

# 弹性公网 IPv6

## 快速入门

### 产品文档



腾讯云

---

**【版权声明】**

©2013-2019 腾讯云版权所有

本文档著作权归腾讯云单独所有，未经腾讯云事先书面许可，任何主体不得以任何形式复制、修改、抄袭、传播全部或部分本文档内容。

**【商标声明】**

及其它腾讯云服务相关的商标均为腾讯云计算（北京）有限责任公司及其关联公司所有。本文档涉及的第三方主体的商标，依法由权利人所有。

**【服务声明】**

本文档意在向客户介绍腾讯云全部或部分产品、服务的当时的整体概况，部分产品、服务的内容可能有所调整。您所购买的腾讯云产品、服务的种类、服务标准等应由您与腾讯云之间的商业合同约定，除非双方另有约定，否则，腾讯云对本文档内容不做任何明示或模式的承诺或保证。

## 文档目录

### 快速入门

#### 操作概述

#### 步骤1：VPC 配置 IPv6

#### 步骤2：云服务器配置 IPv6

# 快速入门

## 操作概述

最近更新时间：2019-12-06 18:15:41

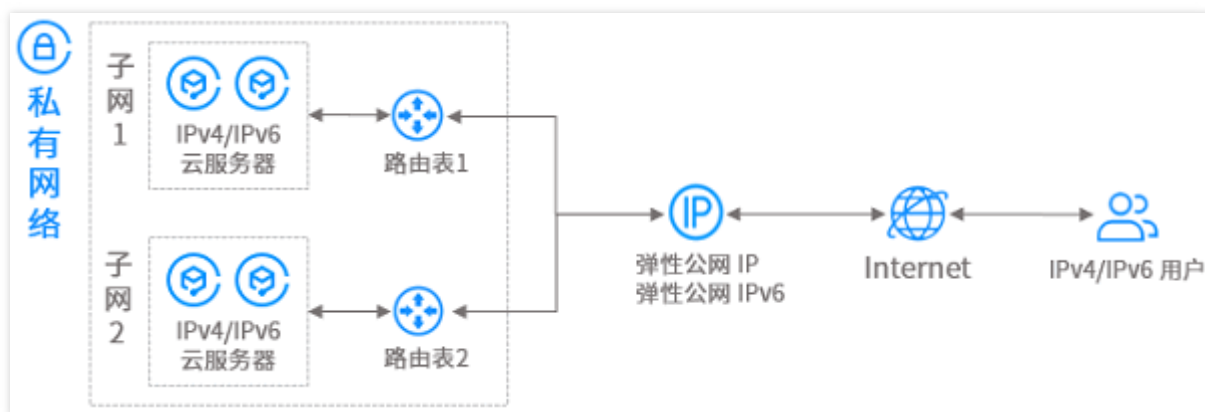
说明：

目前弹性公网 IPv6 处于内测中，如有需要，请提交 [内测申请](#)。

本教程将帮助您搭建一个具有 IPv6 CIDR 的私有网络（VPC），并为 VPC 内的云服务器或者弹性网卡开启 IPv6，实现 IPv6 的内外网通信。

## 操作场景

1. 云服务器启用 IPv6，和 VPC 内其他云服务器的 IPv6 内网互通。
2. 云服务器启用 IPv6，和 Internet 的 IPv6 用户进行双向通信。



## 操作须知

1. 在开始使用腾讯云产品前，您需要先 [注册腾讯云账号](#)。
2. 目前支持 IPv6 的地域为北京、上海、广州、上海金融云、深圳金融云，请在这些地域部署 IPv6 服务。
3. IPv6 地址为 GUA 地址，每个 VPC 分配1个 /56 的 IPv6 CIDR，每个子网分配1个 /64 的 IPv6 CIDR，每个弹性网卡分配1个 IPv6 地址。
4. 主网卡、辅助网卡均支持申请 IPv6 地址。想要了解更多云服务器和弹性网卡的关系，请参见 [弹性网卡](#) 产品文档。

## 操作步骤

[步骤1：VPC 配置 IPv6](#)

[步骤2：云服务器配置 IPv6](#)

# 步骤1：VPC 配置 IPv6

最近更新时间：2020-02-05 16:52:37

本教程将帮助您搭建一个具有 IPv6 CIDR 的私有网络（VPC）。

## 操作须知

1. 在开始使用腾讯云产品前，您需要先 [注册腾讯云账号](#)。
2. 目前弹性公网 IPv6 处于内测中，如有需要，请提交 [内测申请](#)。
3. 目前支持 IPv6 的地域为北京、上海、广州、上海金融云、深圳金融云，请在这些地域部署 IPv6 服务。
4. IPv6 地址为 GUA 地址，每个 VPC 分配1个 /56 的 IPv6 CIDR，每个子网分配1个 /64 的 IPv6 CIDR，每个弹性网卡分配1个 IPv6 地址。
5. 主网卡、辅助网卡均支持申请 IPv6 地址。想要了解更多云服务器和弹性网卡的关系，请参见 [弹性网卡](#) 产品文档。

## 操作步骤

说明：

如下步骤1 - 步骤5中的目标云服务器均指需配置 IPv6 的云服务器。

### 步骤1：VPC 分配 IPv6 CIDR

1. 登录 [私有网络控制台](#)。
2. 在目标云服务器所属 VPC 所在行的操作栏下，单击【编辑 CIDR】。
3. 在弹框中的 IPv6 CIDR 单击【获取】并确认操作，系统将为 VPC 分配一个 /56 的 IPv6 地址段，您可以在列表里看到 IPv6 地址段的详细信息。

### 编辑CIDR

私有网络

IPv4 CIDR

1

IPv6 CIDR

获取

确认

取消

## 步骤2：为子网分配 IPv6 CIDR

1. 登录 [私有网络控制台](#)。
2. 在左侧目录下选择【子网】，进入管理页面。
3. 在目标云服务器所属子网所在行的操作栏下，单击【获取 IPv6 CIDR】并确认操作，系统将从 VPC 的 /56 IPv6 CIDR 分配一个 /64 的 IPv6 CIDR。

| ID名称 ↓ | 所属网络 | IPv4 CIDR | IPv6 CIDR | 可用区 ① | 关联路由表 | 子网广播 | 云服务器 | 可用IP | 默认子网 | 操作                                                                      |
|--------|------|-----------|-----------|-------|-------|------|------|------|------|-------------------------------------------------------------------------|
|        |      | 1         | -         | 广州四区  |       |      | 2    | 4087 | 是    | <a href="#">获取IPv6 CIDR</a><br><a href="#">删除</a> <a href="#">更换路由表</a> |
|        |      |           |           | 广州三区  |       |      | 5    | 4086 | 是    | <a href="#">释放IPv6</a> <a href="#">删除</a><br><a href="#">更换路由表</a>      |

