Elastic Public IPv6

Product Documentation

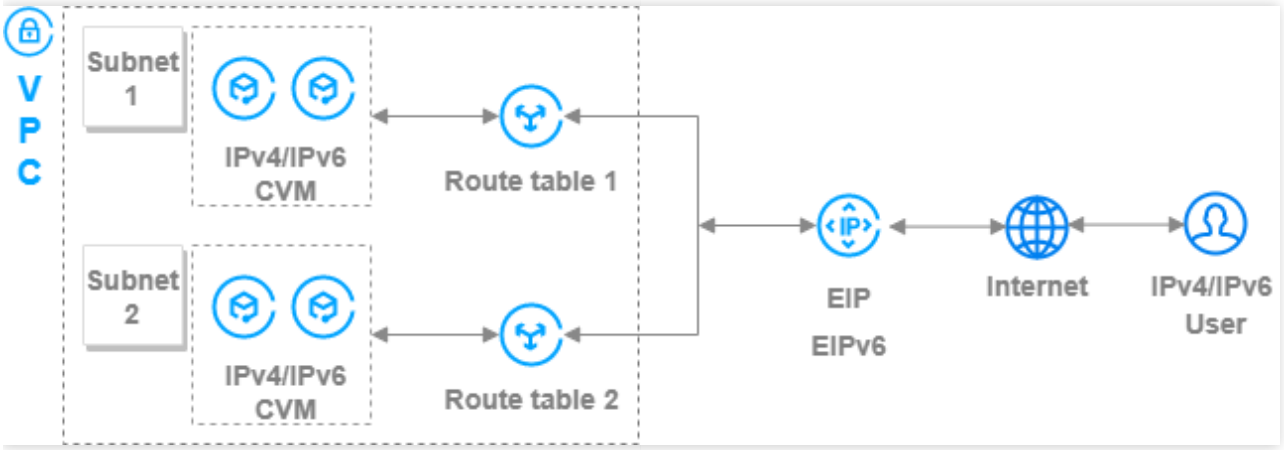
Contents

Elastic Public IPv6 3
- Product Introduction 3
  - Elastic IPV6 Overview 3
  - Strengths 5
  - Use Cases 6
  - Quota Description 8
- Quick Start 9
- Operation Guide 40
  - Allocating and Releasing IPv6 CIDR for VPC 40
  - Allocating and Releasing IPv6 CIDR for a Subnet 41
  - Applying for and Releasing IPv6 Addresses for ENI 42
  - Managing IPv6 Public Network 44
- FAQs 47
  - General 47
  - Troubleshooting IPv6 Connectivity 48
- Glossary 55

Product Introduction
Elastic IPV6 Overview

With Elastic Public IPv6, you can enable or disable public network access for each CVM's IPv6 address and set the public network bandwidth. Elastic Public IPv6 (EIPv6) is the public network gateway of the CVM IPv6.

> Note:
>
> The Elastic IP in this document refers to the Elastic IPv4.



Product Features

After an IPv6 address is applied for an ENI, public network access is disabled by default, and only IPv6 address communication within the VPC is supported. The public network can be enabled or disabled for a single IPv6 address or multiple IPv6 addresses through Elastic IPv6.

Intra-VPC Communication

After the IPv6 addresses are obtained and enabled for different ENIs in the same VPC, the IPv6 addresses in the VPC can communicate with each other by default.

Enabling the Public Network

For IPv6 addresses for which the public network is not enabled, you can use Elastic IPv6 to enable the public network and set the upper limit of a public network bandwidth. The public network can be enabled individually or in batches.

Disabling the Public Network

For IPv6 addresses for which the public network communication capabilities have been enabled, you can

use Elastic IPv6 to disable the public network. The public network can be disabled individually or in batches.

Strengths

Easy Operation

You can use Elastic Public IPv6 to enable or disable public network access for your IPv6 CVM at any time, and flexibly set the peak IPv6 public network bandwidth. Provides batch enable and disable operations for easy management.

Security and Reliability

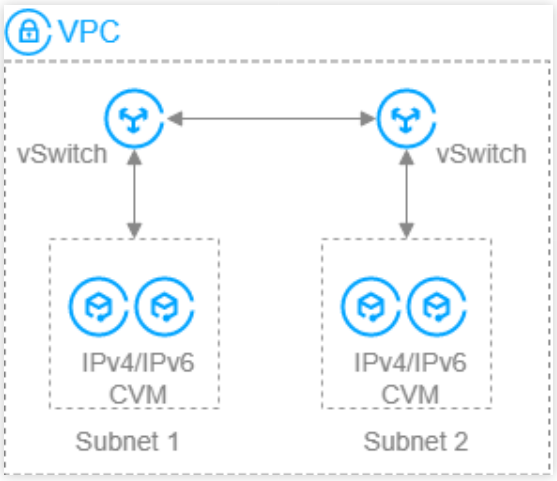
Elastic Public IPv6 ensures the security and reliability of IPv6 communication access in a variety of ways. For example, disabling public network access by default. At the same time, the high availability of the overall architecture is achieved through the underlying architecture capabilities of cross-rack disaster recovery and cross-IDC disaster recovery.

Use Cases

Scenario 1: Building IPv4/IPv6 dual-stack communication within a VPC

You can quickly build an IPv4/IPv6 dual-stack VPC by enabling IPv6.

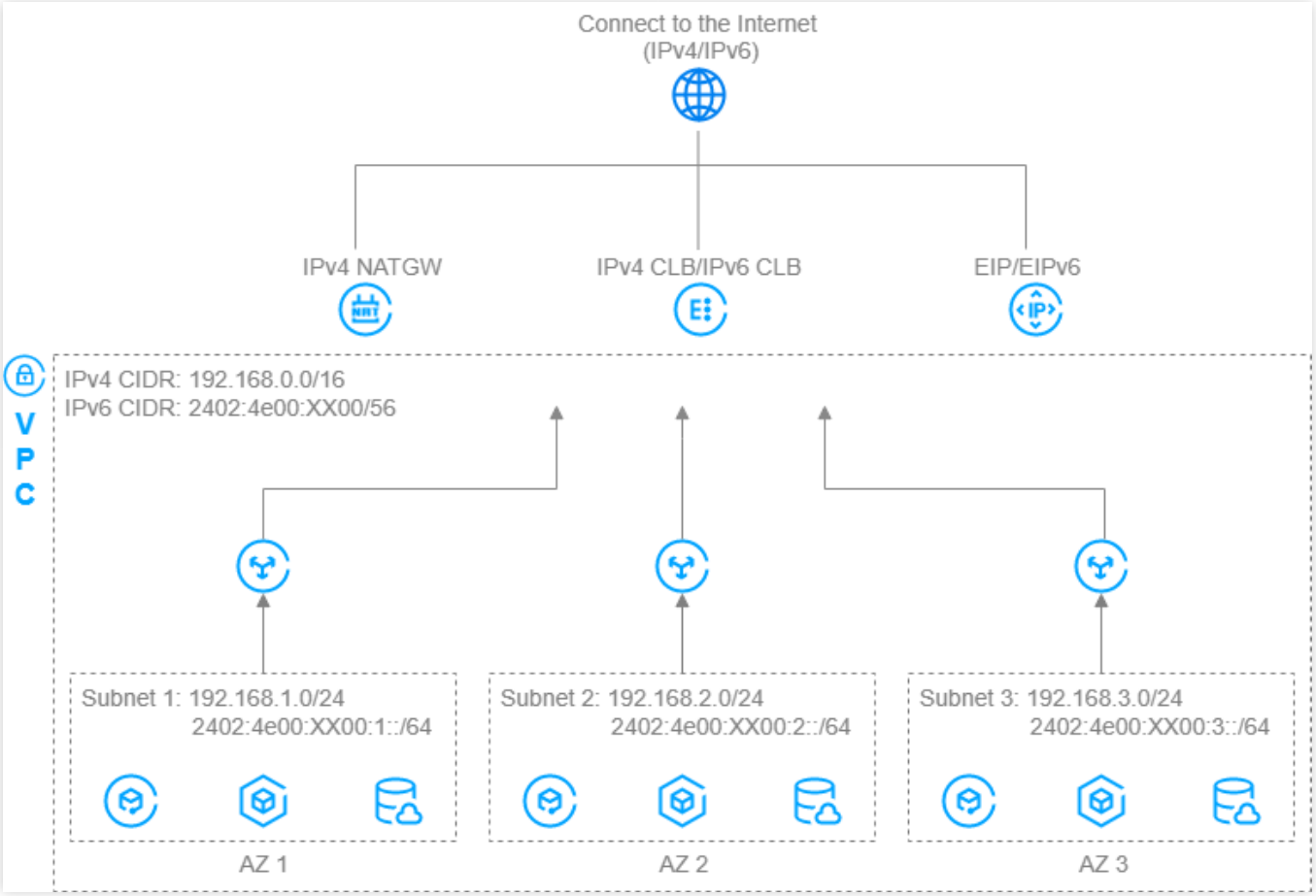
- After the VPC obtains the IPv6 CIDR, the VPC will support IPv4 and IPv6 dual protocol stacks.
- After the CVM obtains IPv6, it will also support IPv4 and IPv6 dual protocol stacks.
- By default, IPv6 communication between CVMs in the same VPC is supported, but IPv6 communication between CVMs in different VPCs is not supported.
- By default, the CVM cannot access the IPv6 public network. You need to manually enable the IPv6 public network bandwidth for the CVM before it can access the IPv6 public network.



Scenario 2: Building IPv6 public network communication for CVM

After the CVM obtains IPv6, it will run IPv4 and IPv6 dual protocol stacks simultaneously.

- You can enable IPv6 public network access for your CVM through Elastic IPv6, while the CVM can still access the IPv4 public network through IPv4 EIP or IPv4 NAT gateway.
- The public network access settings of IPv6 and the settings of IPv4 EIP will not affect each other. Therefore, if the public network is enabled only for IPv6, while the IPv4 EIP is not set, the CVM cannot access the IPv4 public network.
- You can set the maximum bandwidth for the CVM IPv6 public network. Through refined IPv6 public network bandwidth thresholds and default basic anti-DDoS policy, you can effectively improve security protection capabilities.


Connect to the Internet
(IPv4/IPv6)
IPv4 NATGW
IPv4 CLB/IPv6 CLB
EIP/EIPv6
VPC
IPv4 CIDR: 192.168.0.0/16
IPv6 CIDR: 2402:4e00:XX00/56
Subnet 1: 192.168.1.0/24
2402:4e00:XX00:1::/64
Subnet 2: 192.168.2.0/24
2402:4e00:XX00:2::/64
Subnet 3: 192.168.3.0/24
2402:4e00:XX00:3::/64
AZ 1
AZ 2
AZ 3

Quota Description

IPv6 Basic Quota

Resources	Limit (pcs)
The number of IPv6 CIDRs per VPC	1
The number of subnets for which IPv6 can be enabled per VPC	256
The number of IPv6 CIDRs per subnet	1
The number of IPv6 addresses per ENI	1
The number of ENIs for which IPv6 can be enabled per VPC	10000
The number of public networks for which IPv6 can be enabled per VPC	1000

> Note:
>
> The public network can be enabled for only 1,000 IPv6 addresses in a VPC. If you want to enable public network for more IPv6, submit a ticket.

Upper Limit of IPv6 Public Network Bandwidth

The upper limit of each IPv6 public network bandwidth is 0 - 100 Mbps.

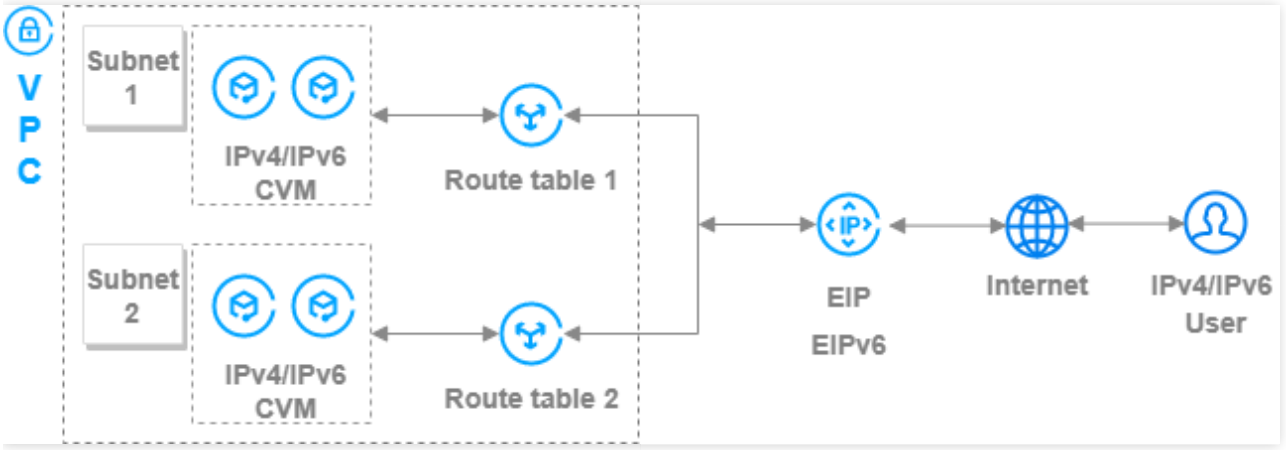
> Note:
>
> The peak IPv6 public network bandwidths of different CVM models are different. If you want to enable a larger public network bandwidth, submit ticket.

Quick Start

This guide will help you build a Virtual Private Cloud (VPC) with IPv6 CIDR, and enable IPv6 for the Cloud Virtual Machine (CVM) in the VPC to implement IPv6 VPC and public network communications.

Overview

1. CVMs are IPv6-enabled to communicate with other CVMs in the VPC through the IPv6 private network.
2. CVMs are IPv6-enabled to communicate bidirectionally with IPv6 users on the Internet.



Instructions

1. The IPv6 address is a GUA address. Each VPC is allocated with one /56 IPv6 CIDR, each subnet is allocated with one /64 IPv6 CIDR, and each Elastic Network Interface (ENI) is allocated with one IPv6 address.
2. Both the primary network interface and the secondary network interface support applying for IPv6 addresses. For more information about the relationship between CVM and ENI, see Elastic Network Interface product documentation.

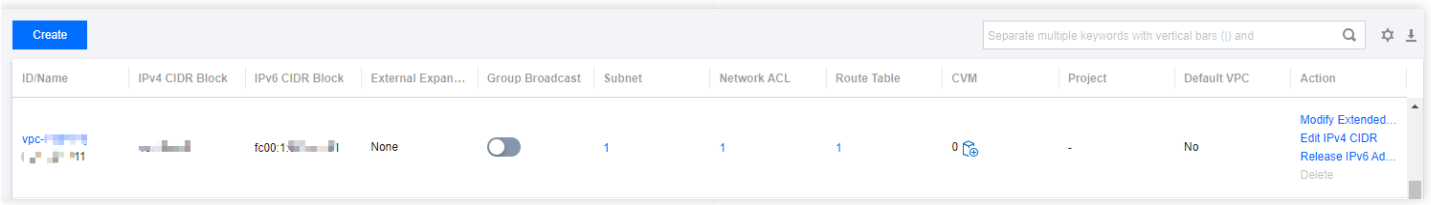
Directions

Step 1: Allocating IPv6 CIDR to VPC.

1. Log in to the VPC Console.

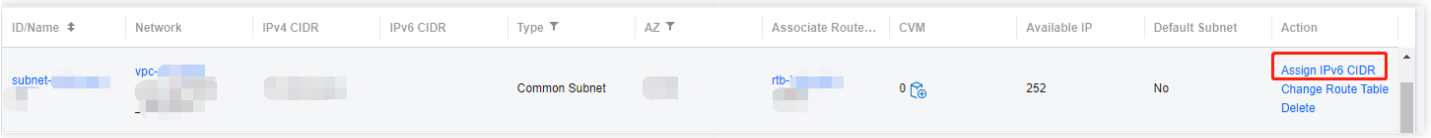
2. Select a region that supports IPv6, and in the operation column of the VPC row, click Obtain IPv6 Address.

The system will allocate one /56 IPv6 address segment for VPC. You can view detailed information about the IPv6 address segment in the list.



Step 2: Allocating IPv6 CIDR to Subnet.

1. Log in to the VPC Console.
2. In the left directory, choose Subnet to go to the management page.
3. In the operation column of the row where the subnet is located in the VPC in Step 1, click Allocate IPv6 CIDR.



4. In the pop-up dialog box, allocate an IPv6 CIDR to the subnet and click OK.

The system will allocate one /64 IPv6 CIDR from VPC /56 IPv6 CIDR.

