbound and inbound Internet Control Message Protocol (ICMP) traffic.
   
   Take the inbound direction as an example. The security group rules must contain any of the following rules.

Figure 5-2 Inbound security group rule
If packets of other protocols are tested, configure the security group rules to allow the corresponding protocol traffic. For example, if UDP packets are tested, check whether the security group allows the inbound UDP traffic.

2. Check network ACLs.
   a. Check whether the ECS NIC is in the associated subnet of the network ACL.
   b. Check the network ACL status in the network ACL list.
      - If Disable is displayed in the Operation column, the network ACL has been enabled. Go to 2.c.
      - If Enable is displayed in the Operation column, the network ACL has been disabled. Go to 2.d.
   c. Click the network ACL name and configure rules on the Inbound and Outbound tabs to allow the ICMP traffic.
   d. When the network ACL is disabled, all packets in the inbound and outbound directions are discarded by default. In this case, delete the network ACL or enable the network ACL and allow the ICMP traffic.

3. Check the NIC information of the ECS. (The following procedure uses a Linux ECS as an example. For a Windows ECS, check the firewall restrictions.)
   a. Check whether multiple NICs are configured for the ECS. If the ECS has multiple NICs and the EIP is bound to an extension NIC, configure policy-based routing for the ECS. For details, see 6.1 How Do I Configure Policy-Based Routing for ECSs with Multiple NICs?
   b. Log in to the ECS and run the following command to check whether the NIC has been created and obtained a private IP address. If there is no NIC information or the private IP address cannot be obtained, contact technical support.
      `ifconfig`

   [Figure 5-3 NIC IP address]

   c. Run the following command to check whether the CPU usage of the ECS is too high. If the CPU usage exceeds 80%, the ECS communication may be adversely affected.
      `top`
   d. Run the following command to check whether the ECS has any restrictions on security group rules:
      `iptables-save`
   e. Run the following command to check whether the `/etc/hosts.deny` file contains the IP addresses that limit communication:
      `vi /etc/hosts.deny`
If the `hosts.deny` file contains the IP address of another ECS, delete the IP address from the `hosts.deny` file and save the file.

4. Check the disconnected ports.
   a. If the special port of the ECS cannot be accessed, check whether the security group rules and network ACL rules enable the port.
   b. On the Linux ECS, run the following command to check whether the ECS listens to the port: If the port is not listened, the ECS communication may be adversely affected.

```
netstat -na | grep <Port number>
```

5.10 What Do I Do If a Virtual IP Address Cannot Be Pinged After Being Bound to an ECS NIC?

**Fault Locating**

1. Check whether the source/destination check function of the NIC is disabled and whether the virtual IP address has been bound to the NIC.
2. Check whether the ECS NIC subinterfaces are successfully created.
3. Check whether the ECS security groups and the network ACL rules associated with the subnets used by the ECS NICs block traffic.

**Troubleshooting Procedure**

1. Check whether the source/destination check function of the NIC is disabled and whether the virtual IP address has been bound to the NIC.
   a. Log in to the management console.
   b. Click Service List and click Elastic Cloud Server under Computing.
   c. In the ECS list, click the name of the target ECS.
   d. On the displayed ECS details page, click the NICs tab.
   e. Check that Source/Destination Check is disabled.
   f. Ensure that an IP address is displayed for Virtual IP Address on the NIC details page. If no IP address is displayed for Virtual IP Address, click Manage Virtual IP Address and configure an IP address.
2. Check whether an ECS has been configured with a virtual IP address.
   This following uses Linux and Windows ECSs as examples to describe how to check whether an ECS has been configured with a virtual IP address.

   **For a Linux ECS:**
   a. Run the following command on the ECS and check whether NIC `ethX:Y` exists:
      ```bash
      ifconfig
      ```
The command output in the preceding figure contains the NIC of the `ethX:X` type. **192.168.1.137** is the virtual IP address in 1.

- If yes, the sub-interface of the ECS NIC has been created properly.
- If no, perform the following operations:
  
b. If the command output does not contain the NIC of the `ethX:X` type, run the following command to switch to the `/etc/sysconfig/network-scripts` directory:

    ```bash
cd /etc/sysconfig/network-scripts
    ```

c. Run the following command to create and then modify the `ifcfg-eth0:1` file:

    ```bash
    vi ifcfg-eth0:1
    ```

    Add the following NIC information to the file:

    ```
    BOOTPROTO=static
    DEVICE=eth0:1
    HWADDR=fa:16:3e:4d:5b:98
    IPADDR=192.168.1.137
    GATEWAY=192.168.1.1
    NETMASK=255.255.255.0
    ONBOOT=yes
    ONPARENT=yes
    ```

d. Press **Esc**, enter :wq!, and save the file and exit.

e. Restart the ECS and run the `ifconfig` command to check whether the virtual IP address has been configured for the ECS.