## 步骤3：弹性网卡获取 IPv6 地址

1. 登录 [私有网络控制台](#)。
2. 在左侧目录下选择【IP 与网卡】>【弹性网卡】，在列表页中单击目标云服务器所绑定的弹性网卡 ID，进入详情页。
3. 选择【IPv6 地址管理】标签页，单击【分配 IP】。

← j

基本信息

IPv4 地址管理

IPv6 地址管理

关联安全组

分配IP

4. 在弹窗中单击【确定】即可。

分配IPv6地址

所属子网

js

子网CIDR

2

分配IP

自动分配

系统将自动分配IP地址

删除

新增

确定

取消

5. 系统将会为弹性网卡分配一个 IPv6 地址，如下图所示。

← j

基本信息 IPv4 地址管理 IPv6 地址管理 关联安全组

分配IP

| IP | 备注 | 操作 |
|----|----|----|
| 2  | -  | 释放 |

#### 步骤4：为弹性网卡的 IPv6 地址开通公网（可选）

1. 登录 [私有网络控制台](#)。
2. 在左侧目录下选择【IP 与网卡】>【弹性公网 IPv6】。
3. 选择需要开通 IPv6 公网的地域，如“华南地区（广州）”，单击【申请】，进入管理页面。
4. 勾选已绑定目标云服务器的 IPv6 地址、设置目标带宽上限，单击【提交】即可。

说明：

- 弹性网卡申请了 IPv6 地址后，默认关闭了公网访问能力，可通过弹性公网 IPv6 [管理 IPv6 公网](#) 能力。
- 当运营商类型为 BGP 时，弹性公网 IPv6 地址即为弹性网卡获取到的 IPv6 地址，所以请确保弹性网卡已经获取到 IPv6 地址。
- 单次操作可支持最多100个 IPv6 地址同时开通公网，如果超过100个 IPv6 地址需要开通公网，请分多次操作。



← 申请弹性公网IPv6

弹性公网IPv6 帮助文档

运营高类型为BGP时，弹性公网IPv6地址即为网卡的IPv6地址。所以使用弹性公网IPv6前，请确保弹性网卡已经获取到IPv6地址。

地域

广州

IP地址类型

普通IPv6

运营商

BGP

计费模式

共享带宽包

IP列表

请选择需要开通公网的IPv6地址

请输入IP/弹性网卡ID

IPv6地址

所属网络

绑定资源

24

v

int

24

vj

int

已选择 (1)

IPv6地址

所属网络

绑定资源

24

v

int

目标带宽上限

0 Mbps

250 Mbps

500 Mbps

750 Mbps

1000 Mbps

−

0

+

Mbps

步骤5：配置 IPv6 的安全组规则

说明：

出入方向的安全组规则支持配置来源为单个 IPv6 地址或者 IPv6 CIDR，其中 `::/0` 代表所有的 IPv6 源地址。

- 1. 登录 [私有网络控制台](#)。
- 2. 在左侧目录下选择【安全】>【安全组】，在列表页中单击目标云服务器绑定的安全组 ID，进入详情页。

版权所有：腾讯云计算（北京）有限责任公司

第9 共34页

3. 选择【进站规则】并单击【添加规则】，添加 IPv6 的入方向安全组规则，单击【完成】即可。

添加进站规则

类型

来源 ①

协议端口 ①

策略

备注

自定义

::/0

all

允许

删除

+ 新增一行

完成

取消

4. 选择【出站规则】并单击【添加规则】，添加 IPv6 的出方向安全组规则，单击【完成】即可。

添加出站规则

类型

目标 ①

协议端口 ①

策略

备注

自定义

::/0

all

允许

删除

+ 新增一行

完成

取消

## 步骤2：云服务器配置 IPv6

最近更新时间：2020-01-08 09:35:58

本教程为您介绍如何为 VPC 内的云服务器配置 IPv6，实现 IPv6 的内外网通信。

### Linux 云服务器配置 IPv6

Linux 云服务器配置 IPv6 有两种方式：[工具配置](#) 和 [手动配置](#)。

- 工具配置通过工具一键配置 IPv6。
- 手动配置需要您对 Linux 命令有一定的熟练掌握程度。

请根据您的实际情况选择对应的方式，推荐您使用更高效的自动配置工具配置 IPv6 地址。

| 镜像类型                                                                                                            | 购买时间                | 是否已开启 IPv6 | 配置方式                                                                                              |
|-----------------------------------------------------------------------------------------------------------------|---------------------|------------|---------------------------------------------------------------------------------------------------|
| CentOS 7.5/CentOS 7.6                                                                                           | 2019-06-31前购买       | 否          | <ul style="list-style-type: none"><li><a href="#">工具配置</a></li><li><a href="#">手动配置</a></li></ul> |
|                                                                                                                 | 2019-06-31后购买       | 是          |                                                                                                   |
| CentOS 6/CentOS 7 ( 不含 7.5/7.6 )<br>Ubuntu14.04/Ubuntu 12.04<br>Debian 8/Debian 9<br>CoreOS 17<br>Tencent Linux | 2019-11-13 01:00前购买 | 否          |                                                                                                   |
|                                                                                                                 | 2019-11-13 01:00后购买 | 是          |                                                                                                   |

#### 工具配置

说明：

不支持工具配置的操作系统：FreeBSD、Suse、Ubuntu18。

请根据云服务器是否已开启 IPv6 选择对应的配置方式：

- [未开启 IPv6 的云服务器](#)
- [已开启 IPv6 的云服务器](#)

#### 未开启 IPv6 的云服务器

enable\_ipv6 工具可以为已分配 IPv6 地址的 CVM 实例一键配置 IPv6 地址。

## 使用限制

- enable\_ipv6 工具仅适用于 VPC 网络环境下。
- enable\_ipv6 工具运行时会自动重启网卡、网络服务，短时间内网络可能会不可用，请慎重执行。

## 操作步骤

1. 登录云服务器，在云服务器中直接执行如下命令下载 enable\_ipv6 工具：

```
wget https://iso-1251783334.cos.ap-guangzhou.myqcloud.com/scripts/enable_ipv6.sh
```

2. 赋予执行权限后使用管理员权限执行：

```
chmod +x ./enable_ipv6.sh
./enable_ipv6.sh [网卡名称]
# 示例 1 : ./enable_ipv6.sh eth0
# 示例 2 : ./enable_ipv6.sh eth1
```