Step 3: Buying a CVM and Configuring IPv6 for the CVM.

After you allocate an IPv6 CIDR for a VPC and a subnet, you can create a CVM with an IPv6 address in the subnet, or obtain an IPv6 address for a CVM running in the subnet. Because IPv6 addresses cannot be automatically delivered to network interfaces, you still need to log in to the CVM console to configure IPv6 after obtaining the IPv6 address.

1. Log in to the Cloud Virtual Machine Purchase Page.

2. On the top of CVM purchase page, select Custom Configuration.

3. On the Select Region and Model tab, select a VPC and subnet that have been allocated with an IPv6 CIDR, set the instance type, and click Next: Select Image.

4. On the Select Image tab, set the image, operating system, system architecture, and image version, and click Next: Select Storage and Bandwidth.

5. On the Select Storage and Bandwidth tab, select the system disk type, specify whether to allocate a public network IP address now, check Allocate IPv6 Address, and click Next: Set Security Groups and Hosts.

6. On the Set Security Groups and Hosts tab, set the log-in password and other related parameters for security groups and instances, and click Next: Confirm Configuration Information.

7. On the Confirm Configuration Information tab, confirm that the CVM information is correct and click Enable.

8. After purchasing the CVM, you can view the IPv6 address information in the CVM list.

> Note:
>
> - If the CVM is not allocated with an IPv6 address when you purchase it, you can choose More > Elastic IP > Manage IPv6 Addresses in the operation column of the corresponding CVM instance to allocate an IPv6 address to the primary network interface.

- If you want to allocate IPv6 addresses to other ENIs in the CVM, see Applying for and Releasing IPv6.

9. Log in to the CVM to configure IPv6. Because the methods of configuring IPv6 for various CVM operating systems are different, see Configuring IPv6 for Linux CVM and Configuring IPv6 for Windows CVM for detailed directions.

Step 4: Enabling the public network for the CVM IPv6 address (optional).

1. Log in to the VPC Console.

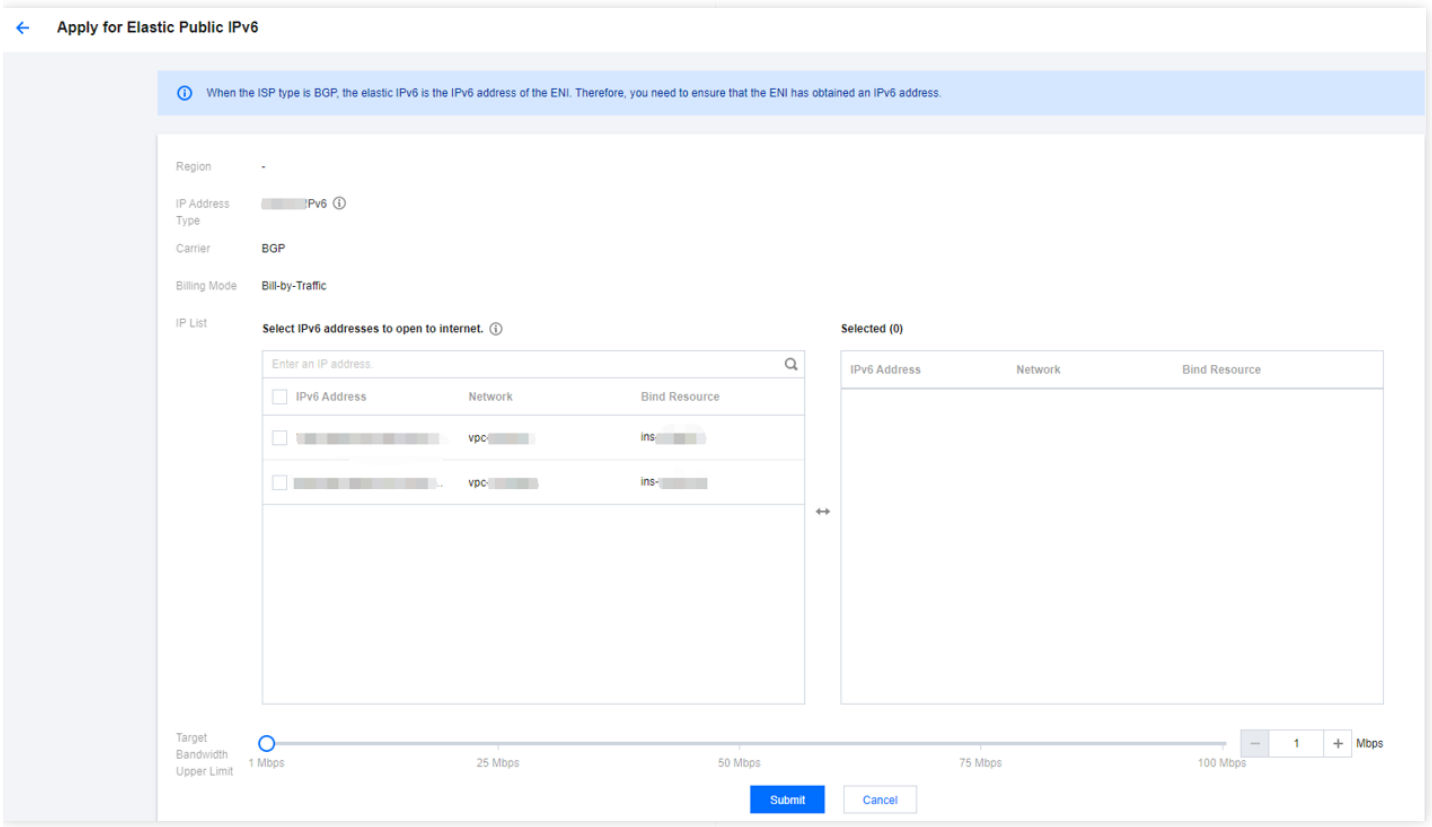
2. In the left directory, choose IP and Network Interface > Elastic IPv6.

3. Select the region where the CVM is located, click Apply to go to the management page.

4. Check the CVM IPv6 address, set the upper limit of the target bandwidth, and then click Submit.

> Note:
>
> - After the CVM has requested an IPv6 address, public network access is disabled by default. You can manage EIPv6 public network capabilities through Manage IPv6 Public Network Capabilities.

- When the ISP type is BGP, the EIPv6 address is the IPv6 address obtained by the CVM. Please ensure that the CVM has obtained the IPv6 address.
- A single operation can support enabling public network access for a maximum of 100 IPv6 addresses simultaneously. If more than 100 IPv6 addresses need public network access, please divide operations into multiple steps.



Step 5: Configuring IPv6 security group rules.

> Note:
>
> Inbound and outbound security group rules support configuration from a single IPv6 address or an IPv6 CIDR, where ::/130618222416261120 represents all IPv6 source addresses.

1. Log in to the VPC Console.
2. In the left directory, choose Security > Security Group. On the list page, click the security group ID bound to the CVM to enter the details page.
3. Select Inbound Rules and click Add Rules to add an inbound security group rule for IPv6, then click Finish.

4. Select Outbound Rules and click Add Rules to add an outbound security group rule for IPv6 and click Finish.

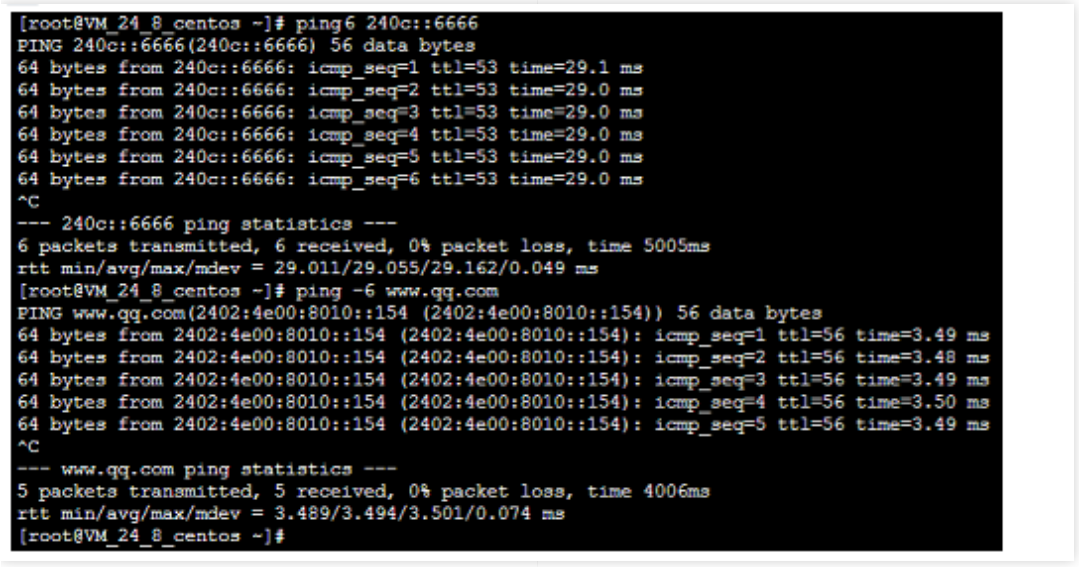
Step 6: Testing IPv6 connectivity.

> Note:
>
> - If you are testing public network connectivity, make sure that the public network has been enabled.
> - If the public network is not enabled to use SSH or remote desktop to test IPv6 connectivity, you can use the CVM SSH in the same VPC or the CVM tested through the remote desktop.

Linux CVM

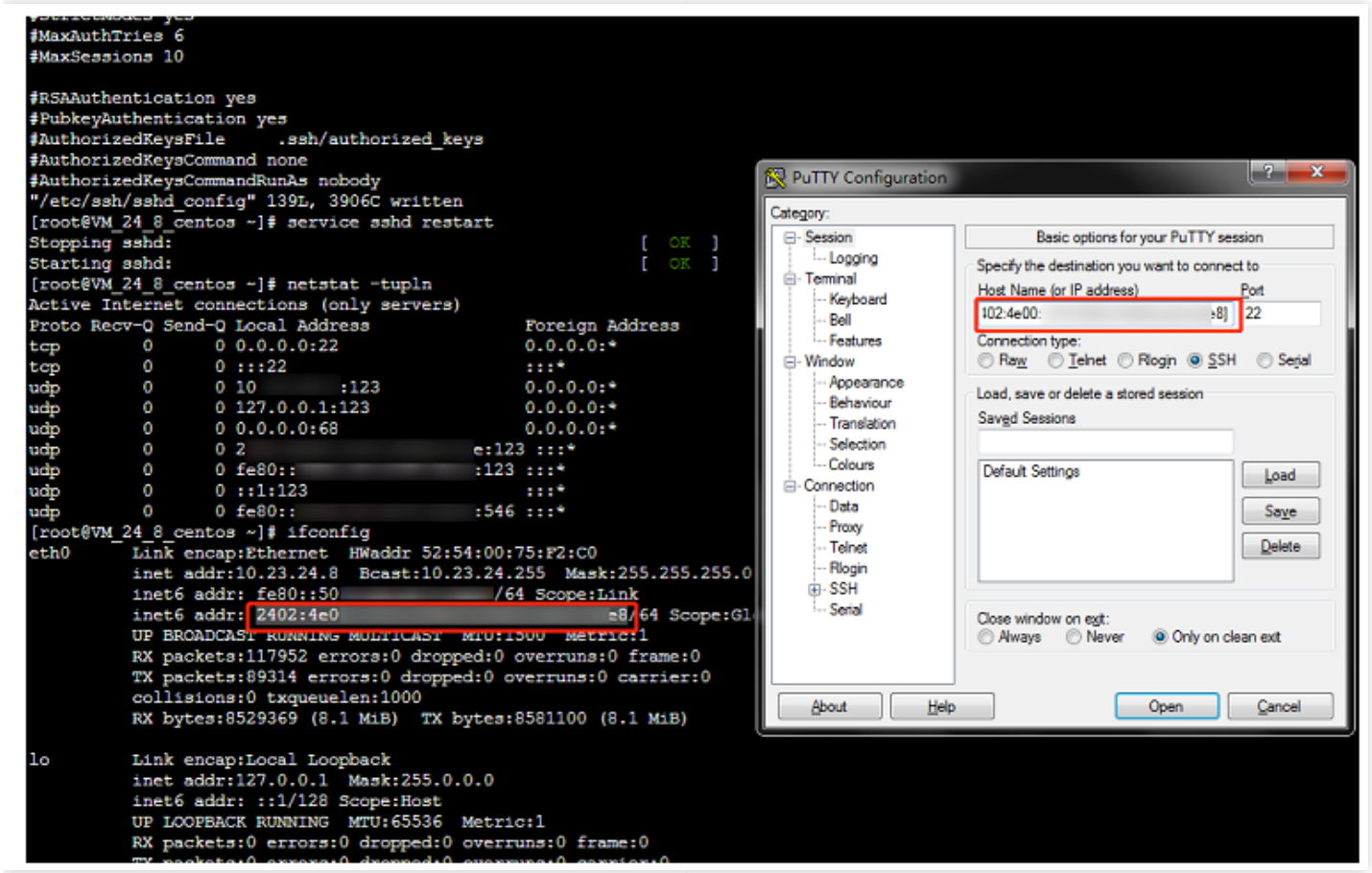
The Linux CVM can test IPv6 connectivity through operations such as Ping or ssh.

- Execute ping6 IPv6 address in the CVM to run a test, for example, ping6 240c::6666 , ping6 www.google.com , and ping6 IPv6 address in the same VPC . The successful result is shown in the figure below:

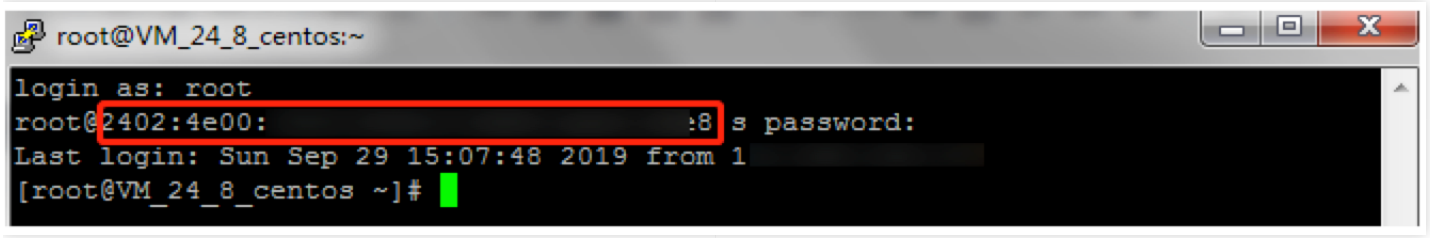


- Method 2: Use SSH to log in to the CVM via IPv6 address, follow these steps: Run the following command to view the IPv6 address, and use PuTTY or Xshell and other software to test whether you can use ssh to log in to the CVM through the IPv6 address.

  ifconfig



The successful result is shown in the figure below.



Windows CVM

Windows CVM can test IPv6 connectivity via Ping or remote desktop.

- Method 1: Test via Ping, follow these steps:

  On the operating system interface, select in the lower left corner, click to open the Windows PowerShell window, and execute ping -6 IPv6 address to run a test, for example, ping -6 240c::6666 or ping -6 the IPv6 address in the same VPC . The successful result is shown in the figure below.

- Method 2: Use the IPv6 address for remote desktop operation. For details on remote desktop operation, see Use Remote Desktop Connection to Log in to a Windows Instance.

Appendix

Configuring IPv6 for Linux CVM

There are two ways to configure IPv6 for Linux CVM: tool configuration and manual configuration.

- Tool Configuration: You can use the tool to configure IPv6 with one click.
- Manual Configuration: A certain level of proficiency in Linux commands is required.
  Select the corresponding method according to your actual situation. It is recommended to use a more efficient automatic configuration tool to configure the IPv6 address.