For a Windows ECS:

a. In the Start menu, open the Windows command line window and run the following command to check whether the virtual IP address has been configured:

    ```cmd
    ipconfig /all
    ```
In the preceding command output, check whether the value of IPv4 Address is the virtual IP address 192.168.10.137 in Figure 5-6.

- If yes, the virtual IP address has been configured for the ECS NIC.
- If no, perform the following operations:
  b. Choose Control Panel > Network and Internet > Network Connections. Right-click the corresponding local connection and then click Properties.
  d. Click Properties.
  e. Select Use the following IP address, and set IP address to the private IP address displayed in Figure 5-6. For example, 192.168.10.41.
f. Click **Advanced**.

g. On the **IP Settings** tab, click **Add** in the **IP addresses** area. Add the virtual IP address displayed in **Figure 5-6**. For example, 192.168.10.137.
3. Check whether the ECS security groups and the network ACL rules associated with the subnets used by the ECS NICs block traffic.
   a. On the ECS details page, click the Security Groups tab and confirm that required security group rules have been configured for the virtual IP address. If the required security group rules have not been configured, click Change Security Group or Modify Security Group Rule to change the security group or modify the security group rules.
   b. Click Service List. Under Network, click Virtual Private Cloud. In the navigation pane on the left of the network console, click Network ACL and check whether the network ACL rules associated with the subnets used by the ECS NICs block access to the virtual IP address.

5.11 How Do I Handle the Cloud-init Connection Failure?

Cloud-init Network

Figure 5-9 shows the process for an ECS to obtain metadata using the cloud-init.
**Troubleshooting Procedure**

1. Check whether the ECS has obtained an IP address. If no IP address is obtained, run the `dhclient` command to obtain the IP address (this command varies depending on the ECS OSs). Alternatively, you can run the `ifdown ethx` command to disable the network port and then run the `ifup ethx` command to enable it to allow the ECS NIC to automatically obtain an IP address again.
Figure 5-10 ECS IP address

```
ifconfig
eth0 Link encap:Ethernet HWaddr FA:16:32:0D:36:DD
 inet addr:192.168.1.120 Bcast:192.168.1.255 Mask:255.255.255.0
 inet6 addr: fe80::191b:3eff:febd:5600/64 Scope:Link
 UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
 RX packets:75998 errors:0 dropped:0 overruns:0 frame:0
 TX packets:26295 errors:0 dropped:0 overruns:0 carrier:0
 collisions:0 txqueuelen:1000
 RX bytes:4162713 (3.9 MiB) TX bytes:2336476 (2.2 MiB)
 Interrupt:35

eth1 Link encap:Ethernet HWaddr FA:16:32:09:67:1B
 inet addr:192.168.1.179 Bcast:192.168.1.255 Mask:255.255.255.0
 inet6 addr: fe80::1916:3eff:fe9e:71d0/64 Scope:Link
 UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
 RX packets:45826 errors:0 dropped:0 overruns:0 frame:0
 TX packets:12244 errors:0 dropped:0 overruns:0 carrier:0
 collisions:0 txqueuelen:1000
 RX bytes:1278534 (1.2 MiB) TX bytes:4178924 (4.9 MiB)
 Interrupt:34

lo Link encap:Local Loopback inet addr:127.0.0.1 Mask:255.0.0.0
 inet6 addr: ::/120 Scope:Host
 UP LOOPBACK RUNNING MTU:65536 Metric:1
 RX packets:1 errors:0 dropped:0 overruns:0 frame:0
 TX packets:1 errors:0 dropped:0 overruns:0 carrier:0
 collisions:0 txqueuelen:0
 RX bytes:28 (28.0 b) TX bytes:28 (28.0 b)
```

2. Ping IP address 169.254.169.254/32 from the ECS. If the IP address cannot be pinged, perform the following steps:

a. Check the exact route configured on the ECS for IP address 169.254.169.254/32.

   In most cases, the next hop of the exact route for IP address 169.254.169.254/32 is the same as that of the default route for the IP address.

Figure 5-11 Route for IP address 169.254.169.254/32

```
ip route
169.254.169.254 via 192.168.1.1 dev eth0 proto static
192.168.1.0/24 dev eth0 proto kernel scope link src 192.168.1.120
192.168.1.0/24 dev eth1 proto kernel scope link src 192.168.1.179
169.254.0.0/16 dev eth0 scope link metric 1002
default via 192.168.1.1 dev eth0 proto static
```

b. If there is no exact route for IP address 169.254.169.254/32, the cause is as follows:

   Images with CentOS 5 OSs do not support the cloud-init function. To use this function, change the ECS OS.

c. If the next hop of the exact route for IP address 169.254.169.254/32 is different from that of the default route for the IP address, handle the issue based on the following information:

   • If the ECS was created before the cloud-init function is enabled, run the `service network restart` command to obtain the correct route.
If the ECS was created after the cloud-init function is enabled, go to step 6.