3. （此步骤仅适用于 CoreOS 操作系统）重启云服务器，使上述配置生效。

## 已开启 IPv6 的云服务器

config\_ipv6 工具可以为已开启 IPv6 且已分配 IPv6 地址的 CVM 实例一键配置 IPv6 地址。

## 使用限制

- config\_ipv6 工具仅适用于 VPC 网络环境下。
- config\_ipv6 工具运行时会自动重启网卡、网络服务，短时间内网络可能会不可用，请慎重执行。

## 操作步骤

1. 登录云服务器，在云服务器中直接执行如下命令下载 config\_ipv6 工具：

```
wget https://iso-1251783334.cos.ap-guangzhou.myqcloud.com/scripts/config_ipv6.sh
```

2. 赋予执行权限后使用管理员权限执行：

```
chmod +x ./config_ipv6.sh
./config_ipv6.sh [网卡名称]
# 示例 1 : ./config_ipv6.sh eth0
# 示例 2 : ./config_ipv6.sh eth1
```

3. （此步骤仅适用于 CoreOS 操作系统）重启云服务器，使上述配置生效。

对于需要自动化配置 IPv6 实例的需求，例如，大批量配置，建议您使用实例自定义数据配合脚本的方式来调用。详情请参见 [实例自定义数据](#)。如下为脚本示例（假设是 RHEL 系列，Bash Shell 脚本）。

说明：

该示例仅对 eth0 进行配置，实际操作时注意修改为实际使用的网卡名。

```
#!/bin/sh
install_dir=/usr/sbin
install_path="$install_dir"/config-ipv6
if [ ! -f "$install_path" ]; then
tool_url="https://iso-1251783334.cos.ap-guangzhou.myqcloud.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
```

## 手动配置

如下列举了四种典型的 Linux 云服务器的操作方法：

- [新购 CentOS 7.5/新购 CentOS 7.6 配置 IPv6](#)
- [CentOS 6.8 配置 IPv6](#)
- [CentOS 7.3/存量 CentOS 7.5/存量 CentOS 7.6 配置 IPv6](#)
- [Debian 8.2 配置 IPv6](#)

说明：

- 新购 CentOS 7.5/新购 CentOS 7.6 指2019年06月31日**后**购买的云服务器。
- 存量 CentOS 7.5/存量 CentOS 7.6 指2019年06月31日**前**购买的云服务器。

### 新购 CentOS7.5 /新购 CentOS7.6 配置 IPv6

1. 进入 [云服务器控制台](#) 并登录实例。



2. 执行如下命令，打开 `/etc/sysconfig/network-scripts/` 文件夹下的 `ifcfg-eth0` 文件。

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

3. 按 “i” 切换至编辑模式，增加如下内容。

```
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. 按 “Esc”，输入 “:wq”，保存文件并返回。
5. 依次执行如下命令，查看是否已经获取到 IPv6 地址。

```
dhclient -6
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 fe80::a8e prefixlen 64 scopeid 0x20<link>
    ether 52:54:00:0e:db: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. 执行如下命令，打开 `/etc/ssh/` 文件夹下的 `sshd_config` 文件。

```
vim /etc/ssh/sshd_config
```

7. 按 “i” 切换至编辑模式，删除对 `AddressFamily any` 的注释（即删除前面的 `#`），为 `ssh` 等应用程序开启 IPv6 监听。

```
$OpenBSD: sshd_config,v 1.100 2016/08/15 12:32:04 naddy Exp $

# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/local/bin:/usr/bin

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options override the
# default value.

# If you want to change the port on a SELinux system, you have to tell
# SELinux about this change.
# semanage port -a -t ssh_port_t -p tcp #PORTNUMBER

#Port 22
AddressFamily any
AddressFamily inet
ListenAddress 10.10.10.10
ListenAddress 10.10.10.10
HostKey /etc/ssh/ssh_host_rsa_key
HostKey /etc/ssh/ssh_host_dsa_key
HostKey /etc/ssh/ssh_host_ecdsa_key
HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
SyslogFacility AUTHPRIV
LogLevel INFO

# Authentication:

#LoginGraceTime 2m
#PermitRootLogin yes
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

#PubkeyAuthentication yes

# The default is to check both .ssh/authorized_keys and .ssh/authorized_keys2
-- INSERT --
```

8. 按“Esc”，输入“:wq”，保存文件并返回。

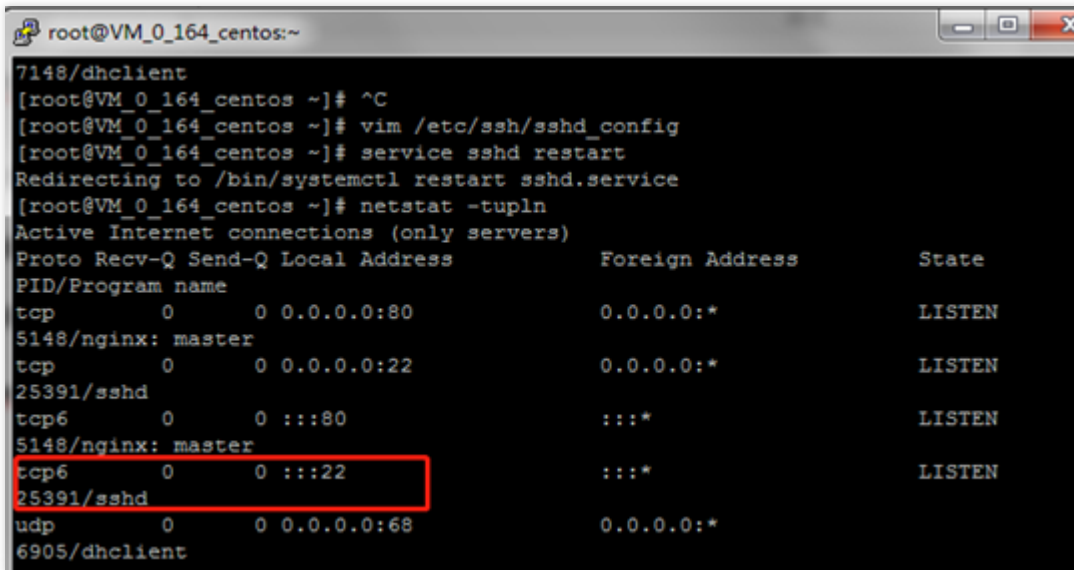
9. 执行如下命令，重启 ssh 进程。

```
service sshd restart
```

10. 执行如下命令，查看 ssh 是否已经监听 IPv6。

```
netstat -tupln
```





```
root@VM_0_164_centos:~  
7148/dhclient  
[root@VM_0_164_centos ~]# ^C  
[root@VM_0_164_centos ~]# vim /etc/ssh/sshd_config  
[root@VM_0_164_centos ~]# service sshd restart  
Redirecting to /bin/systemctl restart sshd.service  
[root@VM_0_164_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  
5148/nginx: master  
tcp        0      0 0.0.0.0:22             0.0.0.0:*               LISTEN  
25391/sshd  
tcp6       0      0 :::80                  :::*                     LISTEN  
5148/nginx: master  
tcp6       0      0 :::22                  :::*                     LISTEN  
25391/sshd  
udp        0      0 0.0.0.0:68             0.0.0.0:*  
6905/dhclient
```