Image Type	Purchased Time	Is IPv6 enabled?	Tool Configuration (Recommended)	Manual Configuration
CentOS 7.5/CentOS 7.6	Purchase before 2019-06-30	No	enable_ipv6 tool	The following are four common mirror operation methods. If they do not meet your needs, submit a Ticket. - Configuring IPv6 for newly purchased CentOS 7.5/newly purchased CentOS 7.6 - Configuring IPv6 for CentOS 6.8 - Configuring IPv6 for CentOS 7.3/Stock CentOS 7.5/Stock CentOS 7.6 - Configuring IPv6 for Debian 8.2
CentOS 7.5/CentOS 7.6	Purchased after 2019-06-30	Yes	config_ipv6 tool	The following lists the operation methods for four commonly used images. If they do not meet your needs, please submit a work order request: Configure IPv6 for New CentOS 7.5/New

Image Type	Purchased Time	Is IPv6 enabled?	Tool Configuration (Recommended)	Manual Configuration
				CentOS 7.6 Configure IPv6 for CentOS 6.8 Configure IPv6 for CentOS 7.3/Existing CentOS 7.5/Existing CentOS 7.6 Configure IPv6 for Debian 8.2
CentOS 6/CentOS 7 (excluding 7.5/7.6) Ubuntu14.04/Ubuntu 12.04 Debian 8/Debian 9 CoreOS 17	Purchase before 2019-11-13 01:00	No	enable_ipv6 tool	The following lists the operation methods for four commonly used images. If they do not meet your needs, please submit a work order request: Configure IPv6 for New CentOS 7.5/New CentOS 7.6 Configure IPv6 for CentOS 6.8 Configure IPv6 for CentOS 7.3/Existing CentOS 7.5/Existing CentOS 7.6 Configure IPv6 for Debian 8.2
CentOS 6/CentOS 7 (excluding 7.5/7.6) Ubuntu14.04/Ubuntu 12.04 Debian 8/Debian 9 CoreOS 17	Purchase after 2019-11-13 01:00	Yes	config_ipv6 tool	The following lists the operation methods for four commonly used images. If they do not meet your needs, please submit a work order request: Configure IPv6 for New CentOS 7.5/New CentOS 7.6 Configure IPv6 for CentOS 6.8 Configure IPv6 for CentOS 7.3/Existing

Image Type	Purchased Time	Is IPv6 enabled?	Tool Configuration (Recommended)	Manual Configuration
				CentOS 7.5/Existing CentOS 7.6 Configure IPv6 for Debian 8.2
FreeBSD,Suse,Ubuntu18	Purchase before 2019-11-13 01:00	No	Not supported.	The following lists the operation methods for four commonly used images. If they do not meet your needs, please submit a work order request: Configure IPv6 for New CentOS 7.5/New CentOS 7.6 Configure IPv6 for CentOS 6.8 Configure IPv6 for CentOS 7.3/Existing CentOS 7.5/Existing CentOS 7.6 Configure IPv6 for Debian 8.2
FreeBSD,Suse,Ubuntu18	Purchase after 2019-11-13 01:00	Yes	Not supported.	The following lists the operation methods for four commonly used images. If they do not meet your needs, please submit a work order request: Configure IPv6 for New CentOS 7.5/New CentOS 7.6 Configure IPv6 for CentOS 6.8 Configure IPv6 for CentOS 7.3/Existing CentOS 7.5/Existing CentOS 7.6 Configure IPv6 for Debian 8.2

Tool Configuration

Select the corresponding configuration method according to whether IPv6 is enabled for the CVM:

- For CVM without IPv6 enabled: enable_ipv6 tool configuration .
- CVM with IPv6 enabled: config_ipv6 tool configuration .

enable_ipv6 Tool Configuration

The enable_ipv6 tool can configure IPv6 addresses for CVM instances that have been allocated with IPv6 addresses with one click.

Limits

- The enable_ipv6 tool is only applicable to VPC network environments.
- The enable_ipv6 tool will automatically restart the network interface and network service when it runs. The network may be unavailable for a short time. Execute with caution.
  Directions

1. Log in to the CVM and directly execute the following command in the CVM to download the enable_ipv6 tool:

   ```
   wget https://iso-1251783334.cos.ap-city.test.com/scripts/enable_ipv6.sh
   ```

2. After you grant execution permissions, execute with administrator permissions:

   ```
   chmod +x ./enable_ipv6.sh
   ./enable_ipv6.sh [Network interface name]
   # Example 1: ./enable_ipv6.sh eth0
   # Example 2: ./enable_ipv6.sh eth1
   ```

3. (This step is only applicable to the CoreOS operating system.) Restart the CVM to make the above configuration take effect.

config_ipv6 Tool Configuration

The config_ipv6 tool can configure IPv6 addresses for CVM instances that have IPv6 enabled and have been allocated with IPv6 addresses with one click.

Limits

- The config_ipv6 tool is only applicable in a VPC network environment.
- When the config_ipv6 tool is running, it will automatically restart the network interface and network service. The network may be unavailable for a short time. Execute with caution.

Directions

1. Log in to the CVM and execute the following command directly in the CVM to download the config_ipv6 tool:

   wget https://iso-1251783334.cos.ap-city.test.com/scripts/config_ipv6.sh

2. After you grant execution permissions, execute with administrator permissions:

   ```
   chmod +x ./config_ipv6.sh
   ./config_ipv6.sh [Network interface name]
   # Example 1: ./config_ipv6.sh eth0
   # Example 2: ./config_ipv6.sh eth1
   ```

3. (This step is only applicable to the CoreOS operating system.) Restart the CVM to make the above configuration take effect.

For automatic configuration of IPv6 instances, such as batch configuration, it is recommended to call using instance custom data in conjunction with scripts. For details, see Instance Custom Data. The following is a script example (assuming it is a RHEL series, Bash Shell script).

> Note:
>
> This example only configures eth0. In actual operation, make sure to modify it to the actual network interface name.

```
#!/bin/sh
install_dir=/usr/sbin
install_path="$install_dir"/config-ipv6
if [ ! -f "$install_path" ]; then
    tool_url="https://iso-1251783334.cos.ap-city.test.com/scripts/config_ipv6.sh"
    # download the tool
    if ! wget "$tool_url" -O "$install_path"; then
        echo "[Error] download tool failed, code $?"
        exit "$?"
    fi
fi
# chmod the tool
if ! chmod +x "$install_path"; then
    echo "[Error] chmod tool failed, code $?"
    exit "$?"
fi
```

```
# run the tool
$install_path eth0
```

Manual Configuration

The following are four common Linux CVM operation methods:

- Configuring IPv6 for newly purchased CentOS 7.5/newly purchased CentOS 7.6
- Configuring IPv6 for CentOS 6.8
- Configuring IPv6 for CentOS 7.3/Stock CentOS 7.5/Stock CentOS 7.6
- Configuring IPv6 for Debian 8.2

> Note:
>
> - Newly purchased CentOS 7.5/Newly purchased CentOS 7.6 refers to CVM purchased after June 30, 2019.
> - Stock CentOS 7.5/Stock CentOS 7.6 refers to CVM purchased before June 30, 2019.

Configuring IPv6 for newly purchased CentOS7.5/Newly purchased CentOS7.6

1. Log in to the Cloud Virtual Machine console and the instance.

2. Execute the following command to open the ifcfg-eth0 file in the folder /etc/sysconfig/network-scripts/ .

   ```
   vim /etc/sysconfig/network-scripts/ifcfg-eth0
   ```

3. Press i to switch to edit mode and add the following content.

   ```
   DHCPV6C=yes
   ```

```
# Created by cloud-init on instance boot automatically, do not edit.
#
BOOTPROTO=dhcp
DEVICE=eth0
HWADDR=52:54:00:06:d5:57
NM_CONTROLLED=no
ONBOOT=yes
PERSISTENT_DHCLIENT=yes
TYPE=Ethernet
USERCTL=no
DHCPV6C=yes
~
~
```

4. Press Esc and enter :wq to save the file and return.
5. Execute the following commands in sequence to check whether an IPv6 address has been obtained.

   # If the CVM has multiple network interfaces, execute dhclient -6 network interface name, such as dhcl
   ient -6 eth0
   dhclient -6 or dhclient -6 network interface name
   ifconfig

```
[root@VM_23_16_centos ~]# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 1                netmask 255.255.255.0  broadcast 1
        inet6 f                          prefixlen 64  scopeid 0x20<link>
        inet6 2                          a8e  prefixlen 64  scopeid 0x0<global>
        ether 52:54:00:06:d5:57  txqueuelen 1000  (Ethernet)
        RX packets 5581952  bytes 567752177 (541.4 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4779345  bytes 683082390 (651.4 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

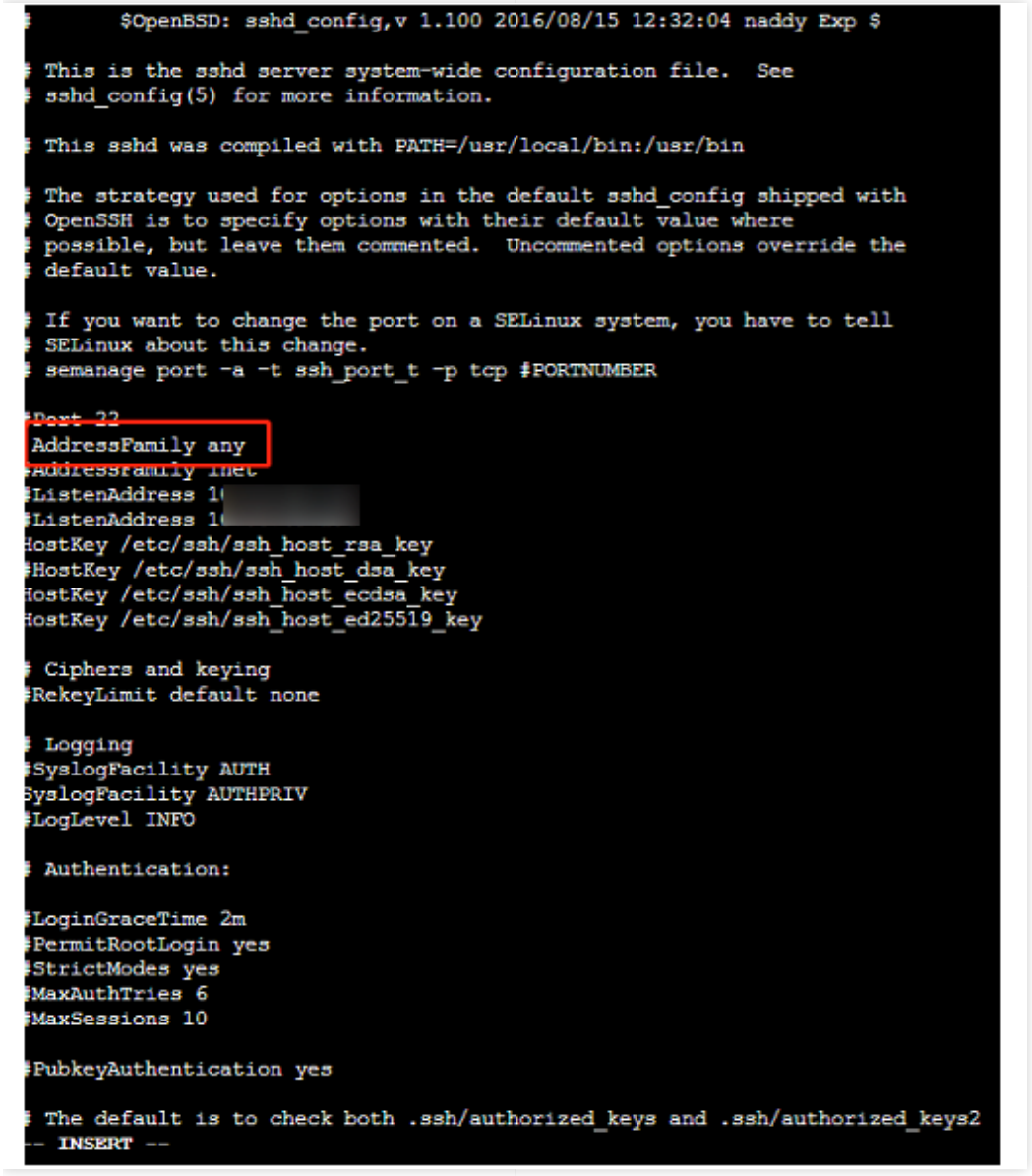
lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 18  bytes 1936 (1.8 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 18  bytes 1936 (1.8 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

6. Execute the following command to open sshd_config file in the folder /etc/ssh/ .

   vim /etc/ssh/sshd_config

   7. Press i to switch to edit mode and delete AddressFamily any comment (delete the preceding #),

and enable IPv6 listening for applications such as ssh.

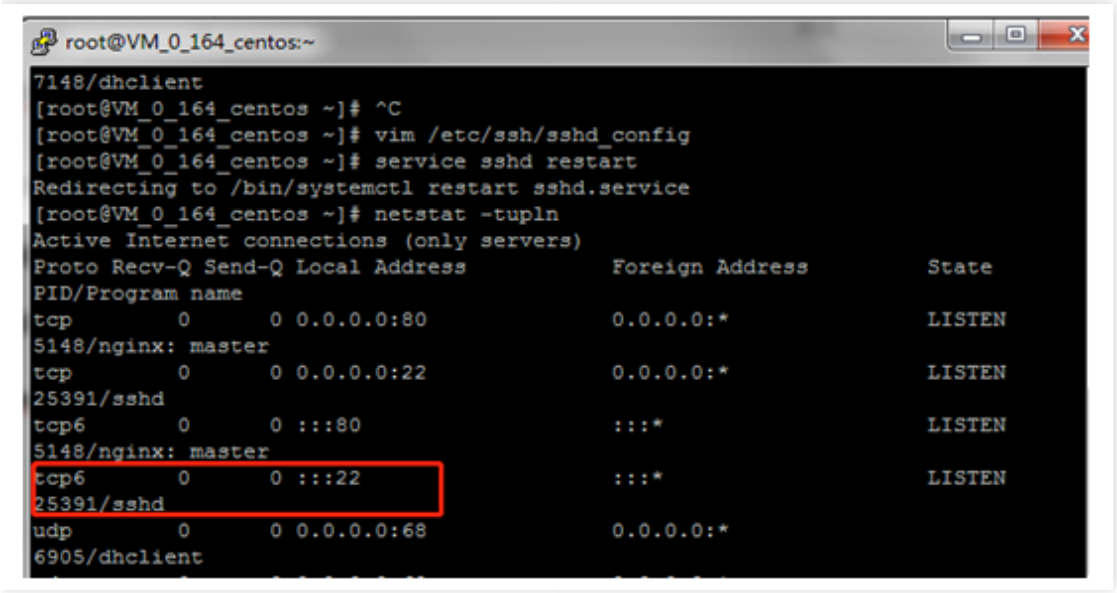


8. Press Esc and enter :wq to save the file and return.
9. Run the following command to restart the ssh process.

   service sshd restart

   10. Run the following command to check whether ssh is listening on IPv6.

   netstat -tupln



Configuring IPv6 for CentOS 6.8

1. Remotely connect instance. For detailed operations, see Log in and Remote Connection.

2. Execute the following command to check whether the IPv6 service is enabled for the instance:

   ip addr | grep inet6
   or
   ifconfig | grep inet6

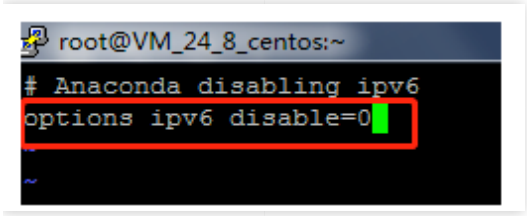
- If the IPv6 service is not enabled for the instance, continue to enable IPv6 service according to the following steps.
- If inet6 related content is returned, it indicates the IPv6 service is enabled for the instance, and you can skip to Step 9 for the following operations.

3. Execute the following command to open the ipv6.conf file in the folder /etc/modprobe.d/ .

   vi /etc/modprobe.d/ipv6.conf

4. Press i to switch to edit mode and set the following kernel parameters to 0.

   options ipv6 disable=0

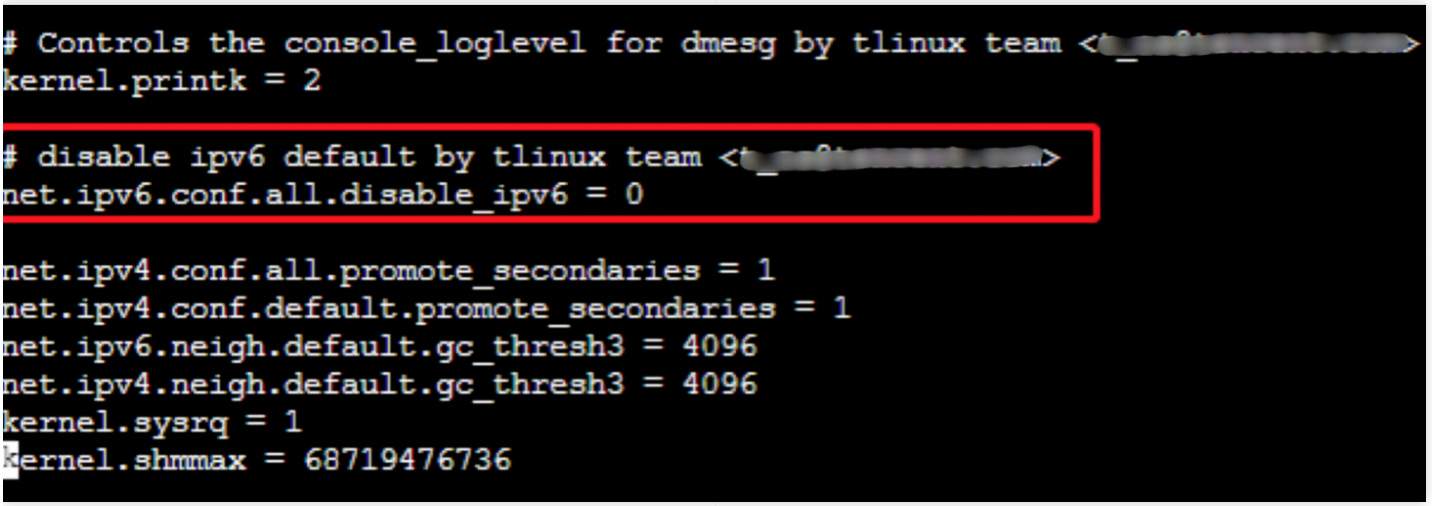


5. Press Esc and enter :wq to save the file and return.
6. Execute the following command to open the sysctl.conf.first file in the folder etc .

vim /etc/sysctl.conf.first

7. Press i to switch to edit mode and set the following configuration file parameters to 0.

net.ipv6.conf.all.disable_ipv6 = 0

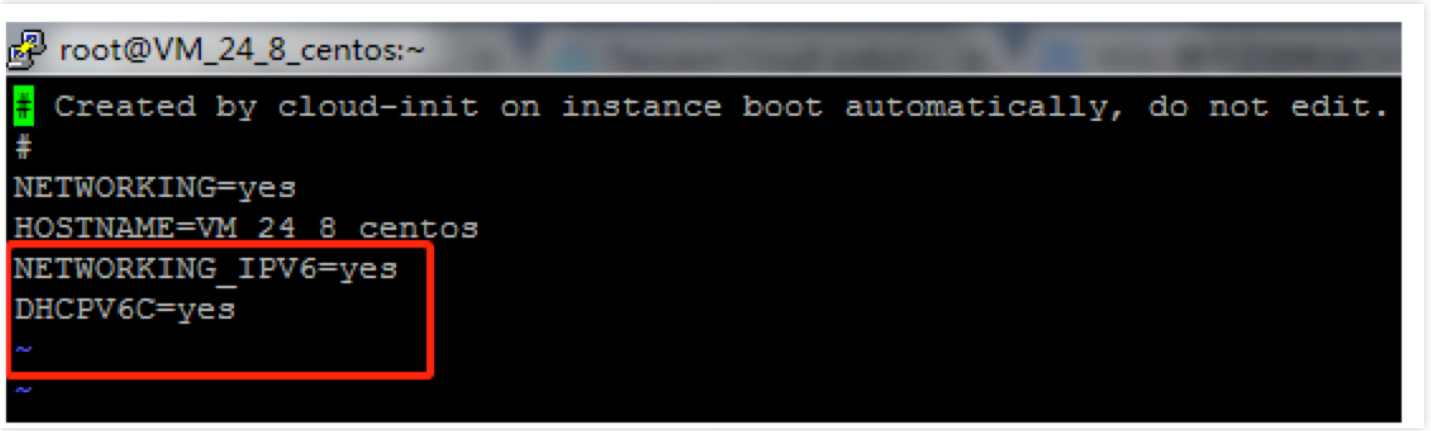


8. Press Esc and enter :wq to save the file and return.
9. Execute the following command to open the sysctl.conf.first file in the folder etc .

vi /etc/sysconfig/network

10. Press i to switch to edit mode and add the following content.

NETWORKING_IPV6=yes
DHCPV6C=yes

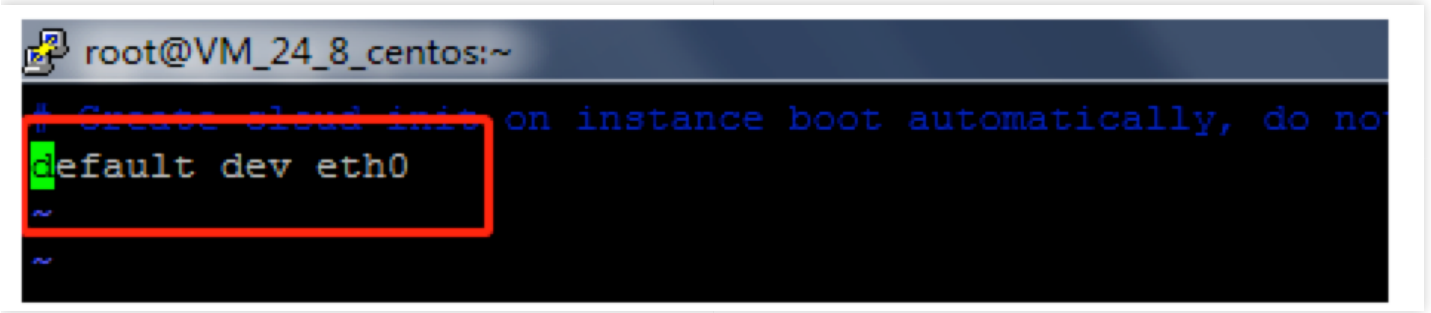


11. Press Esc and enter :wq to save the file and return.
12. Execute the following command to open the network file in the folder /etc/sysconfig/ .

    vim /etc/sysconfig/network-scripts/route6-eth0

    13. Press i to switch to edit mode, add the following content, and add a default exit for IPv6 of the network interface.

    default dev eth0



14. Press Esc and enter :wq to save the file and return.
15. Restart the CVM only through service network restart , IPv6 cannot be loaded normally.
16. Run the following command to check whether IPv6 is loaded normally after restart.

    sysctl -a | grep ipv6 | grep disable