3. The cloud-init connection failure may also be caused by the metadata obtaining fault on the ECS.

Run the following command on the ECS to enable it to obtain the metadata:
```
curl http://169.254.169.254/openstack/latest/meta_data.json
```
If information similar to that shown in Figure 5-12 is displayed, the ECS successfully obtains the metadata.

4. If you cannot log in to the ECS or cannot create a non-root user after cloud-init is configured and when the service is running properly, the cause may be as follows:

Check whether the `/etc/cloud/cloud.cfg` configuration file format is correct.
For details, see the file format requirements posed by Linux OS providers. The following figure shows the example `/etc/cloud/cloud.cfg` configuration file for the Ubuntu OSs.

5. If you cannot use an obtained private key to log in to an ECS after the ECS starts or you cannot obtain the ECS login password, restart the ECS to rectify the fault.

6. If you still cannot use the cloud-init function after the preceding steps, contact technical support for assistance.
You need to provide the technical support engineer with the following information.
### 5.12 How Do I Handle the EIP Connection Failure?

**EIP Network**

*Figure 5-14* shows the process for an ECS to access the Internet using an EIP.
The possible causes to the EIP connection failure are as follows:

- The ECS is not running properly.
- The internal network configuration of the ECS is incorrect.
- No EIP is bound to the ECS.
- The EIP is not bound to the primary NIC of the ECS.
- Required security group rules are not configured for the ECS.
- Required packets are discarded by the firewall.

**Troubleshooting Procedure**

1. Check whether the ECS is running properly.
   
   If the ECS state is not **Running**, start or restart the ECS.
2. Check the ECS internal network configuration.
   a. Confirm that the ECS NIC has an IP address assigned.
      Log in to the ECS, and run the `ifconfig` or `ip address` command to check
      the ECS NIC IP address.
      The `ipconfig` command applies only to Windows ECSs.
   b. Check whether the IP address is correctly configured on the ECS NIC.
      Log in to the ECS, and run the `ifconfig` or `ip address` command to check
      the ECS NIC IP address. If the ECS NIC does not have an IP address
      configured, run a command to configure an IP address for the ECS NIC.
      For example, run the `ip addr add 192.168.1.192/24 eth0` command to
      configure IP address 192.168.1.192/24 for the NIC.

   ![Figure 5-16 NIC virtual IP address](image)

   Check whether the default route exists. If no, run the `ip route add` command to add the default route.

   ![Figure 5-17 Default route](image)

3. Check whether the EIP has been assigned and bound to the ECS. (If the EIP
   has not been assigned or bound to the ECS, assign an EIP and bind it to the
   ECS.)

   ![Figure 5-18 EIP status](image)

4. Check whether the EIP is bound to the primary NIC of the ECS.

   ![Figure 5-19 EIP binding status](image)
5. Check whether required security group rules have been configured. Configure security group rules 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.)

6. Check whether traffic filtering has been configured on the firewall for the subnet used by the ECS NIC. If you can configure the firewall on the VPC console, confirm that the firewall rules allow traffic from the subnet used by the ECS to pass through.

7. Contact technical support. If you still cannot properly use the EIP after the preceding steps, contact technical support for assistance. You need to provide the technical support engineer with the following information.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
<th>Example</th>
<th>Your Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPC CIDR block</td>
<td>Required for customer gateway configuration</td>
<td>Example: 10.0.0.0/16</td>
<td>N/A</td>
</tr>
<tr>
<td>VPC ID</td>
<td>N/A</td>
<td>Example: 120b71c7-94ac-45b8-8ed6-30aafc8fdba</td>
<td>N/A</td>
</tr>
<tr>
<td>CIDR block of subnet 1 (can be the same as the VPC CIDR block)</td>
<td>N/A</td>
<td>Example: 10.0.1.0/24</td>
<td>N/A</td>
</tr>
<tr>
<td>ECS ID</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>ECS IP address</td>
<td>N/A</td>
<td>Example: 192.168.1.192/24</td>
<td>N/A</td>
</tr>
<tr>
<td>ECS route information</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>EIP</td>
<td>Required for the customer ECS to access the Internet</td>
<td>Example: 10.154.55.175</td>
<td>N/A</td>
</tr>
<tr>
<td>EIP bandwidth</td>
<td>Maximum bandwidth size used by the customer ECS to access the Internet</td>
<td>Example: 1 Mbit/s</td>
<td>N/A</td>
</tr>
<tr>
<td>EIP ID</td>
<td>N/A</td>
<td>Example: b556c80e-6345-4003-b512-4e6086abbd48</td>
<td>N/A</td>
</tr>
</tbody>
</table>
5.13 How Do I Handle the IB Network Failure?