1. 测试连通性，请参见 [测试 Linux 云服务器 IPv6 的连通性](#)。

## CentOS 6.8 配置 IPv6

1. 远程连接实例。具体操作，请参见 [连接 Linux 实例](#)。
2. 检查实例是否已开启 IPv6 服务，执行如下命令：

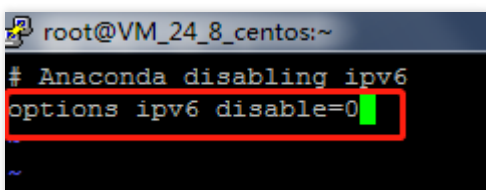
```
ip addr | grep inet6  
或者  
ifconfig | grep inet6
```

- 若实例未开启 IPv6 服务，请根据下文继续开启 IPv6 服务。
  - 若返回 inet6 相关内容，表示实例已成功开启 IPv6 服务，您可以跳至 [第9步](#) 继续操作。
3. 执行如下命令，打开 /etc/modprobe.d/ 文件夹下的 ipv6.conf 文件。

```
vi /etc/modprobe.d/ipv6.conf
```

4. 按 “i” 切换至编辑模式，将如下的内核参数设置为0。

```
options ipv6 disable=0
```



```
root@VM_24_8_centos:~  
# Anaconda disabling ipv6  
options ipv6 disable=0
```

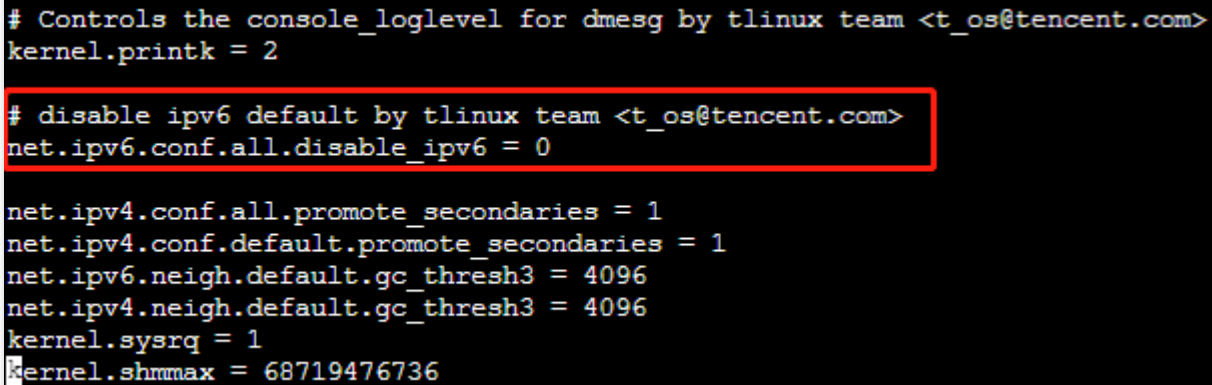
5. 按 “Esc”，输入 “:wq”，保存文件并返回。

6. 执行如下命令，打开 `etc` 文件夹下的 `sysctl.conf.first` 文件。

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

7. 按 “i” 切换至编辑模式，将如下的配置文件参数设置为0。

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



```
# Controls the console_loglevel for dmesg by tlinux team <t_os@tencent.com>
kernel.printk = 2

# disable ipv6 default by tlinux team <t_os@tencent.com>
net.ipv6.conf.all.disable_ipv6 = 0

net.ipv4.conf.all.promote_secondaries = 1
net.ipv4.conf.default.promote_secondaries = 1
net.ipv6.neigh.default.gc_thresh3 = 4096
net.ipv4.neigh.default.gc_thresh3 = 4096
kernel.sysrq = 1
kernel.shmmax = 68719476736
```

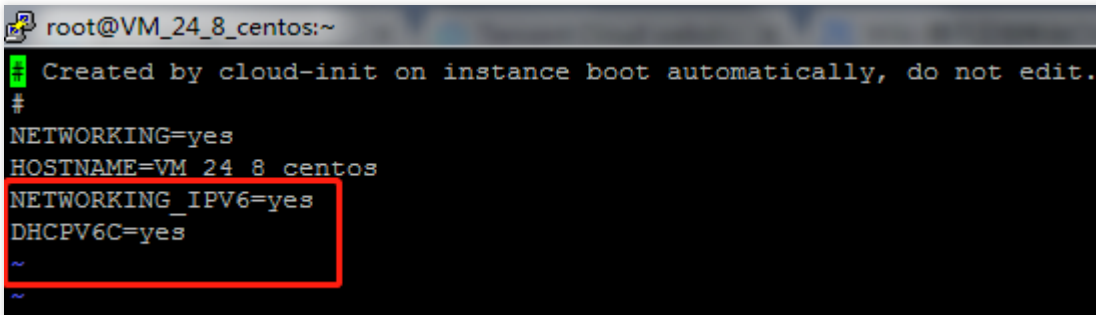
8. 按 “Esc”，输入 “:wq”，保存文件并返回。

9. 执行如下命令，打开 `/etc/sysconfig/` 文件夹下的 `network` 文件。

```
vi /etc/sysconfig/network
```

0. 按 “i” 切换至编辑模式，增加如下内容。

```
NETWORKING_IPV6=yes
DHCPV6C=yes
```



```
root@VM_24_8_centos:~
Created by cloud-init on instance boot automatically, do not edit.
#
NETWORKING=yes
HOSTNAME=VM_24_8_centos
NETWORKING_IPV6=yes
DHCPV6C=yes
~
~
```