```
[root@VM 24 8 centos ~]#  sysctl -a | grep ipv6 | grep disable
net.ipv6.conf.all.disable_ipv6 = 0
net.ipv6.conf.default.disable_ipv6 = 0
net.ipv6.conf.lo.disable_ipv6 = 0
net.ipv6.conf.eth0.disable_ipv6 = 0
net.ipv6.conf.eth1.disable_ipv6 = 0
```

17. Execute the following commands in sequence to check whether an IPv6 address has been obtained.

    # If the CVM has multiple network interfaces, execute dhclient -6 network interface name, such as dhcl
    ient -6 eth0
    dhclient -6 or dhclient -6 network interface name
    ifconfig

```
[root@VM_24_8_centos ~]# ifconfig
eth0      Link encap:Ethernet  HWaddr 52:54:00:75:F2:C0
          inet addr:10.23.24.8  Bcast:10.23.24.255  Mask:255.255.255.0
          inet6 addr: fe80::5[redacted]:f2c0/64 Scope:Link
          inet6 addr: 2402:[redacted]:2be8/64 Scope:Global
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:4074 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2772 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:274150 (267.7 KiB)  TX bytes:260211 (254.1 KiB)

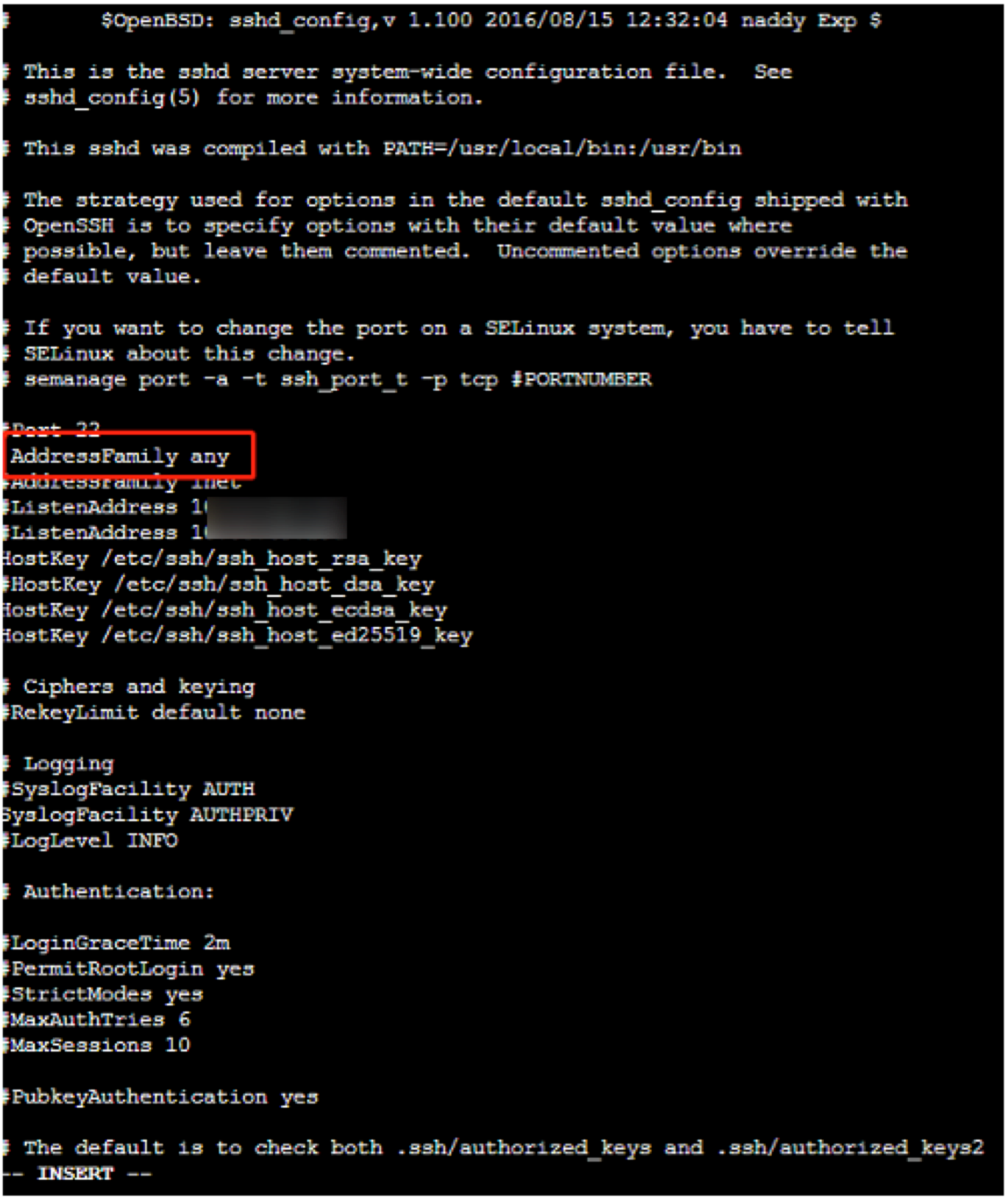
eth1      Link encap:Ethernet  HWaddr 20:90:6F:74:53:D7
          inet6 addr: 2402:[redacted]:575e/64 Scope:Global
          inet6 addr: fe80::[redacted]:3d7/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:318 errors:0 dropped:0 overruns:0 frame:0
          TX packets:7 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:16124 (15.7 KiB)  TX bytes:696 (696.0 b)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
```

18. Execute the following command to open sshd_config file in the folder /etc/ssh/ .

    vim /etc/ssh/sshd_config

    19. Press i to switch to edit mode and delete AddressFamily any comment (delete the preceding #),
        and enable IPv6 listening for applications such as ssh.

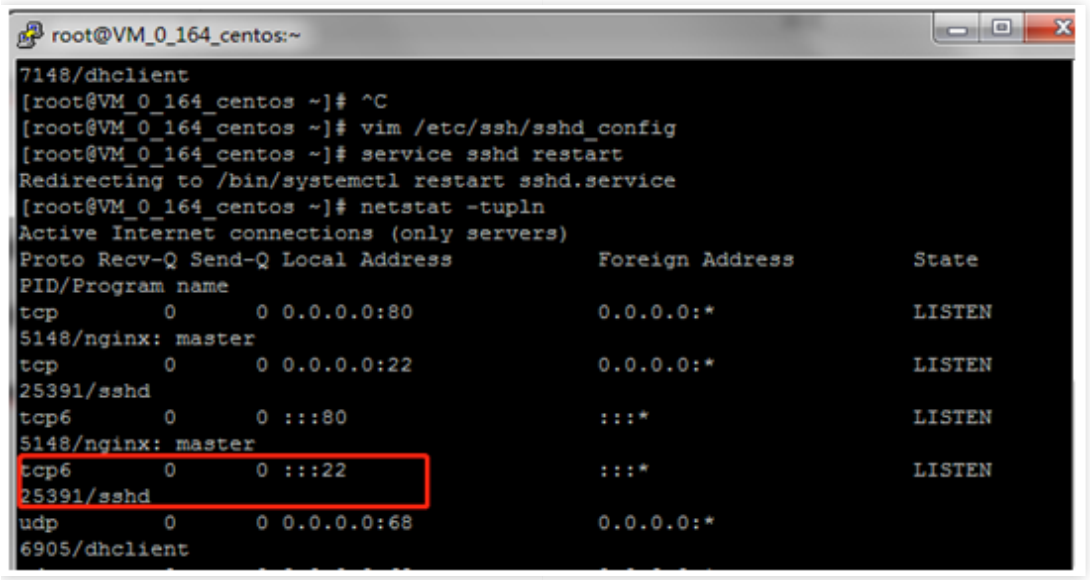


20. Press Esc and enter :wq to save the file and return.
21. Run the following command to restart the ssh process.

service sshd restart

22. Run the following command to check whether ssh is listening on IPv6.

netstat -tupln



Configuring IPv6 for CentOS 7.3/Stock CentOS 7.5/Stock CentOS 7.6

1. Remotely connect instance. For detailed operations, see Log in and Remote Connection.

2. Execute the following command to check whether the IPv6 service is enabled for the instance:

   ip addr | grep inet6
   or
   ifconfig | grep inet6

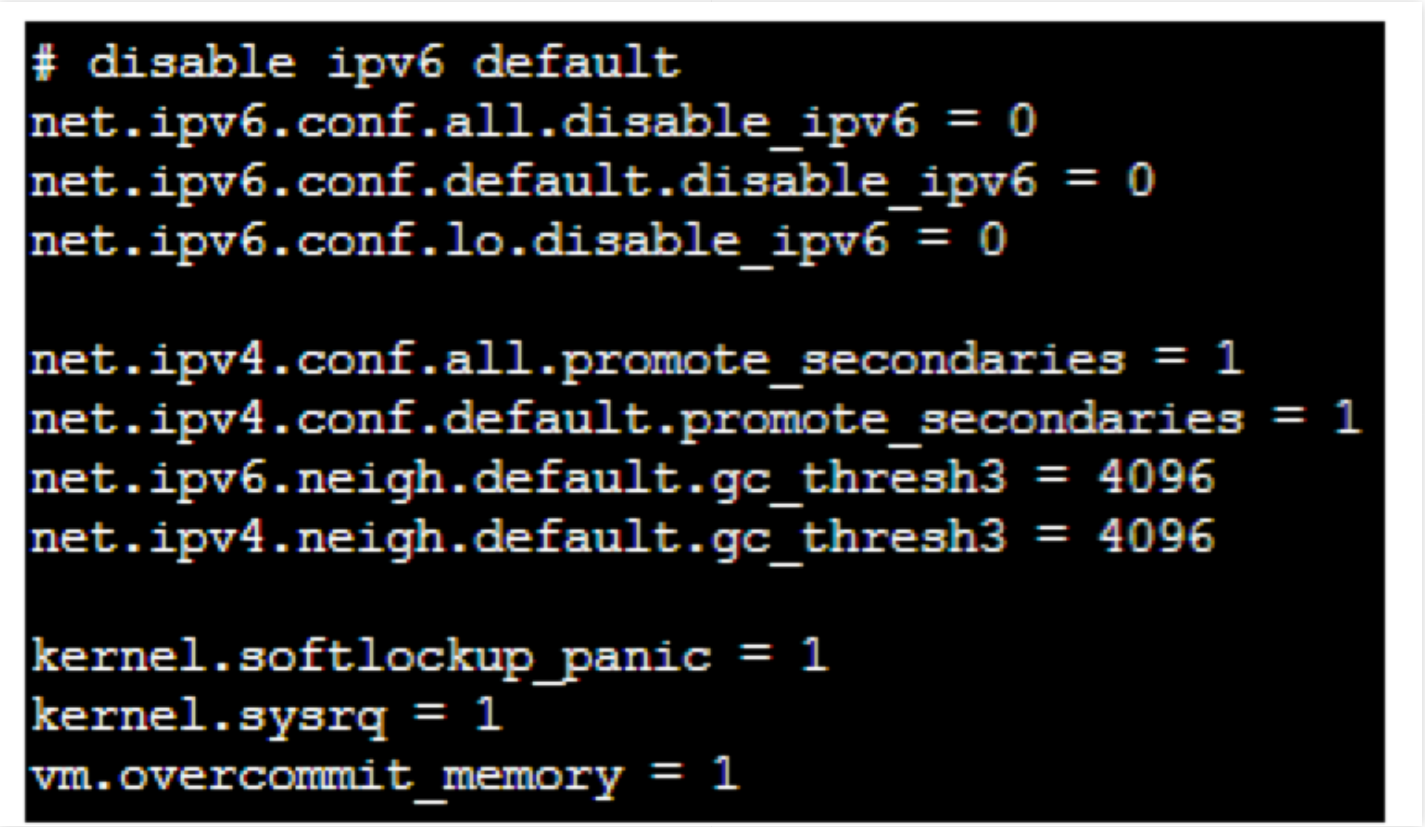
- If the IPv6 service is not enabled for the instance, continue to enable IPv6 service according to the following steps.
- If inet6 related content is returned, it indicates the IPv6 service is enabled for the instance, you can skip to Step 8 for the following operations.

3. Execute the following command to open sysctl.conf file in the folder etc .

   vim /etc/sysctl.conf

4. Press i to switch to edit mode and set the following IPv6 related parameters to 0.