RDMA Communication Failure Between Two IB ECSs

1. Check whether the Pkeys on the two ECSs are consistent.
   Run the following command to check for the Pkeys allocated to the ECSs:
   
   ```
   cat /sys/class/infiniband/mlx5_0/ports/1/pkeys/* | grep -v "0x0000"
   ```
   
   ![Figure 5-20 Checking Pkey consistency](image)
   
   - If only one Pkey is obtained, contact technical support.
   - If two Pkeys are obtained, ensure that the two Pkeys on the two ECSs are the same.

2. Run the following command to check whether the firewall is disabled:
   
   ```
   service firewalld status
   ```
   
   ![Figure 5-21 Checking the firewall](image)
   
   If the firewall is not disabled, run the following command to disable it:
   
   ```
   service firewalld stop
   ```

3. Check whether the RDMA communication command is correct.
   Run the following command on ECS 1 (client):
   
   ```
   ib_write_lat -x 0 --pkey_index 0 192.168.0.218
   ```
   
   Run the following command on ECS 2 (server):
   
   ```
   ib_write_lat -x 0 --pkey_index 0
   ```

No IP Address for the ECS IB Port

After you run the `ifconfig` command, it is found that no IP address has been assigned to the ECS InfiniBand (IB) port.

1. Run the following command to check for the Pkey:
   
   ```
   cat /sys/class/infiniband/mlx5_0/ports/1/pkeys/* | grep -v "0x0000"
   ```
   
   ![Figure 5-22 Checking Pkey](image)
If only one Pkey is obtained, contact technical support.

2. Run the following command to assign an IP address to the ECS IB port:

   `dhclient ib0`

   If no command output is displayed, the IP address cannot be obtained using DHCP.

3. Contact technical support.

   After you have performed the preceding steps, if the IB network still cannot be used for communication or the IB port still cannot obtain an IP address, contact technical support for assistance and provide the technical support engineer with the following information.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
<th>Example</th>
<th>Your Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VP C1 ID</td>
<td>VPC 1 ID</td>
<td>Example: fef6559-c154-4229-afc4-9ad0314437ea</td>
<td>N/A</td>
</tr>
<tr>
<td>VM 1 ID</td>
<td>ID of ECS 1 in VPC 1</td>
<td>Example: f7619b12-3683-4203-9271-f34f283cd740</td>
<td>N/A</td>
</tr>
<tr>
<td>VM 2 ID</td>
<td>ID of ECS 2 in VPC 1</td>
<td>Example: f75df766-68aa-4ef3-a493-06c26ac37a</td>
<td>N/A</td>
</tr>
</tbody>
</table>

### 5.14 How Do I Handle the VPC Peering Connection Failure?

**VPC Peering Connection Network**

*Figure 5-23* shows the VPC peering connection network.
Figure 5-23 VPC peering connection network

Routes are required to enable communication between Subnet A in VPC1 and Subnet X in VPC2 in the figure. Figure 5-24 shows the route table configuration.

Figure 5-24 VPC peering connection route table

Checking ECS Basic Network Functions

1. Confirm that the ECS NIC has an IP address assigned.
   Log in to the ECS, and run the `ifconfig` or `ip address` command to check the ECS NIC IP address.
   The `ipconfig` command applies only to Windows ECSs.

2. Ping the gateway address of the subnet from the ECS to check the ECS communication with external networks.
   Obtain the gateway address from the VPC details page on the console. In most cases, the gateway address is `xxx.xxx.xxx.1`. Ping the gateway address to check the communication. If the gateway address cannot be pinged, troubleshoot the layer 2 and layer 3 networks.

Checking VPC Network Configuration

1. Confirm that the security group configuration of the ECS NIC is correct.
Obtain the security group used by the ECS NIC from the ECS details page. The security group rule that allows the ECS to access the peer subnet has been configured for the security group. For example, you must configure security group rules described in Figure 5-25 for the NICs of all ECSs in VPC 1 in Figure 5-23.

Figure 5-25 Security group configuration

<table>
<thead>
<tr>
<th>Direction</th>
<th>Type</th>
<th>Protocol</th>
<th>Port Range/Port Type</th>
<th>Remote END</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inbound</td>
<td>IPv4</td>
<td>Any</td>
<td>Any</td>
<td>10.0.0.1/24</td>
<td>Delete</td>
</tr>
</tbody>
</table>

2. Confirm that the firewall for the subnet used by the ECS NIC does not block required traffic.

   If you can configure the firewall on the VPC console, confirm that the firewall rules allow traffic from the subnets used by the VPC peering connection to pass through.