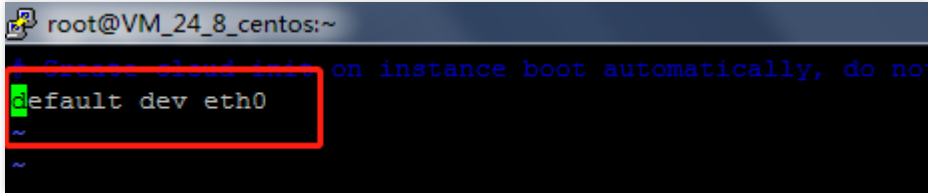
1. 按 “Esc”，输入 “:wq”，保存文件并返回。

2. 执行如下命令，打开或创建 `/etc/sysconfig/network-scripts/` 文件夹下的 `route6-eth0` 文件。

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

3. 按 “i” 切换至编辑模式，增加如下内容，为网卡的 IPv6 添加默认出口。

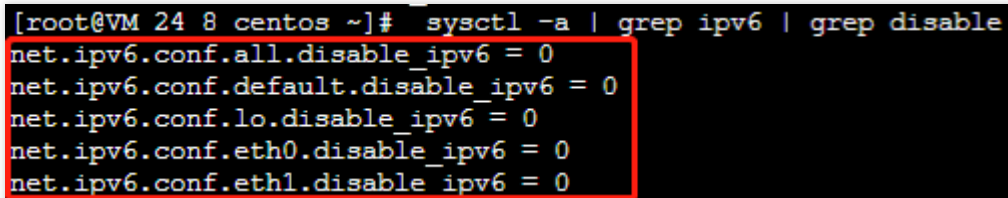
```
default dev eth0
```



```
root@VM_24_8_centos:~  
+ Create cloud-init on instance boot automatically, do not  
default dev eth0
```

4. 按“Esc”，输入“:wq”，保存文件并返回。
5. 重启云服务器，仅通过 `service network restart`，IPv6 无法正常加载。
6. 执行如下命令查看重启后 IPv6 是否已经正常加载。

```
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
```

7. 依次执行如下命令，查看是否已经获取到 IPv6 地址。

```
dhclient -6  
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::5c...:f2c0/64 Scope:Link
          inet6 addr: 2402::...: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::...:575e/64 Scope:Global
          inet6 addr: fe80::...: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)
```

8. 执行如下命令，打开 `/etc/ssh/` 文件夹下的 `sshd_config` 文件。

```
vim /etc/ssh/sshd_config
```

9. 按 “i” 切换至编辑模式，删除对 `AddressFamily any` 的注释（即删除前面的 `#`），为 `ssh` 等应用程序开启 IPv6 监听。

```
$OpenBSD: sshd_config,v 1.100 2016/08/15 12:32:04 naddy Exp $

# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/local/bin:/usr/bin

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options override the
# default value.

# If you want to change the port on a SELinux system, you have to tell
# SELinux about this change.
# semanage port -a -t ssh_port_t -p tcp #PORTNUMBER

#Port 22
AddressFamily any
AddressFamily inet
ListenAddress 10.10.10.10
ListenAddress ::

HostKey /etc/ssh/ssh_host_rsa_key
HostKey /etc/ssh/ssh_host_dsa_key
HostKey /etc/ssh/ssh_host_ecdsa_key
HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
SyslogFacility AUTHPRIV
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
#PermitRootLogin yes
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

#PubkeyAuthentication yes

# The default is to check both .ssh/authorized_keys and .ssh/authorized_keys2
-- INSERT --
```

!0. 按“Esc”，输入“:wq”，保存文件并返回。

!1. 执行如下命令，重启 ssh 进程。

```
service sshd restart
```

!2. 执行如下命令，查看 ssh 是否已经监听 IPv6。

```
netstat -tupln
```

```
root@VM_0_164_centos:~  
7148/dhclient  
[root@VM_0_164_centos ~]# ^C  
[root@VM_0_164_centos ~]# vim /etc/ssh/sshd_config  
[root@VM_0_164_centos ~]# service sshd restart  
Redirecting to /bin/systemctl restart sshd.service  
[root@VM_0_164_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  
5148/nginx: master  
tcp        0      0 0.0.0.0:22             0.0.0.0:*               LISTEN  
25391/sshd  
tcp6       0      0 :::80                  :::*                     LISTEN  
5148/nginx: master  
tcp6       0      0 :::22                  :::*                     LISTEN  
25391/sshd  
udp        0      0 0.0.0.0:68             0.0.0.0:*  
6905/dhclient
```

!3. 测试连通性，请参见 [测试 Linux 云服务器 IPv6 的连通性](#)。

### CentOS 7.3/存量 CentOS 7.5/存量 CentOS 7.6 配置 IPv6

1. 远程连接实例。具体操作，请参见 [连接 Linux 实例](#)。
2. 检查实例是否已开启 IPv6 服务，执行如下命令：

```
ip addr | grep inet6  
或者  
ifconfig | grep inet6
```

- 若实例未开启 IPv6 服务，请根据下文继续开启 IPv6 服务。
- 若返回 inet6 相关内容，表示实例已成功开启 IPv6 服务，您可以跳至 [第8步](#) 继续操作。

3. 执行如下命令，打开 etc 文件夹下的 sysctl.conf 文件。

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

4. 按 “i” 切换至编辑模式，将如下的 IPv6 相关参数设置为0。

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

```
# disable ipv6 default
net.ipv6.conf.all.disable_ipv6 = 0
net.ipv6.conf.default.disable_ipv6 = 0
net.ipv6.conf.lo.disable_ipv6 = 0

net.ipv4.conf.all.promote_secondaries = 1
net.ipv4.conf.default.promote_secondaries = 1
net.ipv6.neigh.default.gc_thresh3 = 4096
net.ipv4.neigh.default.gc_thresh3 = 4096

kernel.softlockup_panic = 1
kernel.sysrq = 1
vm.overcommit_memory = 1
```

5. 按“Esc”，输入“:wq”，保存文件并返回。

6. 执行如下命令，对参数进行加载。

```
sysctl -p
```

7. 执行如下命令，查看是否修改成功。

```
sysctl -a | grep ipv6 | grep disable
```

显示结果如下，则已成功修改。

```
/etc/sysctl.conf 45L, 1385C Written
[root@VM_23_16_centos ~]# sysctl -a | grep ipv6 | grep disable
sysctl: reading key "net.ipv6.conf.all.stable_secret"
sysctl: reading key "net.ipv6.conf.default.stable_secret"
sysctl: reading key "net.ipv6.conf.eth0.stable_secret"
sysctl: reading key "net.ipv6.conf.lo.stable_secret"
net.ipv6.conf.all.disable_ipv6 = 0
net.ipv6.conf.default.disable_ipv6 = 0
net.ipv6.conf.eth0.disable_ipv6 = 0
net.ipv6.conf.lo.disable_ipv6 = 0
[root@VM_23_16_centos ~]#
```

8. 执行如下命令，打开或创建 `/etc/sysconfig/network-scripts/` 文件夹下的 `ifcfg-eth0` 文件。

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

9. 按“i”切换至编辑模式，增加如下内容。

```
DHCPV6C=yes
```

```
DHCPV6C=yes
```

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

- ```
default dev eth0
```



[illegible]