    net.ipv6.conf.all.disable_ipv6 = 0
    net.ipv6.conf.default.disable_ipv6 = 0
    net.ipv6.conf.lo.disable_ipv6 = 0



5. Press Esc and enter :wq to save the file and return.

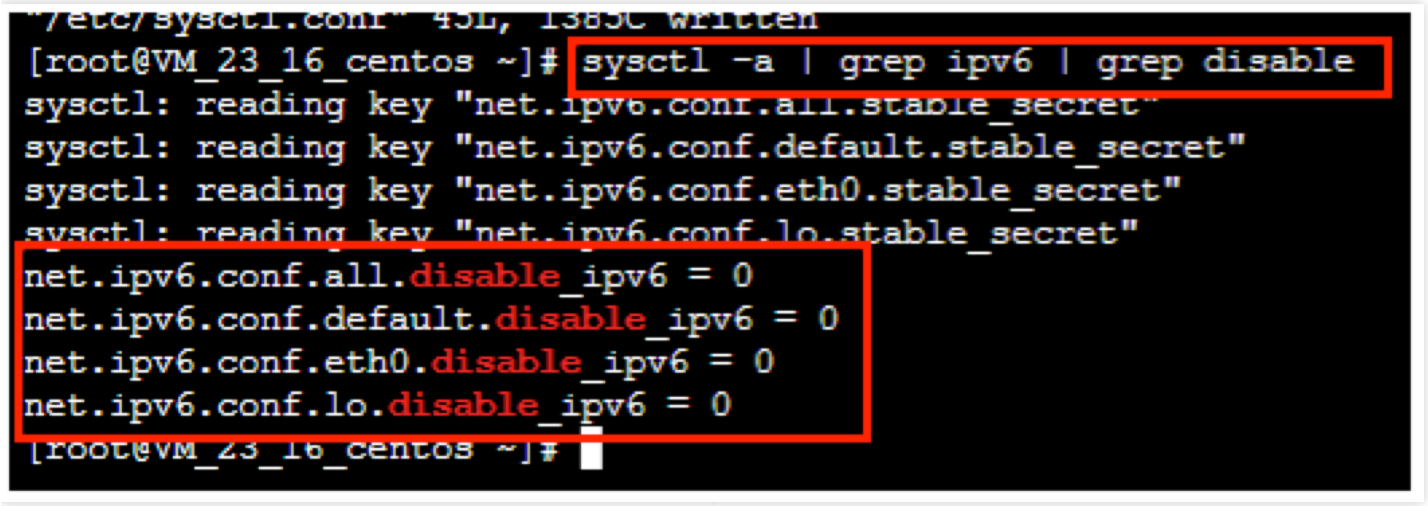
6. Run the following command to load the parameters.

    sysctl -p

7. Run the following command to check whether the modification is successful.

    sysctl -a | grep ipv6 | grep disable

If the result is as follows, the modification has been successful.

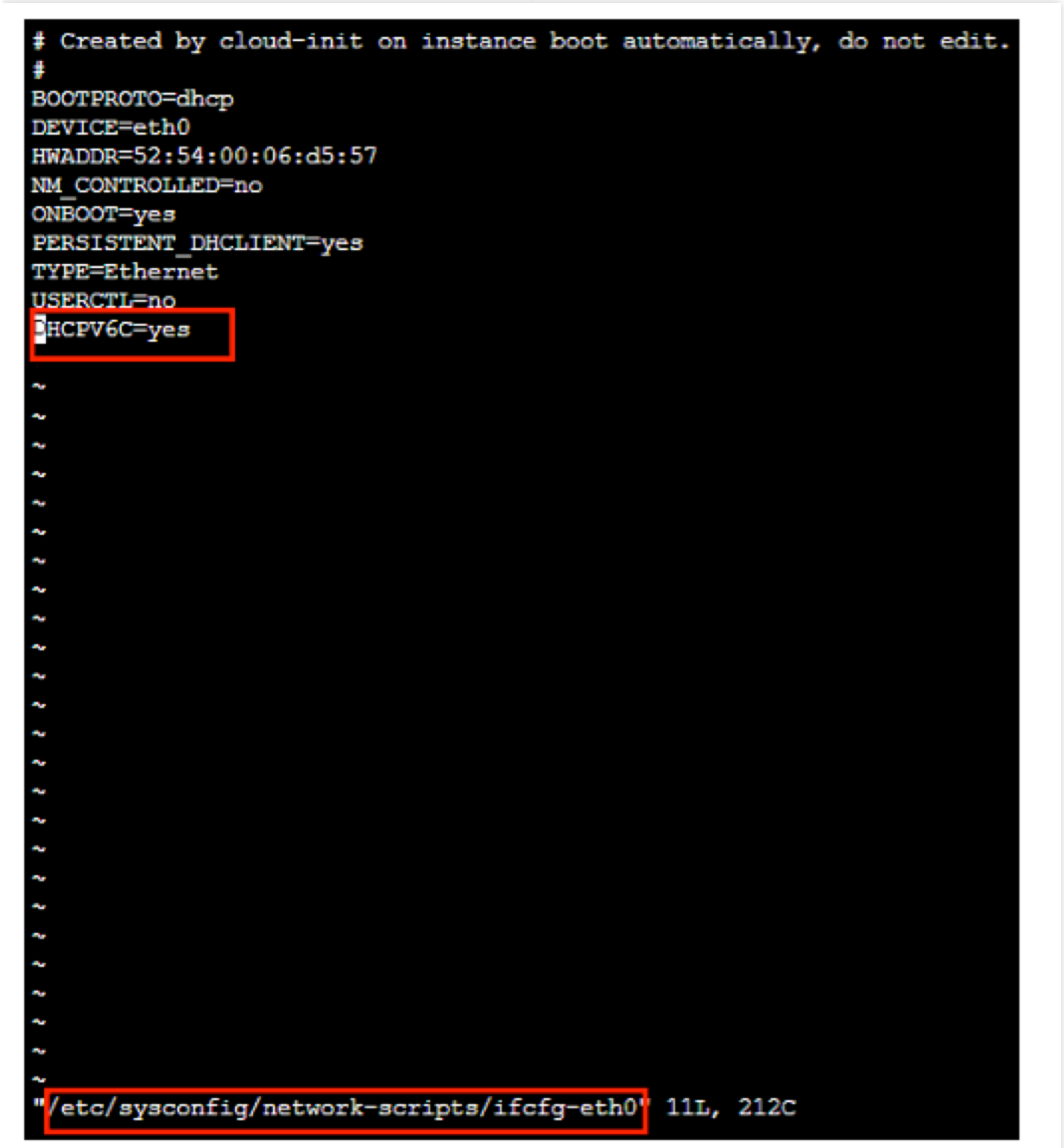


8. Execute the following command to open or create ifcfg-eth0 file in the folder /etc/sysconfig/network-scripts/ .

vim /etc/sysconfig/network-scripts/ifcfg-eth0

9. Press i to switch to edit mode and add the following content.

DHCPV6C=yes

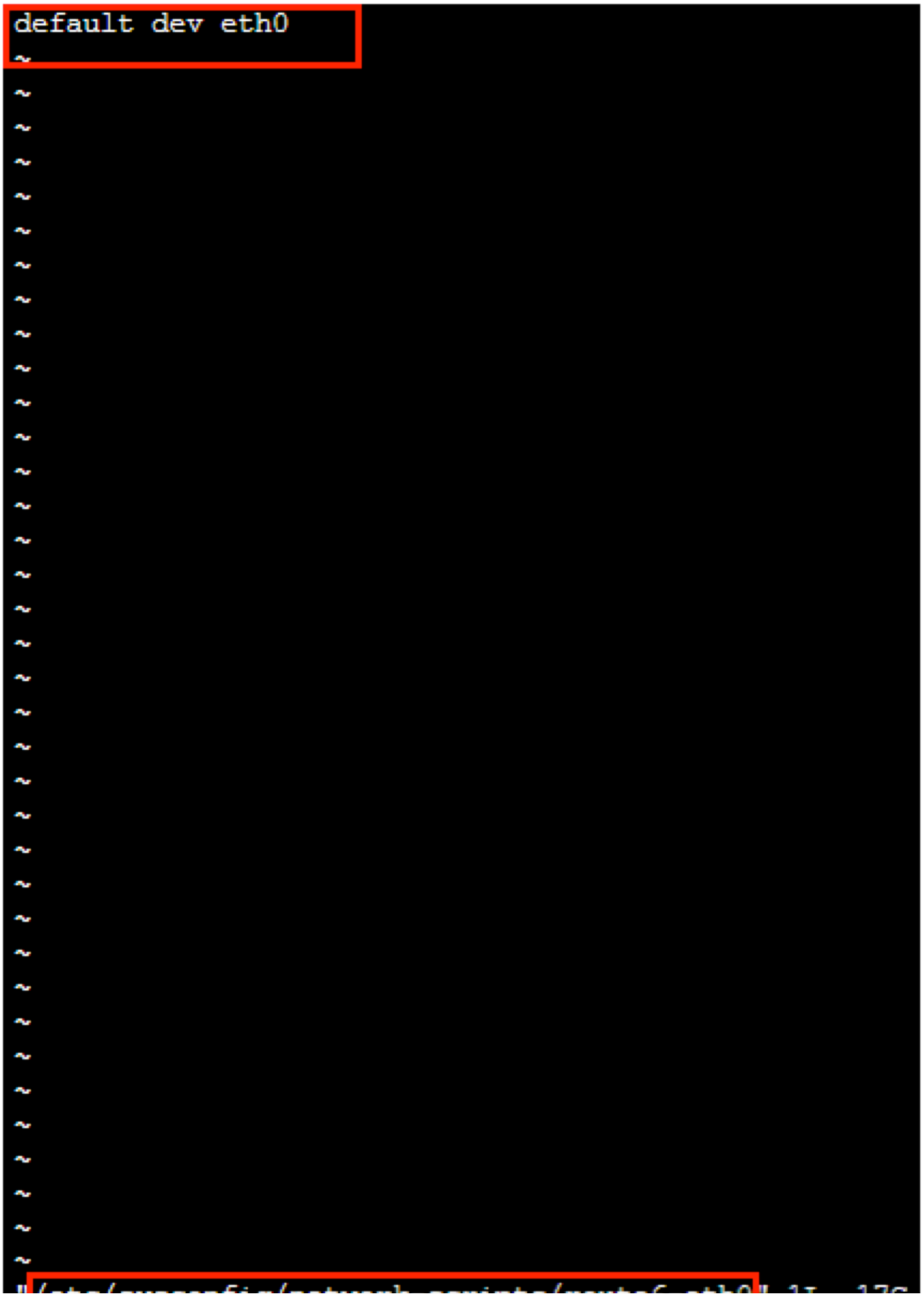


10. Press Esc and enter :wq to save the file and return.
11. Execute the following command to open the network file in the folder /etc/sysconfig/ .

    vim /etc/sysconfig/network-scripts/route6-eth0

12. Press i to switch to edit mode, add the following content, and add a default exit for IPv6 of the network interface.

default dev eth0


default dev eth0

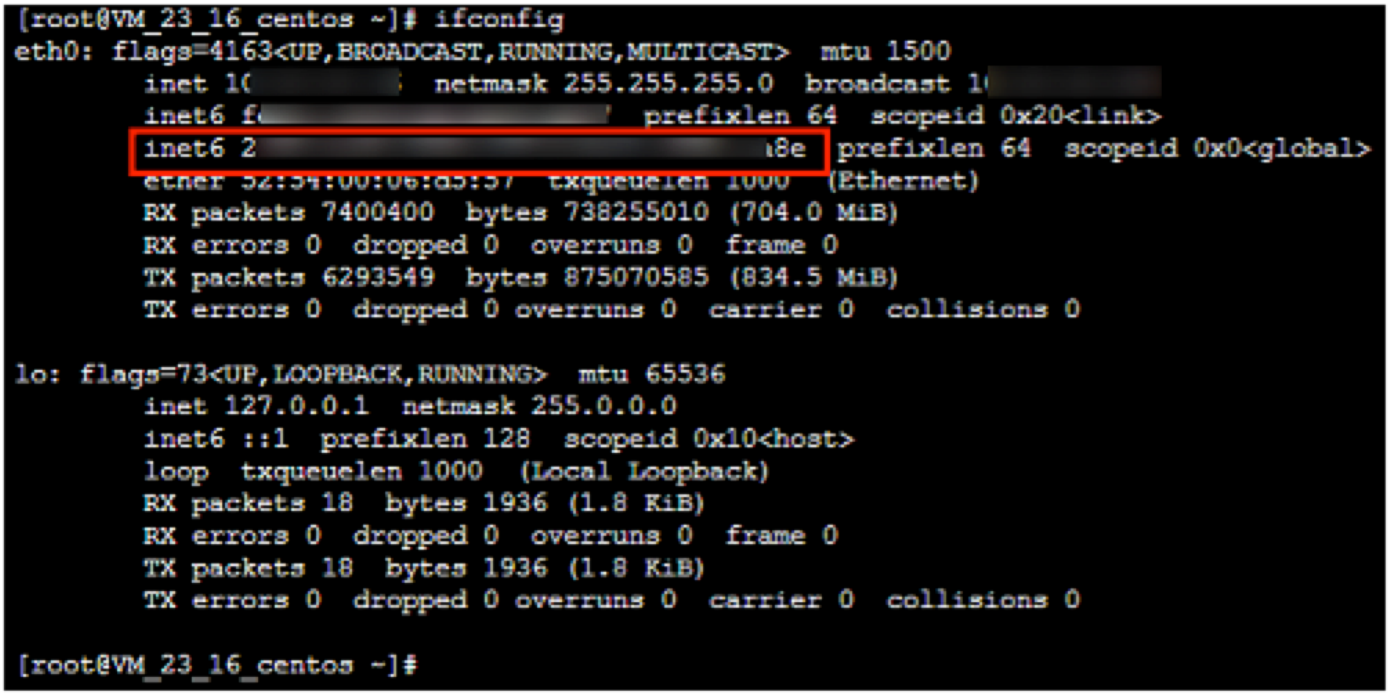


13. Press Esc and enter :wq to save the file and return.
14. Run the following command to restart the network interface.

service network restart
or
systemctl restart network

15. Execute the following commands in sequence to check whether an IPv6 address has been obtained.

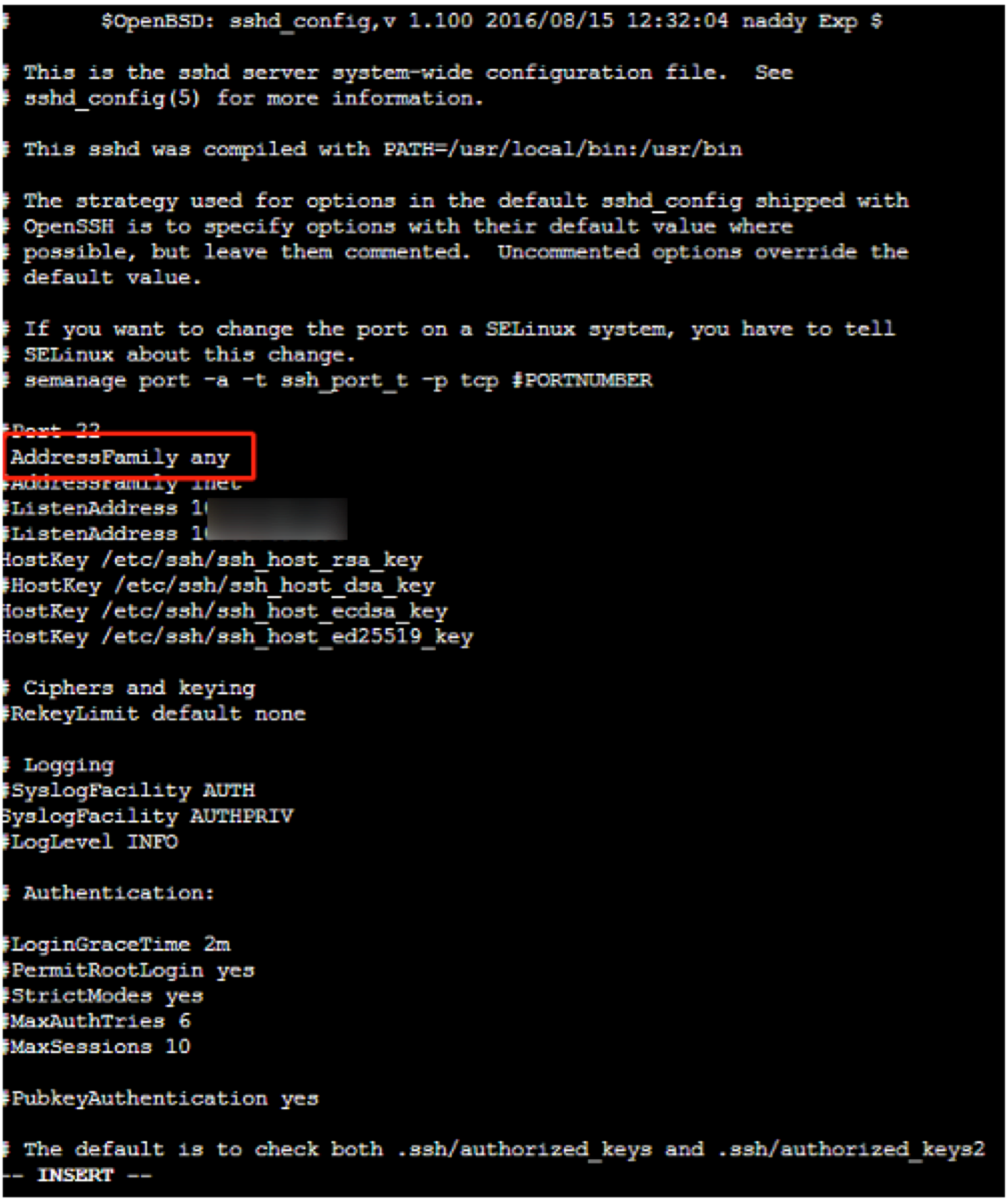
If the CVM has multiple network interfaces, execute dhclient -6 network interface name, such as dhclient -6 eth0
dhclient -6 or dhclient -6 network interface name
ifconfig



16. Execute the following command to open sshd_config file in the folder /etc/ssh/ .

vim /etc/ssh/sshd_config

17. Press i to switch to edit mode and delete AddressFamily any comment (delete the preceding #), and enable IPv6 listening for applications such as ssh.

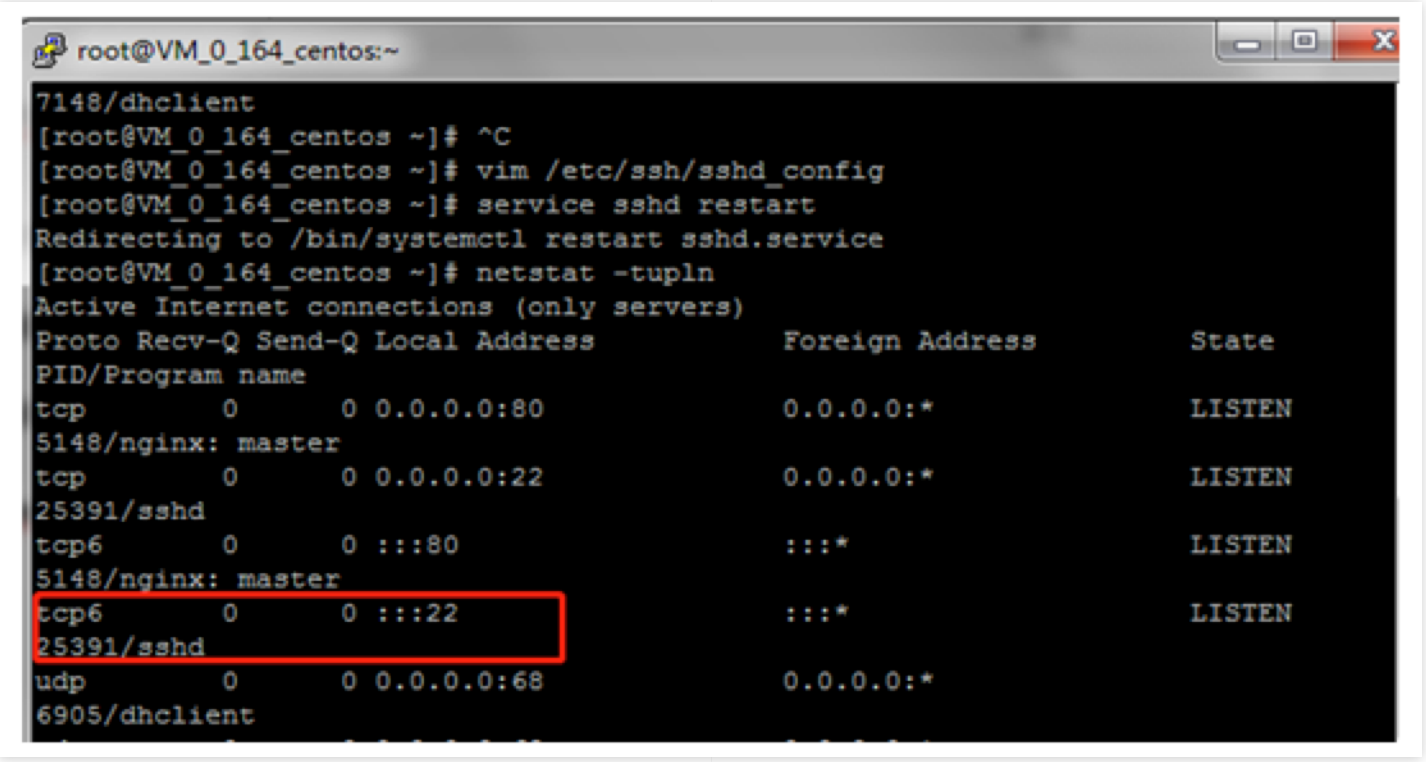


18. Press Esc and enter :wq to save the file and return.
19. Run the following command to restart the ssh process.

service sshd restart

20. Run the following command to check whether ssh is listening on IPv6.

netstat -tupln



Configuring IPv6 for Debian 8.2

1. Remotely connect instance. For detailed operations, see Log in and Remote Connection.

2. Execute the following command to check whether the IPv6 service is enabled for the instance:

   ip addr | grep inet6
   or
   ifconfig | grep inet6

- If the IPv6 service is not enabled for the instance, continue to enable IPv6 service according to the following steps.
- If inet6 related content is returned, it indicates the IPv6 service is enabled for the instance, you can skip to Step 6 for the following operations.

3. Execute the following command to open sysctl.conf file in the folder etc .