3. If the ECS has more than one NIC, ensure that correct policy-based routing has been configured for the ECS and that packets with different source IP addresses match their own rules.

   For example, if the IP address of eth0 is 192.168.1.10/24, and that of eth1 is 192.168.2.10/24, run the following commands:

   ```
   ping -I 192.168.1.10 192.168.1.1
   ping -I 192.168.2.10 192.168.2.1
   ```

   If the IP addresses can be pinged, the policy-based routing configured for the two NICs is correct.

Checking VPC Peering Connection Configuration

1. The VPC peering connection described in Figure 5-23 is used as an example to show how to check the configuration. Check whether correct routes have been added to the VPC peering connection. For example, the destination of the route for VPC 1 must be the subnet CIDR block in VPC 2.

   Add local and peer routes on the VPC peering connection page. The VPC peering connection works properly after the routes are correctly configured.

2. Check VPC 1 and VPC 2 for subnets that conflict with the subnets involved in the VPC peering connection. For example, if VPC 1 and VPC 2 each has a subnet with the same CIDR block, such as 192.168.11.0/24, the VPC peering connection will become invalid. Figure 5-26 shows the invalid VPC peering connection.
O&M Operations That Require Assistance

If the VPC peering connection failure cannot be rectified after you perform the preceding operations, contact technical support.

You need to ping the ECS at one side of the VPC peering connection from another ECS at the other side of the VPC peering connection to send ICMP packets and provide the technical support engineer with the following information:

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
<th>Your Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPC1 ID</td>
<td>VPC 1 ID</td>
<td>N/A</td>
</tr>
<tr>
<td>VPC2 ID</td>
<td>VPC 2 ID</td>
<td>N/A</td>
</tr>
<tr>
<td>VM1 ID</td>
<td>ID of the ECS in VPC 1</td>
<td>N/A</td>
</tr>
<tr>
<td>VM2 ID</td>
<td>ID of the ECS in VPC 2</td>
<td>N/A</td>
</tr>
<tr>
<td>Subnet1 ID</td>
<td>ID of the subnet used by ECS 1</td>
<td>N/A</td>
</tr>
<tr>
<td>Subnet2 ID</td>
<td>ID of the subnet used by ECS 2</td>
<td>N/A</td>
</tr>
<tr>
<td>IP1</td>
<td>ECS 1 IP address</td>
<td>N/A</td>
</tr>
<tr>
<td>IP2</td>
<td>ECS 2 IP address</td>
<td>N/A</td>
</tr>
</tbody>
</table>

**NOTE**

You can add `-t` to the end of the ping command to enable the Windows ECS to continuously send ICMP packets.
5.15 How Do I Handle the Layer 2 or Layer 3 Network Communication Failure?

1. Check whether the ECS has obtained an IP address.
   Log in to the ECS, and run the `ifconfig` or `ip address` command to check the ECS NIC IP address information. The `ipconfig` command applies only to Windows ECSs.

2. If the ECS does not have an IP address, check whether DHCP has been enabled for the required subnet.
   Switch to the subnet details page and check whether the DHCP function has been enabled.

3. If the ECS has an IP address, check whether the security group rules and firewall rules allow the required traffic to pass through.
   a. Check the security group rules.
      Obtain the security group used by the ECS NIC from the ECS details page. The security group rule that allows the ECS to access the required subnet has been configured for the security group.
   b. Check the firewall rules.
      If you can configure the firewall on the VPC console, confirm that the firewall rules allow traffic from the required subnets to pass through.

5.16 How Do I Handle the BMS Network Failure?

1. Run the following command to check whether the BMS network ports have been bonded:
   `ifconfig`
If no bonding information is obtained, the BMS network ports are not bonded. Contact technical support.

2. Run the following command to check whether the BMS route information is correct:

```
route –n
```

Check whether the default route (with a destination of 0.0.0.0) exists.

```
0.0.0.0 192.168.2.1 0.0.0.0 UG 0 0 0 0 bond0
```

Check whether a route to 169.254.169.254 exists.

```
169.254.169.254 169.254.192.168.2.1 0.0.0.0 UG 0 0 0 0 bond0
```

If required routes do not exist, contact technical support engineers.

3. If BMSs in a VPC cannot communicate with each other or the BMS with an EIP cannot access the Internet, rectify the failure based on the related ECS FAQ.