3. 按“Esc”，输入“:wq”，保存文件并返回。
4. 执行如下命令，重新启动网卡。

service network restart  
或者  
systemctl restart network

5. 依次执行如下命令，查看是否已经获取到 IPv6 地址。

```
dhclient -6  
ifconfig
```

```
[root@VM_23_16_centos ~]# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.0.1 netmask 255.255.255.0 broadcast 10.0.0.255
    inet6 fe80::208:1:ff:fe00:0000 prefixlen 64 scopeid 0x20<link>
    inet6 2001::18e prefixlen 64 scopeid 0x0<global>
    ether 52:54:00:06:05:57 txqueuelen 1000 (Ethernet)
    RX packets 7400400 bytes 738255010 (704.0 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 6293549 bytes 875070585 (834.5 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

[root@VM_23_16_centos ~]#
```

6. 执行如下命令，打开 `/etc/ssh/` 文件夹下的 `sshd_config` 文件。

```
vim /etc/ssh/sshd_config
```

7. 按 “i” 切换至编辑模式，删除对 `AddressFamily any` 的注释（即删除前面的 `#`），为 `ssh` 等应用程序开启 IPv6 监听。

```
$OpenBSD: sshd_config,v 1.100 2016/08/15 12:32:04 naddy Exp $

# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/local/bin:/usr/bin

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options override the
# default value.

# If you want to change the port on a SELinux system, you have to tell
# SELinux about this change.
# semanage port -a -t ssh_port_t -p tcp #PORTNUMBER

#Port 22
AddressFamily any
AddressFamily inet
ListenAddress 10.10.10.10
ListenAddress 10.10.10.10
HostKey /etc/ssh/ssh_host_rsa_key
HostKey /etc/ssh/ssh_host_dsa_key
HostKey /etc/ssh/ssh_host_ecdsa_key
HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
SyslogFacility AUTHPRIV
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
#PermitRootLogin yes
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

#PubkeyAuthentication yes

# The default is to check both .ssh/authorized_keys and .ssh/authorized_keys2
-- INSERT --
```

8. 按“Esc”，输入“:wq”，保存文件并返回。

9. 执行如下命令，重启 ssh 进程。

```
service sshd restart
```

10. 执行如下命令，查看 ssh 是否已经监听 IPv6。

```
netstat -tupln
```

```
root@VM_0_164_centos:~  
7148/dhclient  
[root@VM_0_164_centos ~]# ^C  
[root@VM_0_164_centos ~]# vim /etc/ssh/sshd_config  
[root@VM_0_164_centos ~]# service sshd restart  
Redirecting to /bin/systemctl restart sshd.service  
[root@VM_0_164_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  
5148/nginx: master  
tcp        0      0 0.0.0.0:22             0.0.0.0:*               LISTEN  
25391/sshd  
tcp6       0      0 :::80                  :::*                     LISTEN  
5148/nginx: master  
tcp6       0      0 :::22                  :::*                     LISTEN  
25391/sshd  
udp        0      0 0.0.0.0:68             0.0.0.0:*               LISTEN  
6905/dhclient
```

1. 测试连通性，请参见 [测试 Linux 云服务器 IPv6 的连通性](#)。

## Debian 8.2 配置 IPv6

1. 远程连接实例。具体操作，请参见 [连接 Linux 实例](#)。
2. 检查实例是否已开启 IPv6 服务，执行如下命令：

```
ip addr | grep inet6  
或者  
ifconfig | grep inet6
```

- 若实例未开启 IPv6 服务，请根据下文继续开启 IPv6 服务。
- 若返回 inet6 相关内容，表示实例已成功开启 IPv6 服务，您可以跳至 [第6步](#) 继续操作。

3. 执行如下命令，打开 etc 文件夹下的 sysctl.conf。

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

4. 按 “i” 切换至编辑模式，将如下的 IPv6 相关参数设置为0。

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

5. 按 “Esc”，输入 “:wq”，保存文件并返回。
6. 执行如下命令，对参数进行加载。

```
sysctl -p
```

7. 依次执行如下命令，查看是否已经获取到 IPv6 地址。

```
dhclient -6  
ifconfig
```

```
root@VM-24-10-debian:~# ifconfig  
eth0      Link encap:Ethernet  HWaddr 52:54:00:bf:8a:4a  
          inet addr:10.0.0.10  Bcast:10.0.0.255  Mask:255.255.255.0  
          inet6 addr: fe80::214:0000:0000:0000/64 Scope:Link  
          inet6 addr: 2001::214:0000:0000:0000/64 Scope:Global  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
          RX packets:12457 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:11235 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:1404471 (1.3 MiB)  TX bytes:1213697 (1.1 MiB)  
  
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)
```

8. Debian 8.2 系统默认为 ssh ( 22端口 ) 开启 IPv6 监听, 无需特殊配置, 您可执行如下命令, 进行查看。

```
netstat -tupln
```

```
root@VM-24-11-debian:~# netstat -tupln  
Active Internet connections (only servers)  
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name  
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      349/sshd  
tcp        0      0 127.0.0.1:25            0.0.0.0:*               LISTEN      664/exim4  
tcp6       0      0 :::22                  :::*                   LISTEN      349/sshd  
tcp6       0      0 :::1:25                 :::*                   LISTEN      664/exim4  
udp        0      0 0.0.0.0:68              0.0.0.0:*               254/dhclient  
udp        0      0 0.0.0.0:25284           0.0.0.0:*               4189/dhclient  
udp        0      0 0.0.0.0:24313           0.0.0.0:*               254/dhclient
```