```
vim /etc/sysctl.conf
```

4. Press i to switch to edit mode and set the following IPv6 related parameters to 0.

```
net.ipv6.conf.all.disable_ipv6 = 0
net.ipv6.conf.default.disable_ipv6 = 0
```

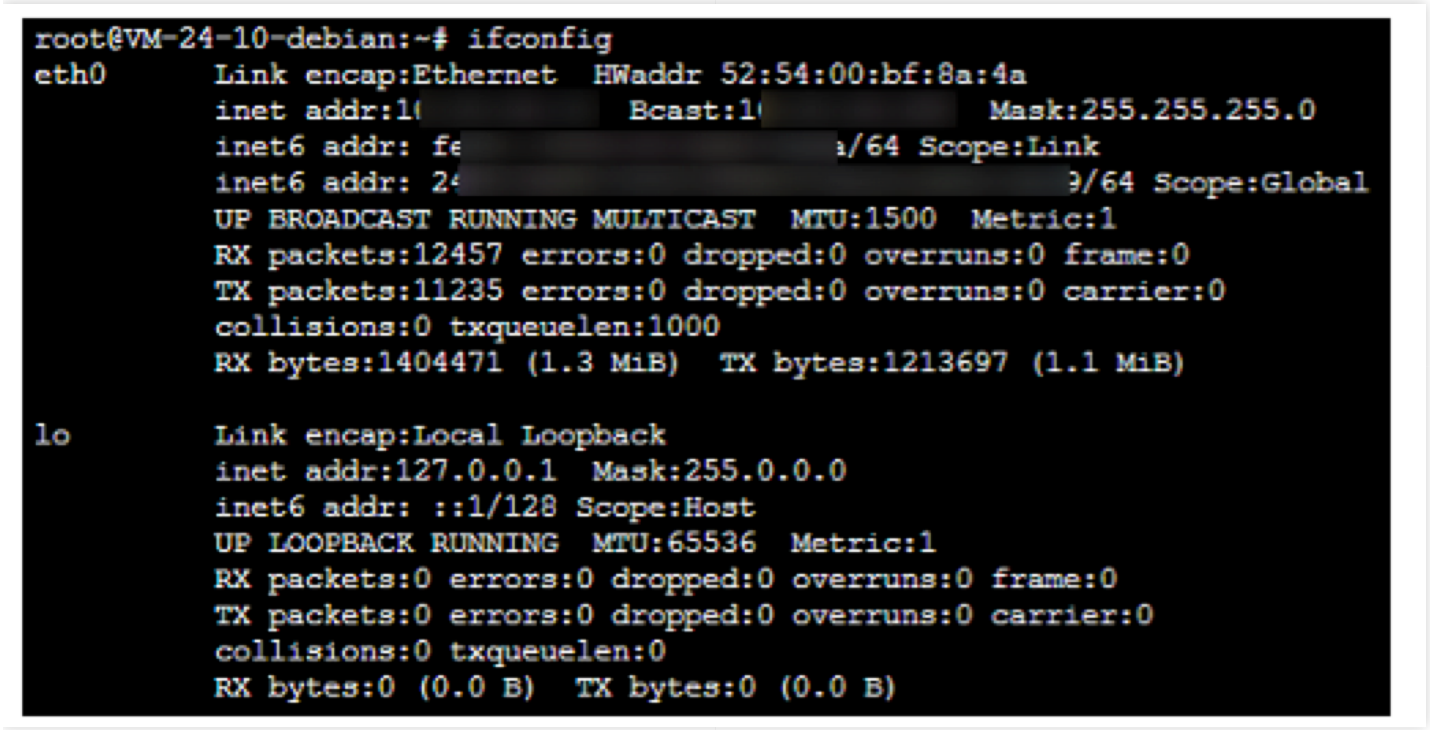
5. Press Esc and enter :wq to save the file and return.

6. Run the following command to load the parameters.

```
sysctl -p
```

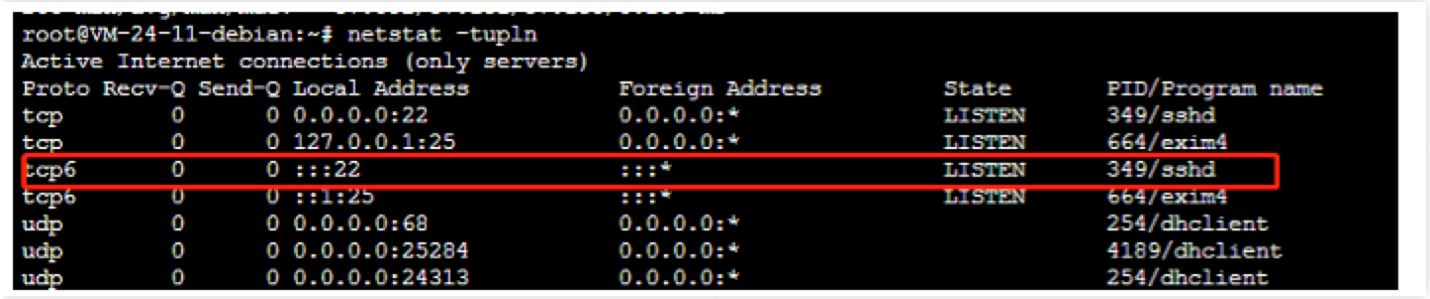
7. Execute the following commands in sequence to check whether an IPv6 address has been obtained.

```
# If the CVM has multiple network interfaces, execute dhclient -6 network interface name, such a
s dhclient -6 eth0
dhclient -6 or dhclient -6 network interface name
ifconfig
```



8. In the Debian 8.2 system, IPv6 listening is enabled for ssh (port 22) by default. No special configuration is required. You can run the following command to view it.

```
netstat -tupln
```



9. Run the following command to configure the default route.

```
ip -6 route add default dev eth0
```

Configuring IPv6 for Windows CVM

The following operation takes Windows 2012 as an example:

1. Log in to the CVM instance, choose Control Panel > Network and Internet > Network and Sharing Center of the operation system, and click and edit the Ethernet network interface.

2. In the Ethernet Status pop-up window, click Attribute.

3. In the Ethernet Attributes pop-up window, select Internet Protocol Version 6 (TCP/IPv6) and click Attribute.

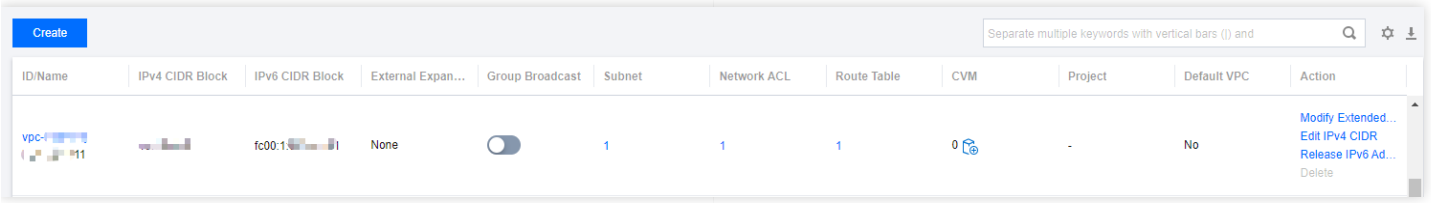
4. In the Internet Protocol Version 6 (TCP/IPv6) Attribute pop-up window, manually enter the IPv6 address obtained by the CVM in Step 3 and set the DNS (recommended to use 240c::6666), and click OK.

5. On the operating system interface, select  in the lower left corner, click  , open the Windows PowerShell window, and execute the following commands in sequence to configure the default route and view the IPv6 address.