4. If the failure cannot be rectified after you perform the preceding operations, contact technical support.

Obtain the VPC and BMS information on the management console and provide the technical support engineer with the following information.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
<th>Example</th>
<th>Your Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPC 1 ID</td>
<td>VPC 1 ID</td>
<td>Example: fe65559-c154-4229-afc4-9ad0314437ea</td>
<td>N/A</td>
</tr>
<tr>
<td>BMS 1 ID</td>
<td>ID of BMS 1 in VPC 1</td>
<td>Example: f7619b12-3683-4203-9271-f34f283cd740</td>
<td>N/A</td>
</tr>
<tr>
<td>BMS 2 ID</td>
<td>ID of BMS 2 in VPC 1</td>
<td>Example: f75df766-68aa-4ef3-a493-06cdc26ac37a</td>
<td>N/A</td>
</tr>
</tbody>
</table>

5.17 How Do I Handle the ECS IP Address Obtaining Failure?

1. Check whether the DHCP function of the subnet is enabled (enabled by default).

Switch to the subnet details page. If DHCP is disabled, you must manually configure a static IP address for the ECS by referring to step 4.

2. Run the following command to check whether the dhclient process exists:
   ```bash
grep dhclient
   ```

3. If the dhclient process does not exist, log in to the ECS and try restarting the ECS NIC or sending a DHCP request.
   - Linux OS:
     Run the `dhclient ethx` command. If dhclient commands are supported, run the `ifdown ethx;ifup ethx` command. In the command, `ethx` indicates the ECS NIC, for example, `eth0` and `eth1`.
   - Windows OS:
     Disconnect the network connection and connect it.

4. If the DHCP client does not send requests for a long time, for example, the fault occurs again after the NIC restarts, you can use the following method to configure the static IP address.
   - Linux OS:
     i. Run the following command to open the `/etc/sysconfig/network-scripts/ifcfg-eth0` file:
vi /etc/sysconfig/network-scripts/ifcfg-eth0

ii. Modify the following configuration items in the /etc/sysconfig/network-scripts/ifcfg-eth0 file.
   BOOTPROTO=static
   IPADDR=192.168.1.100 #IP address
   NETMASK=255.255.255.0 #Subnet mask
   GATEWAY=192.168.1.1 #Gateway address

iii. Run the following command to restart the network service:

   service network restart

   – Windows OS:

     On the Local Area Connection Status tab, click Properties. In the displayed area, Select Internet Protocol Version 4 (TCP/IPv4) and click Properties. In the displayed area, enter the IP address, subnet mask, and the default gateway address.

5. Check the ECS messages log in the /var/log/messages directory to troubleshoot the ECS.

   Search for the NIC MAC address and check whether processes that cause failures in obtaining IP addresses over DHCP exists.

6. If the failure cannot be rectified after you perform the preceding operations, contact technical support.

   Provide the customer service with the ECS ID, the ID of the subnet used by the ECS, and the ID of the VPC used by the ECS.

5.18 How Do I Handle the VPN or Direct Connect Connection Network Failure?

VPN Network

   Figure 5-31 shows your network, the customer gateway, the VPN, and the VPC.
Customer Self-Check Guidance

1. Provide your network information.
   Obtain information listed in Table 5-1. This table lists example values. You can determine the actual values based on the example values. You must obtain all actual values of your project.

   ![NOTE](image)

   You can print this table and fill in your values.

   **Table 5-1 Network information**

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
<th>Example</th>
<th>Your Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPC CIDR block</td>
<td>Required for customer gateway configuration</td>
<td>Example: 10.0.0.0/16</td>
<td>N/A</td>
</tr>
<tr>
<td>VPC ID</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>CIDR block of subnet 1</td>
<td>N/A</td>
<td>Example: 10.0.1.0/24</td>
<td>N/A</td>
</tr>
<tr>
<td>ECS ID</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>
### Customer gateway type (for example, Cisco)
N/A
N/A
N/A

### Public IP address used by the customer gateway
N/A
The value must be static.
N/A

2. Provide your gateway configuration information.
   
   You can check the gateway connectivity issues based on the following steps:
   
   You must take the IKE, IPsec, ACL rules, and route selection into consideration.
   
   You can rectify the failure in any desired sequence. However, it is recommended that you check for the failure in the following sequence: IKE, IPsec, ACL rules, and route selection.
   
   a. Obtain the IKE policy used by your gateway device.
   b. Obtain the IPsec policy used by your gateway device.
   c. Obtain the ACL rule used by your gateway device.
   d. Check whether your gateway device can communicate with the gateway devices in the public cloud system.

   **NOTE**
   
   The commands used on different gateway devices are different. You can run the commands based on your gateway device (such as Cisco, H3C, AR, or Fortinet device) to obtain the preceding required information.

### O&M Operations That Require Assistance

You must send communication requests from the ECSs in the public cloud system to the remote device.

**Method:**

Log in to an ECS in the public cloud system and ping an IP address in your on-premises data center.

### 5.19 Can a VPC Peering Connection Be Deployed Across Regions?

No, but it can be deployed across AZs in the same region.