9. 执行如下命令, 配置默认路由。

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

10. 测试连通性, 请参见 [测试 Linux 云服务器 IPv6 的连通性](#)。

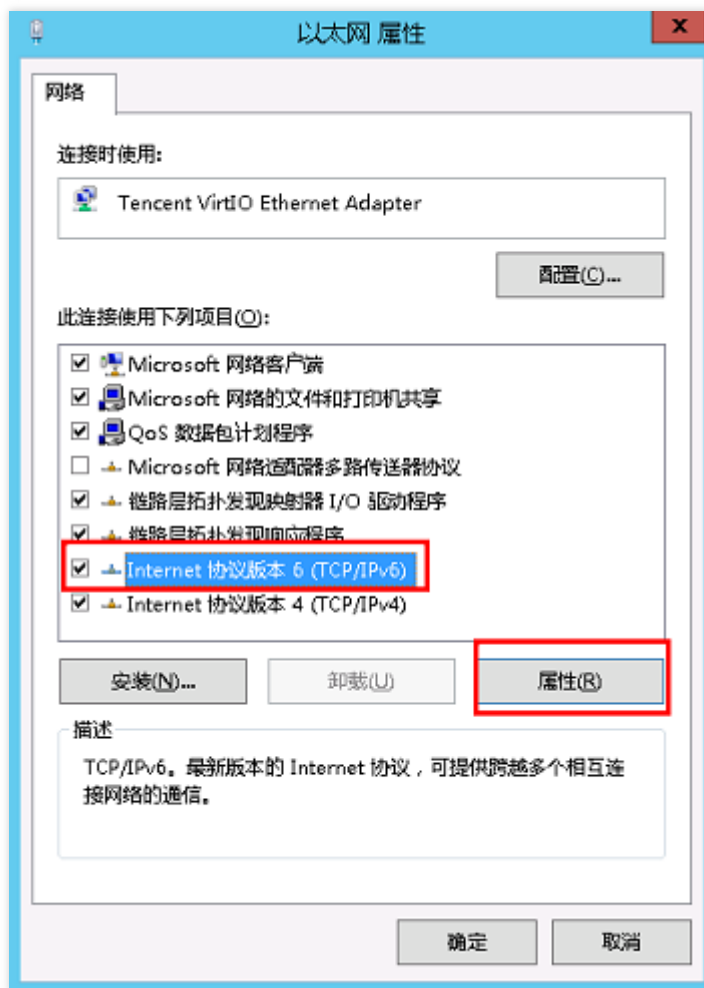
## Windows 云服务器配置 IPv6

如下操作以 Windows 2012 为例：

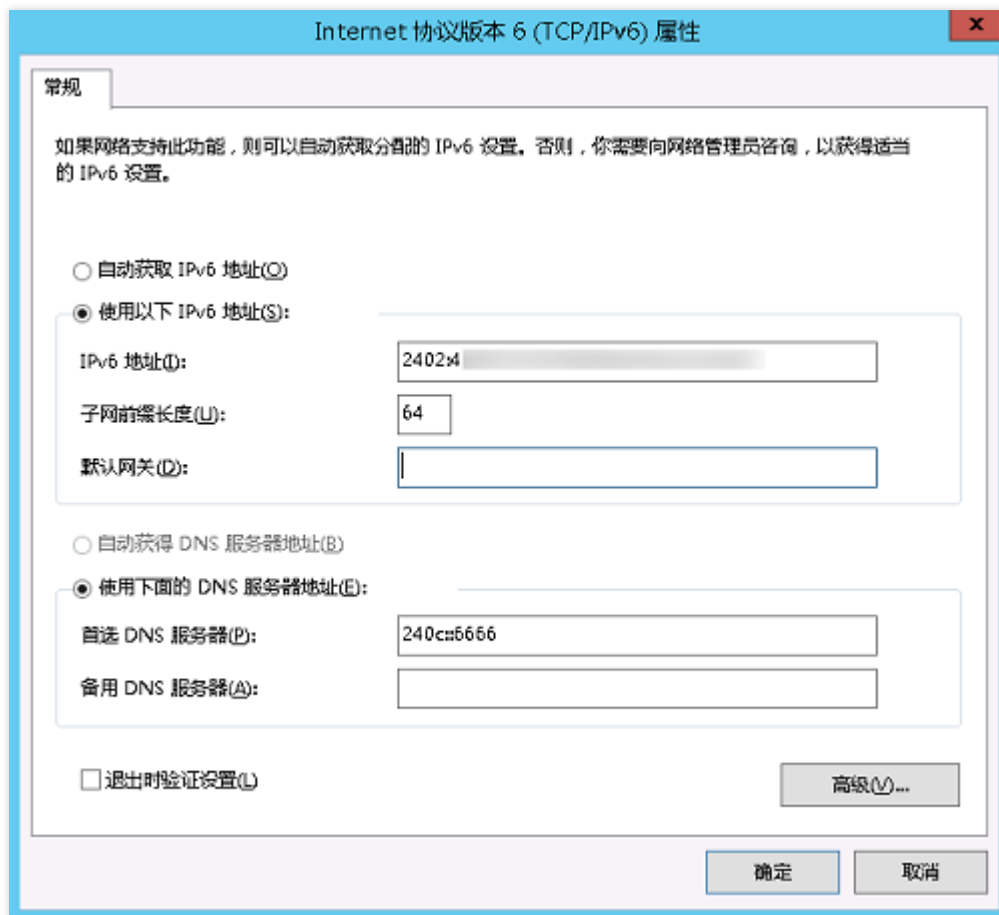
1. 登录云服务器实例, 进入操作系统的【控制面板】>【网络和 Internet】>【网络和共享中心】, 单击命名为“以太网”的网卡进行编辑。



2. 在“以太网状态”弹窗中，单击【属性】。
3. 在“以太网属性”弹窗中，选中【Internet 协议版本6 (TCP/IPv6)】并单击【属性】。



4. 在“Internet 协议版本6 (TCP/IPv6) 属性”弹窗中，手工输入云服务器获取到的 IPv6 地址并设置 DNS，单击【确定】。



5. 在操作系统界面,选择左下角的 , 单击 , 打开“Windows PowerShell”窗口,依次执行如下命令配置默认路由以及查看 IPv6 地址,并通过 Ping 和远程桌面测试 IPv6 连通性。

```
netsh interface ipv6 add route ::/0 "以太网"  
ipconfig
```



```
PS C:\Users\Administrator> netsh interface ipv6 add route ::/0 "以太网"
确定。

PS C:\Users\Administrator> ipconfig

Windows IP 配置

以太网适配器 以太网:

    连接特定的 DNS 后缀 . . . . . : 
    IPv6 地址 . . . . . : 240c::6666
    本地链接 IPv6 地址. . . . . : fe80::...
    IPv4 地址 . . . . . : 10.23.255.255
    子网掩码 . . . . . : 255.255.255.0
    默认网关. . . . . : ::
                           10.23.255.255

隧道适配器 isatap.{A971A...}:

    媒体状态 . . . . . : 媒体已断开
    连接特定的 DNS 后缀 . . . . . : 

PS C:\Users\Administrator> ping -6 240c::6666

正在 Ping 240c::6666 具有 32 字节的数据:
来自 240c::6666 的回复: 时间=26ms
来自 240c::6666 的回复: 时间=27ms
来自 240c::6666 的回复: 时间=26ms

240c::6666 的 Ping 统计信息:
    数据包: 已发送 = 3, 已接收 = 3, 丢失 = 0 (0% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 26ms, 最长 = 27ms, 平均 = 26ms
Control-C
PS C:\Users\Administrator>
```