```
netsh interface ipv6 add route ::/130618223492100096 "Ethernet"
ipconfig
```

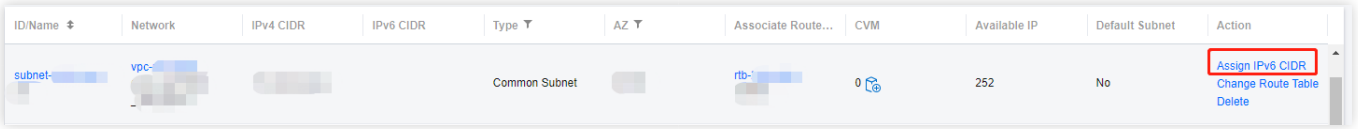
Operation Guide
Allocating and Releasing IPv6 CIDR for VPC

1. Log in to the VPC Console.
2. On the top of the VPC list, select Region to display all the VPC information in the region.
3. In the operation column of the row where the VPC is located, for which IPv6 needs to be enabled, click Obtain IPv6 Address. The system will allocate one /56 IPv6 CIDR.
4. If the IPv6 address is idle, you can click Release IPv6 Address in the Action column, and the system will release the IPv6 CIDR of the VPC.

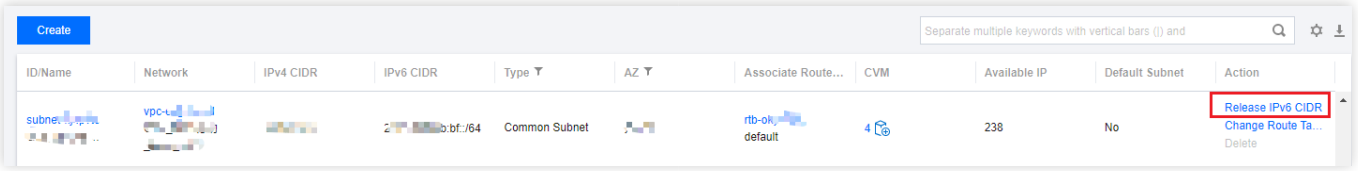


Allocating and Releasing IPv6 CIDR for a Subnet

1. Log in to the VPC Console.
2. Click Subnet in the left directory. On the top of the Subnet list, select Region and VPC. All subnet information under the region and VPC will be displayed.
3. Select a subnet, click Allocate IPv6 CIDR, and the system will assign one /64 IPv6 CIDR block to this subnet.



4. Select a subnet that has already been assigned an IPv6 CIDR, click Release IPv6 CIDR, and confirm the operation. The system will reclaim the IPv6 CIDR of the subnet.



Applying for and Releasing IPv6 Addresses for ENI

1. Log in to the VPC Console.

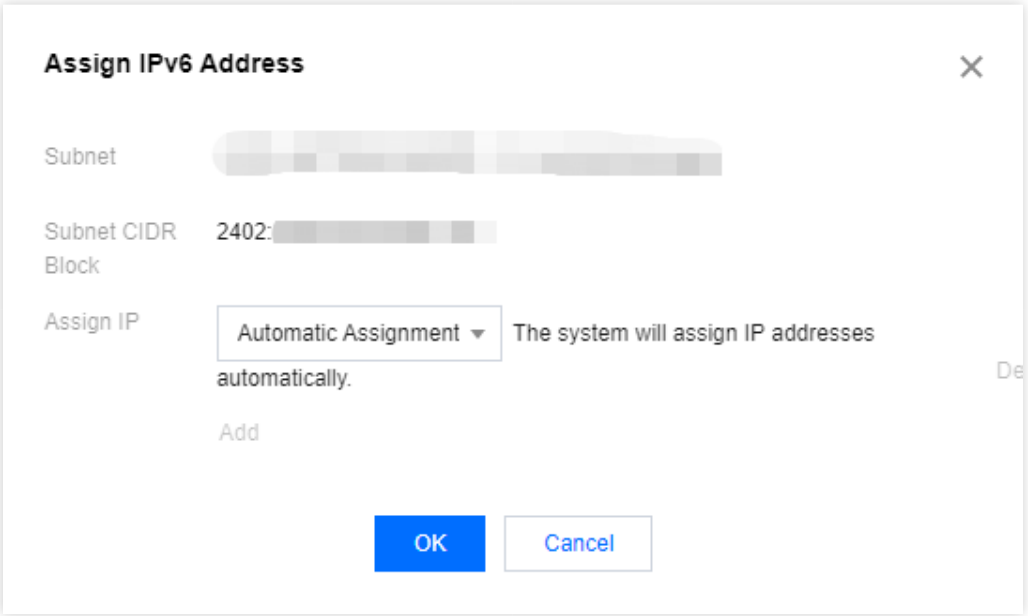
2. Click IP and Network Interface > Elastic Network Interface in the left-side directory to open the Elastic Network Interface list page.

3. Click the instance ID you want to view to open the details page.

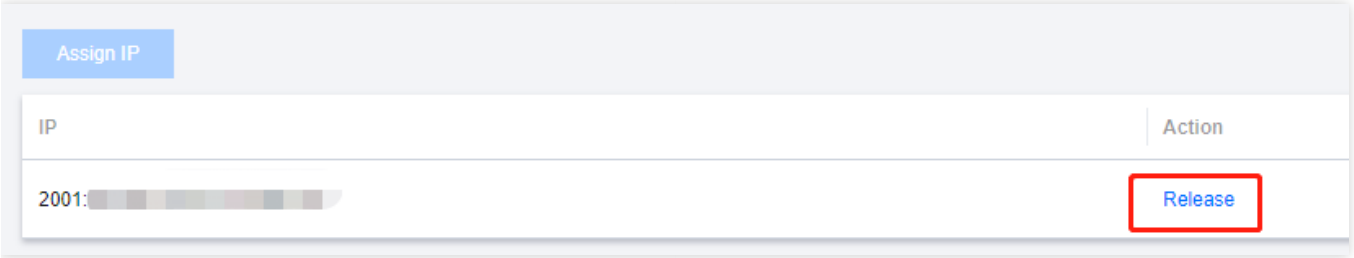
4. Select the IPv6 Address Management tab and click Allocate IP to request for an IPv6 address.



5. Click OK in the pop-up.



6. In the IPv6 Address Management tab, you can see that the system has allocated an IPv6 address to the ENI.



7. You can release the IPv6 address by clicking Release under the operation bar.

> Note:
>
> Before releasing it, please disable the public network of the IPv6 address.

Managing IPv6 Public Network

Enabling IPv6 Public Network

1. Log in to the VPC Console.

2. In the left directory, choose IP and Network Interface > Elastic IPv6.

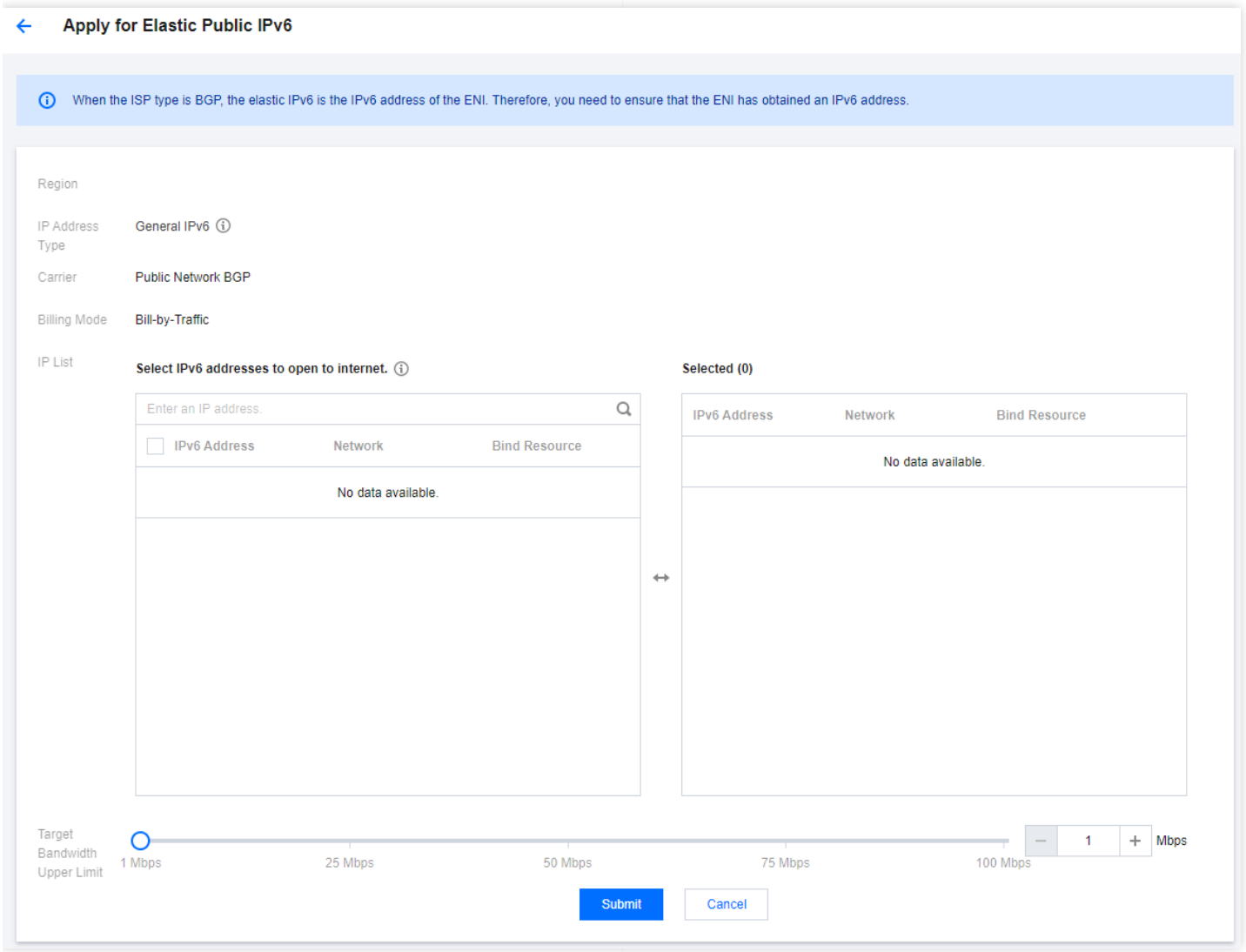
3. Select the region where you want to enable IPv6 public network, and click Apply to enter the Apply for Elastic IPv6 page.

4. Check the CVM IPv6 address, set the upper limit of the target bandwidth, and then click Submit.

> Note:
>
> - After the CVM applies for an IPv6 address, public network access capability is disabled by default. You can manage the IPv6 public network capability through Elastic IPv6.

- When the ISP type is BGP, the Elastic IPv6 address is the IPv6 address obtained by the CVM. Therefore, please ensure that the CVM has obtained an IPv6 address.

- A single operation can support enabling public network access for up to 100 IPv6 addresses simultaneously. If more than 100 IPv6 addresses need to enable public network access, please operate in multiple batches.



Disabling IPv6 public network

1. Log in to the VPC Console.
2. In the left directory, choose IP and Network Interface > Elastic IPv6.
3. On the Elastic IPv6 list page, check the IPv6 address for which you want to disable the public network, and click Release.
4. Verify the information in the pop-up window and click OK to release the Elastic Ipv6. After the Elastic IPv6 is released, the public network access is disabled for the corresponding IPv6 address.

Adjusting IPv6 Public Network Bandwidth

1. Log in to the VPC Console.

2. In the left directory, choose IP and Network Interface > Elastic IPv6.

3. In the operation column of a single elastic IPv6, click Adjust Bandwidth.

4. In the pop-up Adjust Bandwidth dialog box, modify the upper limit of the public network bandwidth of the Elastic IPv6 and click Adjust.

FAQs
General

What is Elastic IPv6?

After a CVM or ENI obtains an IPv6 address, the IPv6 public network is disabled by default. With Elastic IPv6, you can:

- Manage CVM or ENI in real time to provide IPv6 public network access.
- You can select a single IPv6 address to open the public network, or select multiple IPv6 addresses in batches to open the public network.
- After the public network is enabled, set the public network bandwidth, view monitoring, disable the public network, etc.

What is the difference between Elastic IPv6 and Elastic IP?

CVM can obtain IPv6 and IPv4 addresses at the same time and run IPv6 and IPv4 dual stack.

- The IPv4 public network is enabled by binding an EIP. The IPv4 EIP is an independent public network address and uses NAT to achieve public network access.
- The IPv6 public network is enabled through the Elastic IPv6. The Elastic IPv6 is implemented based on the IPv6 private network address on the ENI without using NAT.

What conditions are required to enable an IPv6 public network for a CVM?

The following conditions must be met to enable IPv6 public network for the CVM:

1. The VPC and subnet where the CVM is located obtains the IPv6 CIDR.
2. The ENI (including primary and secondary network interface) associated with the CVM obtains an IPv6 address.
3. Enable public network for the IPv6 of the ENI.

Does IPv6 public network communication support Anti-DDoS by default?

All CVMs for which the IPv6 public network has been enabled support IPv6 Anti-DDoS by default.

Troubleshooting IPv6 Connectivity

Overview

This document will provide you with basic troubleshooting ideas for IPv6 connectivity issues on CVM.

Directions

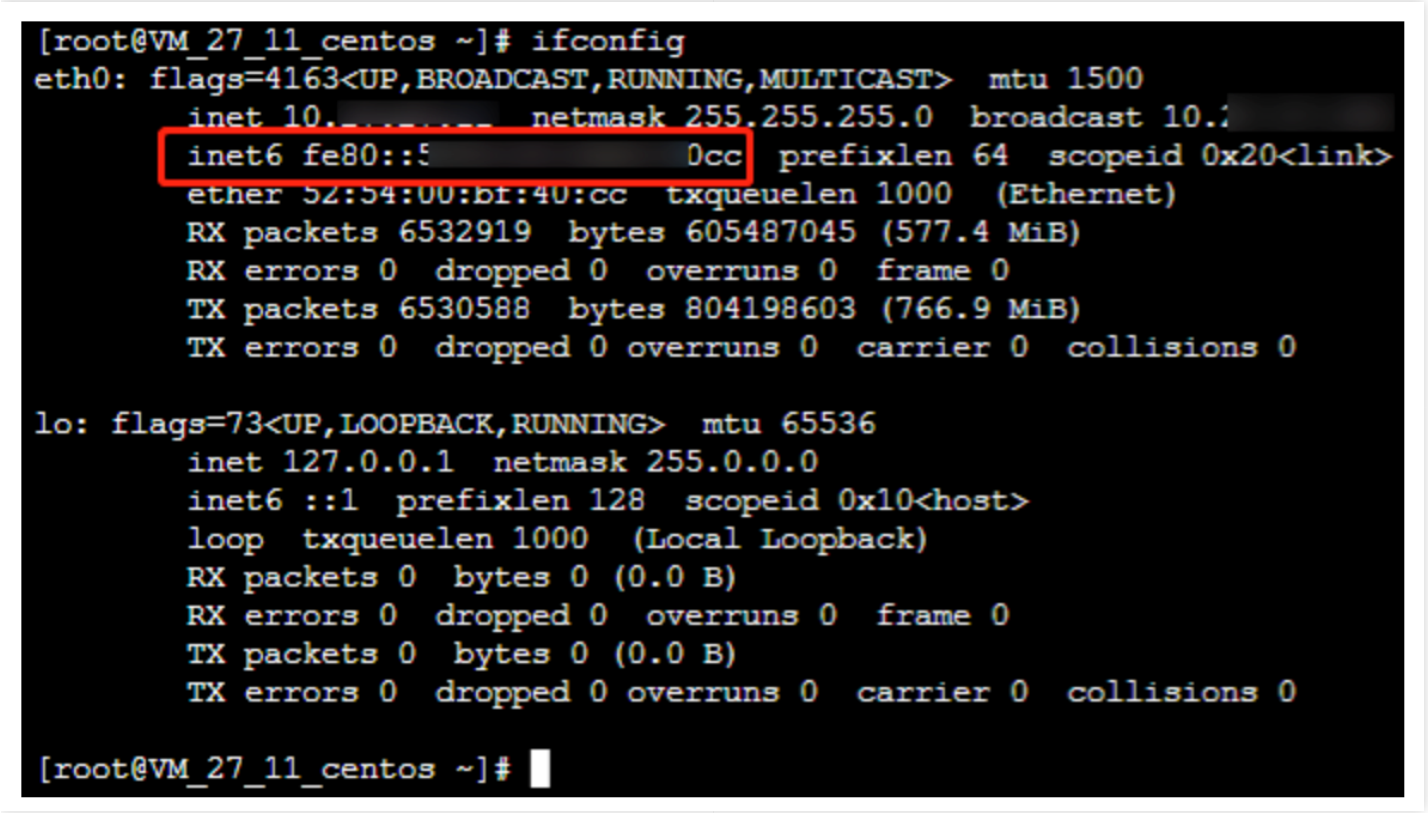
First, check whether the IPv6 configuration has been completed for CVM by following the four steps below:

1. Run the following command to check whether the network interface (usually eth0) of the CVM has obtained a link-local IPv6 address starting with fe80.

- If obtained, it indicates that the image has enabled the IPv6 feature. Please proceed to Step 2.
- If not obtained, please refer to "Solution Step 1".

> Note:
>
> The IPv6 address that begins with fe80 is not an IPv6 address used for communication.

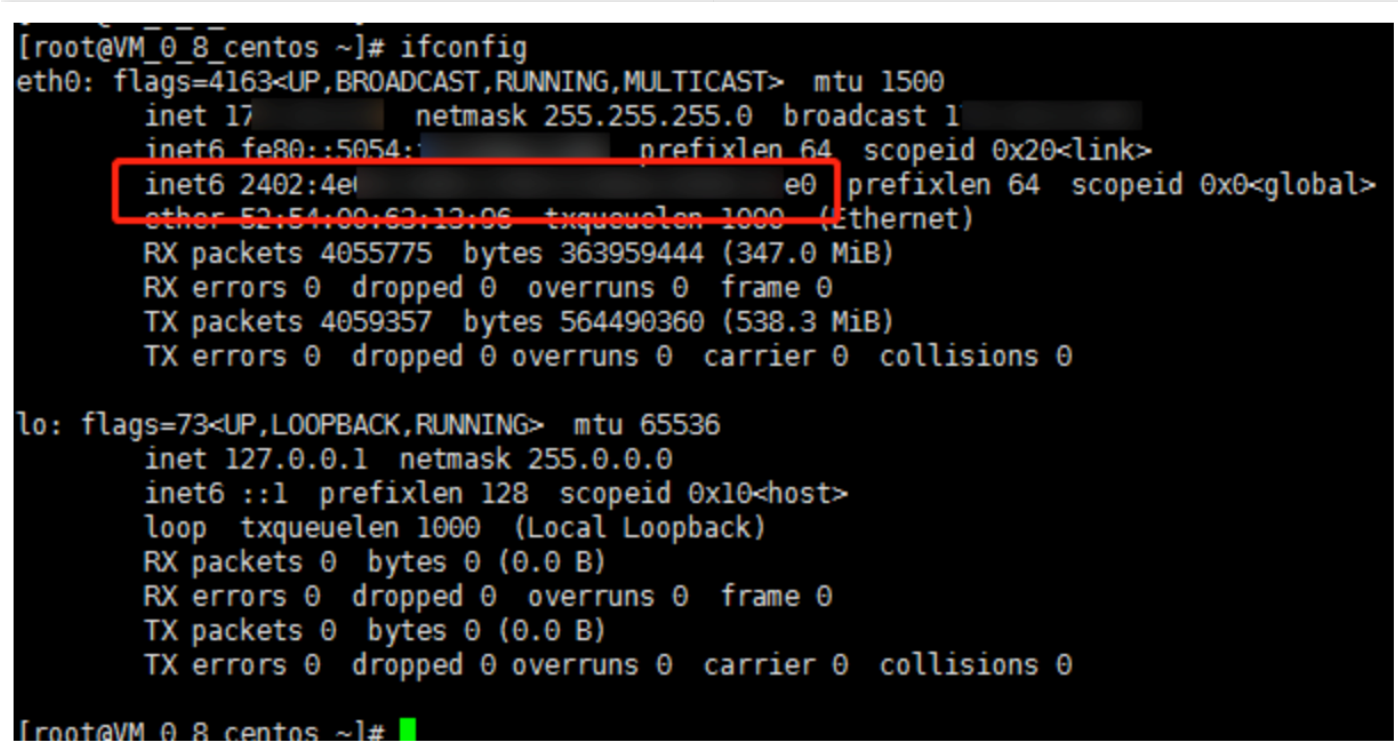
ifconfig



2. Run the following command to check whether the network interface of the CVM (usually eth0) has obtained an IPv6 address starting with "2402" (not an address starting with "fe80").

- If obtained, please proceed to Step 3.
- If not obtained, please refer to "Solution Step 2".

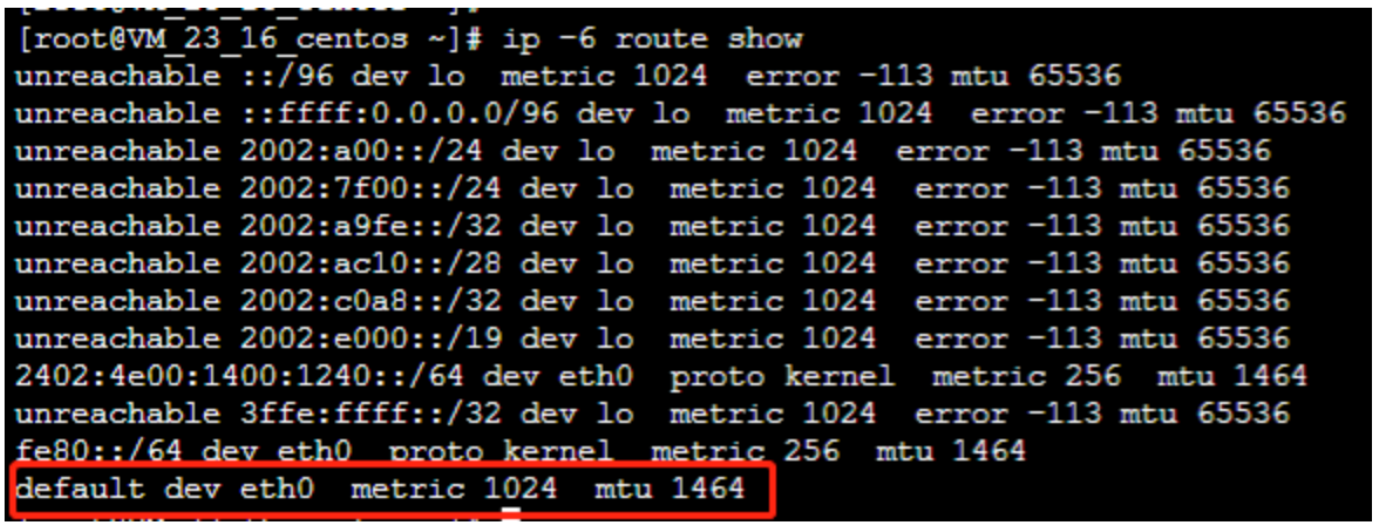
ifconfig



3. Run the following command to check the default route of the network interface.

- If the default route is configured and the public network is reachable via Ping, please proceed to Step 4.
- If the default route is not visible or the public network cannot be reached via Ping, please refer to "Solution Step 3".

ip -6 route show



Use ping6 240c::6666 Or ping -6 240c::6666 to test public network connectivity.