### 5.20 Is a VPC Peering Connection Charged?

It is free of charge currently.
6.1 How Do I Configure Policy-Based Routing for ECSs with Multiple NICs?

If an ECS has multiple NICs, perform the following operations to configure policy-based routing for the ECS to enable the network communication of secondary NICs.

**For a Linux ECS:**

1. Run the following command and add two route tables (`net1` and `net2`) and their priorities to the `/etc/iproute2/rt_tables` file. The priorities of `net1` and `net2` are 252 and 251, respectively. A smaller value indicates a higher priority.

   ```
   vi /etc/iproute2/rt_tables
   # added for dual net
   252     net1
   251     net2
   ```

2. Run the following command and add the NIC routing information to the `/etc/rc.local` file:

   ```
   vi /etc/rc.local
   ```

   The IP addresses of NICs `eth0` and `eth1` are 192.168.1.23 and 192.168.2.4, respectively. The subnet mask is 24 bits. The gateway addresses of NICs `eth0` and `eth1` are 192.168.1.1 and 192.168.2.1, respectively. The information to be added is as follows:

   ```
   # Request IP address for eth1
dhclient eth1
   # Add routes
   ip route flush table net1
   ip route add default via 192.168.1.1 dev eth0 src 192.168.1.23 table net1
   ip route add 192.168.1.0/24 dev eth0 src 192.168.1.23 table net1
   ip rule add from 192.168.1.23 table net1
   ```

   ```
   ip route flush table net2
   ip route add default via 192.168.2.1 dev eth1 src 192.168.2.4 table net2
   ip route add 192.168.2.0/24 dev eth1 src 192.168.2.4 table net2
   ip rule add from 192.168.2.4 table net2
   ```

3. Run the following command to add the execute permission for the `rc.local` file:

   ```
   ```
# chmod +x /etc/rc.local
4. Run the `reboot` command to restart the ECS.

**For a Windows ECS:**

1. Choose **Control Panel > Network and Internet > Network Connections**. Right-click **Local Area Connection 2** and then click **Properties**.

   **NOTE**

   Right-click to add NICs based on the site requirements.

2. On the **Network** tab page, select **Internet Protocol Version 4 (TCP/IPv4)**.
3. Click **Properties**.
4. On the **General** tab page, click **Advanced**.
5. On the **IP Settings** tab, click **Add** in the **Default gateways** area.

**Figure 6-1** Advanced TCP/IP settings

6. Enter the gateway address of the secondary NIC and click **Add**.
7. Click **OK**.

**6.2 Can a Route Table Span Multiple VPCs?**

No.

**6.3 How Many Routes Can Exist in a Route Table?**

Currently, a route table can contain 100 routes.

**6.4 What Are the Limitations of a Route Table?**

- The ECS providing SNAT can have only one NIC.
- The ECS providing SNAT must have the **Unbind IP from MAC** function enabled.
- The destination of each route in a route table must be unique. The next hop must be a private IP address or a virtual IP address in the VPC. Otherwise, the route table will not take effect.
- If a virtual IP address is set to the next hop in a route, EIPs bound with the virtual IP address in the VPC will become invalid.

**6.5 Will a Route Table be Billed?**

The route table function itself is free of charge. However, you are charged for the ECSs and bandwidth used together with the route table function.

**6.6 Are There Different Routing Priorities for Direct Connect Connections and Custom Routes in the Same VPC?**

No. Direct Connect connections and custom routes are used in different scenarios. Therefore, there is no routing priority competition between them.
6.7 Are There Different Routing Priorities of the VPN and Custom Routes in the Same VPC?

The routing priority of custom routes and that of VPNs are the same.

6.8 How Many Routes Can Be Added in a VPC?

By default, a maximum of 100 routes can be added for a VPC. The routes include those added for Direct Connect connections and VPC peering connections.
7.1 Are the Security Group Rules Considered as the Same If All Their Parameters Except the Description Are the Same?

Yes. When you add or import a security group rule with the same parameters except the description as an existing one in the security group, the adding or importing will fail.

7.2 What Should I Do Before Deleting a Security Group?

- Before deleting a security group, ensure that the security group is not used by any cloud resource, such as ECS, Relational Database Service (RDS), and Distributed Cache Service (DCS). If the security group is used by any cloud resource, release the corresponding cloud resource or change the security group used by the cloud resource, and then delete the security group.
- If the security group to be deleted has been associated with rules of another security group (Source), delete or modify the associated security group rules, and then delete the security group.

7.3 What Do I Do If Outbound Access Through TCP Port 25 Is Restricted?

**Symptom:** TCP port 25 cannot be used to access an external address. For example, you cannot run the `Telnet smtp.***.com 25` command.

**Cause:** Outbound traffic from TCP port 25 is denied by default.

**Solution:** Request to allow outbound traffic from TCP port 25.
Before sending the request, you must agree and guarantee that TCP port 25 is only used to connect third-party Simple Mail Transfer Protocol (SMTP) servers and that emails are sent using the third-party SMTP servers. If you use the EIP specified in the service ticket to directly send emails over SMTP, we will permanently disable TCP port 25 for you and will no longer enable it even you request.

1. On the Create Service Ticket page, choose Products > Elastic Cloud Server. For details about how to submit a service ticket, see Submitting a Service Ticket.
2. Click Open Port 25 under Select Subtype and click Create Service Ticket.

![Figure 7-1 Creating a service ticket](image)

3. On the displayed page, enter the required information as prompted.

### 7.4 Can I Change the Security Group of an ECS?

Yes. Log in to the ECS console, switch to the page showing ECS details, and change the security group of the ECS.

### 7.5 How Many Security Groups Can Each User Have?

Each user can have a maximum of 100 security groups and 5000 security group rules.

When creating an ECS, you can select multiple security groups (no more than five is recommended).

### 7.6 Is the Security Group Service Charged?

The security group service is free of charge.

### 7.7 How Can I Configure a Security Group for Multi-Channel Protocols?

**ECS Configuration**

The TFTP daemon determines whether the configuration file specifies the port range. If you use the TFTP configuration file that allows the data channel ports to be configurable, it is a best practice to configure a small range of ports that are not listened on.
Security Group Configuration

You can configure both port 69 and the data channel ports used by TFTP for the security group. In RFC1350, the TFTP protocol specifies that ports available to data channels range from 0 to 65535. However, not all these ports are used by the TFTP daemon processes of different applications. Therefore, you can configure a small range of ports for the TFTP daemon.

The following figure provides an example of the security group rule configuration if the ports used by data channels range from 60001 to 60100.

**Figure 7-2 Security group rules**

<table>
<thead>
<tr>
<th>Type</th>
<th>Protocol</th>
<th>PortRange</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4</td>
<td>All</td>
<td>All</td>
<td>sg1021</td>
</tr>
<tr>
<td>IPv4</td>
<td>UDP</td>
<td>60001-60100</td>
<td>0.0.0.0.0</td>
</tr>
</tbody>
</table>

7.8 How Many Network ACLs Can a User Have?

A user can have a maximum of 200 network ACLs. It is recommended that you configure a maximum of 20 inbound or outbound rules for each network ACLs. If more than 20 inbound or outbound rules are configured, the forwarding performance will deteriorate.

7.9 Does a Security Group Rule or Network ACL Rule Immediately Take Effect for Its Original Traffic After Being Modified?

No. After a security group rule or network ACL Rule is modified, the new rule may not immediately take effect for its original traffic. Users need to interrupt the original traffic for about 120 seconds for the new rule to take effect for the traffic.

7.10 Which Security Group Rule Has Priority When Multiple Security Group Rules Conflict?

Security group rules use the whitelist mechanism. If multiple security group rules conflict, the union of these rules takes effect.

7.11 What Do I Do If Some Ports in the Public Cloud System Are Inaccessible?

**Symptom**: Users in some areas cannot access some ports in the public cloud system.

**Analysis**: Ports listed in the following table are high-risk ports and are blocked by default.
### Table 7-1 High-risk ports

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP</td>
<td>42, 135, 137, 138, 139, 444, 445, 593, 1025, 1068, 1434, 3127, 3128, 3129, 3130, 4444, 5554, 5800, 5900, and 9996</td>
</tr>
<tr>
<td>UDP</td>
<td>135 to 139, 1026, 1027, 1028, 1068, 1433, 1434, 5554, and 9996</td>
</tr>
</tbody>
</table>

**Solution:** It is recommended that you use ports not listed in the table for your services.

### 7.12 Why the Access from a Specified IP Address Is Still Allowed After a Network ACL Rule that Denies the Access from this Specified IP Address Has Been Added?

Network ACL rules have priorities. A smaller priority value represents a higher priority. Each network ACL includes a default rule whose priority value is an asterisk (*). Default rules have the lowest priority.

If network ACL rules conflict, the rule with the highest priority takes effect. If you need a rule to take effect before or after a specific rule, you can insert that rule before or after the specific rule. For example, if the priority of rule A is 1 and the priority of rule B is higher than that of rule A, insert rule B before rule A. In this case, the priority of rule B is 1 and that of rule A is 2. Similarly, if the priority of rule B is lower than that of rule A, insert rule B after rule A.

When a rule that denies access from a specified IP address is added, put the rules that allow access from all IP addresses to the end. The rule that denies access from the specified IP address takes effect. For details, see [Changing the Sequence of a Network ACL Rule](#).