```
[root@VM_24_8_centos ~]# ping6 240c::6666
PING 240c::6666(240c::6666) 56 data bytes
64 bytes from 240c::6666: icmp_seq=1 ttl=53 time=45.8 ms
64 bytes from 240c::6666: icmp_seq=2 ttl=53 time=45.3 ms
64 bytes from 240c::6666: icmp_seq=3 ttl=53 time=45.4 ms
64 bytes from 240c::6666: icmp_seq=4 ttl=53 time=45.4 ms
64 bytes from 240c::6666: icmp_seq=5 ttl=53 time=45.4 ms
64 bytes from 240c::6666: icmp_seq=6 ttl=53 time=45.3 ms
```

4. Run the following command to confirm whether the IPv6 is being listened to on port 22 and port 80. If port 22 and port 80 are not listening to IPv6, please refer to Solution Step 4.

netstat - tupln

```
[root@VM_23_4_centos ~]# netstat -tupln
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      3204/nginx: master
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      1159/sshd
tcp6       0      0 :::80                   :::*                    LISTEN      3204/nginx: master
tcp6       0      0 :::22                   :::*                    LISTEN      1159/sshd
udp        0      0 0.0.0.0:68              0.0.0.0:*                           914/dhclient
udp        0      0 10.24.23.4:123          0.0.0.0:*                           636/ntpd
udp        0      0 127.0.0.1:123           0.0.0.0:*                           636/ntpd
udp6       0      0 fe80::5054:ff:fefa::546 :::*                                3066/dhclient
udp6       0      0 2402:4e00:1400:1240:123 :::*                                636/ntpd
udp6       0      0 fe80::5054:ff:fefa::123 :::*                                636/ntpd
udp6       0      0 ::1:123                 :::*                                636/ntpd
[root@VM_23_4_centos ~]#
```

Solutions

1. If you cannot see an IPv6 address starting with fe80 using ifconfig , it indicates that the IPv6 feature is not enabled for the CVM. See Quick Start - Configuring IPv6 for CVM, select the image you need to enable IPv6 and reconfigure it. You can confirm by executing sysctl -a | grep ipv6 | grep disable .

2. If you do not see an IPv6 address starting with "2402" via ifconfig , there are two possibilities:
   - The ENI of the CVM in the console is not allocated with an IPv6 address. You can solve this problem by logging in to the console to allocate an IPv6 address for the ENI. For details, see Applying for and Releasing IPv6 Address for Elastic Network Interface.
   - The dhcpv6 related configuration in the CVM is not configured properly or dhclient -6 is not

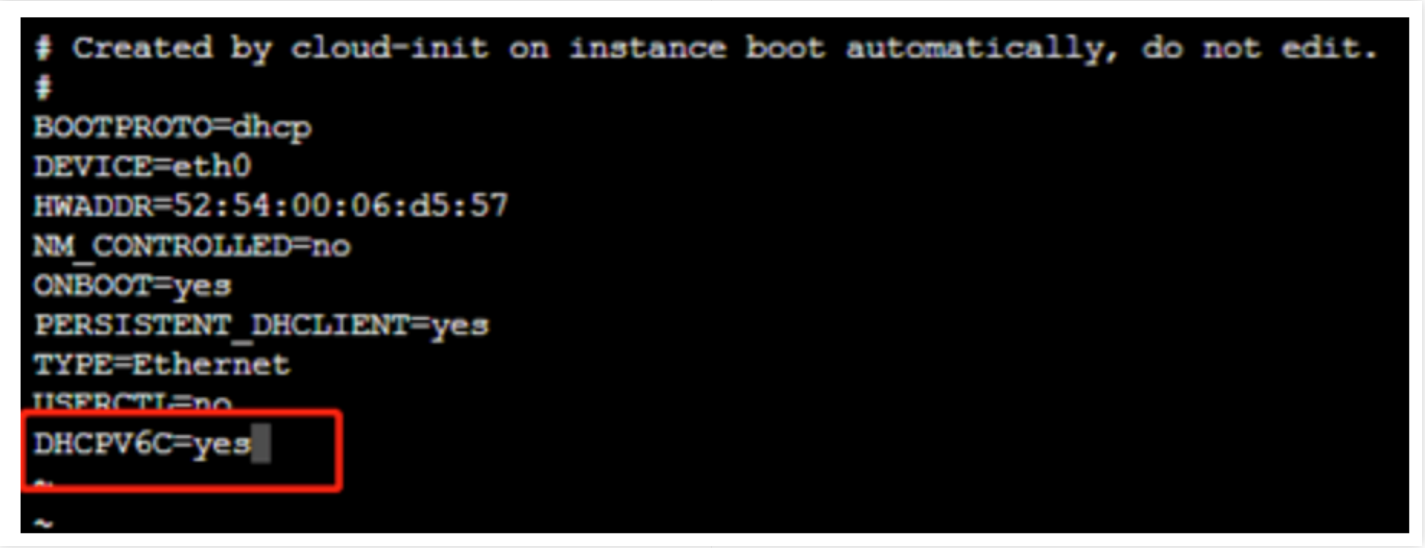
executed . Log in to the CVM:

3. Execute the following command to open the ifcfg-eth0 file in the folder /etc/sysconfig/network-scripts/ .

   vim /etc/sysconfig/network-scripts/ifcfg-eth0

4. Press i to switch to edit mode and add the following content.

   dhcpv6c=yes



5. Press Esc, enter :wq, save and return the file, and restart the CVM.
6. Execute the following commands in sequence to check whether an IPv6 address starting with 2402 has been obtained.

   # If the CVM has multiple network interfaces, execute dhclient -6 network interface name, such as dhclient -6 eth0
   dhclient -6 or dhclient -6 network interface name
   ifconfig

7. If an IPv6 address is obtained but the public network is not reachable via Ping, there are two possibilities:
   - The public network is not enabled for the IPv6 address. You can solve this problem by logging in to the console to enable the public network for the IPv6 address. For details, see Managing IPv6 Public Network.

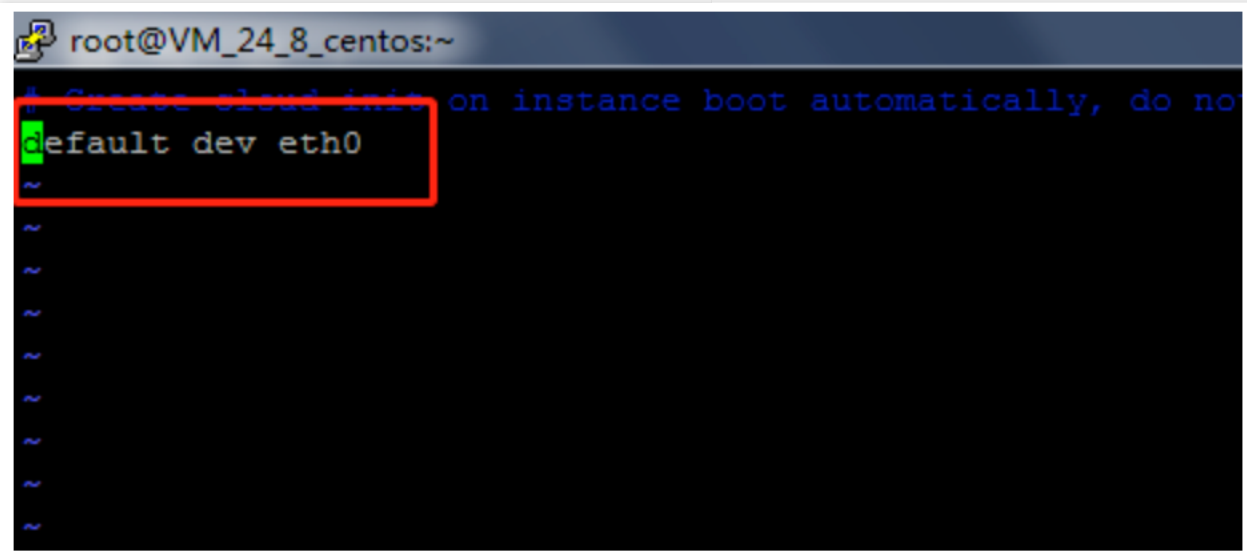
- No default route is configured. Use ip -6 route show to check whether the default route has been configured. If you don't see a default route, you need to:

8. Execute the following command to open route6-eth0 file in the folder /etc/sysconfig/network-scripts/ .

   vim /etc/sysconfig/network-scripts/route6-eth0

9. Press i to switch to edit mode and add the following content.

   default dev eth0

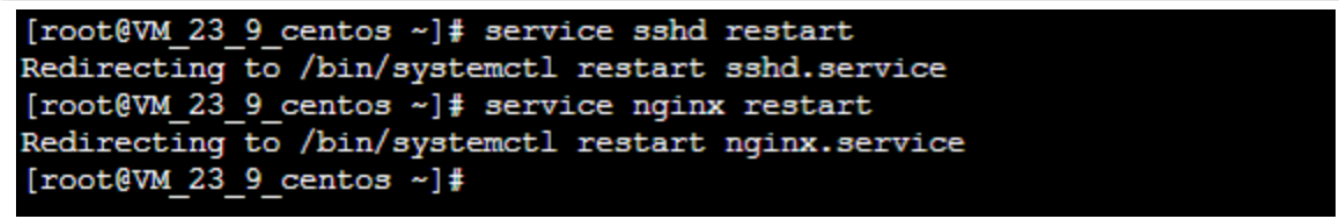


10. Press Esc, enter :wq, save and return the file. Run the following command to restart the network service or restart the CVM.

    service network restart
    or
    systemctl restart network

11. If the IPv6 public network is reachable via Ping, but ports 22 or 80 cannot be accessed, it is usually due to configuration issues with sshd and Nginx files. The sshd and Nginx configurations need to be modified to make ports 22 or 80 listen to IPv6. After configuration is completed:
12. Execute the following commands in sequence to restart the sshd and Nginx services.

service sshd restart
service nginx restart



13. By running netstat -tupln to check whether ports 22 or 80 are listening to IPv6, you can refer to the above "Operation Steps - Step 4".

Glossary

Virtual Private Cloud

A VPC is a logically isolated network space that you custom on a cloud platform, similar to the traditional network you run in a data center. IPv4 and IPv6 dual stack can be enabled for the VPC at the same time.

Subnet

A VPC consists of at least one subnet, and the subnet's CIDR block must be within the VPC's CIDR. All cloud resources in a VPC, such as cloud virtual machines and databases, must be deployed within a subnet. Subnets can also support both IPv4 and IPv6, enabling dual stack.

Elastic Network Interface

An Elastic Network Interface (ENI) is an elastic network interface bound to a CVM in a VPC and can be freely migrated between multiple CVMs. An ENI can obtain both IPv4 and IPv6 addresses at the same time.

Cloud Virtual Machine

CVM provides you with secure and reliable elastic computing services and supports dual-stack networking with both IPv4 and IPv6, with its IPv6 address assigned through the associated ENI.

Global Unicast Address

The Global Unicast Address (GUA) is equivalent to the public network address in IPv4 and can be globally routed and accessed on the IPv6 Internet. This address type allows aggregation of routing prefixes, thereby limiting the number of global routing table entries.