## 测试 Linux 云服务器 IPv6 的连通性

可通过 Ping 和 ssh 等操作来测试 Linux 云服务器 IPv6 的连通性。

- **步骤1**：通过 Ping 进行测试，操作如下：
  - 如果弹性网卡的 IPv6 地址已开通公网，则可在云服务器中执行 `ping6 240c::6666` 或 `ping6 www.qq.com` 进行测试，如下图所示：

```
[root@VM_24_8_centos ~]# ping -6 240c::6666
PING 240c::6666(240c::6666) 56 data bytes
64 bytes from 240c::6666: icmp_seq=1 ttl=53 time=29.1 ms
64 bytes from 240c::6666: icmp_seq=2 ttl=53 time=29.0 ms
64 bytes from 240c::6666: icmp_seq=3 ttl=53 time=29.0 ms
64 bytes from 240c::6666: icmp_seq=4 ttl=53 time=29.0 ms
64 bytes from 240c::6666: icmp_seq=5 ttl=53 time=29.0 ms
64 bytes from 240c::6666: icmp_seq=6 ttl=53 time=29.0 ms
^C
--- 240c::6666 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5005ms
rtt min/avg/max/mdev = 29.011/29.055/29.162/0.049 ms
[root@VM_24_8_centos ~]# ping -6 www.qq.com
PING www.qq.com(2402:4e00:8010::154 (2402:4e00:8010::154)) 56 data bytes
64 bytes from 2402:4e00:8010::154 (2402:4e00:8010::154): icmp_seq=1 ttl=56 time=3.49 ms
64 bytes from 2402:4e00:8010::154 (2402:4e00:8010::154): icmp_seq=2 ttl=56 time=3.48 ms
64 bytes from 2402:4e00:8010::154 (2402:4e00:8010::154): icmp_seq=3 ttl=56 time=3.49 ms
64 bytes from 2402:4e00:8010::154 (2402:4e00:8010::154): icmp_seq=4 ttl=56 time=3.50 ms
64 bytes from 2402:4e00:8010::154 (2402:4e00:8010::154): icmp_seq=5 ttl=56 time=3.49 ms
^C
--- www.qq.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 3.489/3.494/3.501/0.074 ms
[root@VM_24_8_centos ~]#
```



- ```
[root@VM_48_14_centos ~]# ping6 2402:          :aad7
PING 2402:          :aad7(2402:          :aad7) 56 data bytes
64 bytes from 2402:          :aad7: icmp_seq=1 ttl=64 time=0.293 ms
64 bytes from 2402:          :aad7: icmp_seq=2 ttl=64 time=0.280 ms
64 bytes from 2402:          :aad7: icmp_seq=3 ttl=64 time=0.295 ms
64 bytes from 2402:          :aad7: icmp_seq=4 ttl=64 time=0.315 ms
^C
--- 2402:          :aad7 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2999ms
rtt min/avg/max/mdev = 0.280/0.295/0.315/0.024 ms
[root@VM_48_14_centos ~]#
```

- 执行如下命令查看 IPv6 地址，并用 PuTTY 或者 Xshell 等软件，测试能否通过 IPv6 地址 ssh 到云服务器。

ifconfig

The screenshot displays two windows side-by-side. The left window is a terminal session on a CentOS system. It shows the configuration of the SSH service, including setting the authorized keys file to `.ssh/authorized_keys`, restarting the `sshd` service, and running `netstat -tupln` to show listening ports. Below this, the output of `ifconfig` is shown for the `eth0` interface, highlighting the IP address `10.23.24.8` and the netmask `255.255.255.0`. The right window is the "PuTTY Configuration" dialog box. In the "Session" category, the "Host Name (or IP address)" field is set to `102.4e00` and the "Port" is `22`. The "Connection type" is set to "SSH".

```
#MaxAuthTries 6
#MaxSessions 10

#RSAAuthentication yes
#PubkeyAuthentication yes
#AuthorizedKeysFile .ssh/authorized_keys
#AuthorizedKeysCommand none
#AuthorizedKeysCommandRunAs nobody
"/etc/ssh/sshd_config" 139L, 3906C written
[root@VM_24_8_centos ~]# service sshd restart
Stopping sshd: [ OK ]
Starting sshd: [ OK ]

[root@VM_24_8_centos ~]# netstat -tupln
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      *
tcp        0      0 :::22                   :::*                    LISTEN      *
udp        0      0 *:123                   0.0.0.0:*               LISTEN      *
udp        0      0 127.0.0.1:123          0.0.0.0:*               LISTEN      *
udp        0      0 0.0.0.0:68             0.0.0.0:*               LISTEN      *
udp        0      0 *:2                      e:123 ::*              LISTEN      *
udp        0      0 fe80::                  :123 ::*               LISTEN      *
udp        0      0 ::1:123                 ::*                     LISTEN      *
udp        0      0 fe80::                  :546 ::*               LISTEN      *

[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::50:/64 Scope:Link
          inet6 addr: 2402:4e00::8/64 Scope:Global
          UP BROADCAST RUNNING MULTICAST Mtu:1500 Metric:1
          RX packets:117952 errors:0 dropped:0 overruns:0 frame:0
          TX packets:89314 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:8529369 (8.1 MiB) TX bytes:8581100 (8.1 MiB)

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 KiB) TX bytes:0 (0.0 KiB)
```

**PuTTY Configuration**

Category:

- Session
  - Logging
- Terminal
  - Keyboard
  - Bell
  - Features
- Window
  - Appearance
  - Behaviour
  - Translation
  - Selection
  - Colours
- Connection
  - Data
  - Proxy
  - Telnet
  - Rlogin
  - + SSH
    - Serial

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address) Port  
 102.4e00 :8| 22

Connection type:  
☐ Raw ☐ Telnet ☐ Rlogin ☒ SSH ☐ Serial

Load, save or delete a stored session

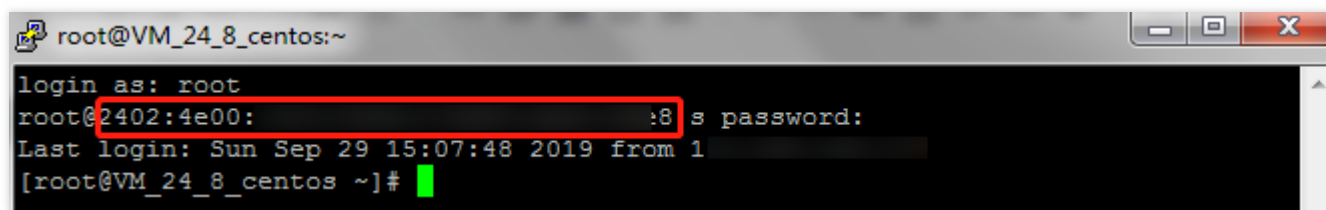
Saved Sessions

Default Settings Load Save Delete

Close window on exit:  
☐ Always ☐ Never ☒ Only on clean exit

About Help Open Cancel

成功结果如下图所示：



```
root@VM_24_8_centos:~  
login as: root  
root@2402:4e00:~# s password:  
Last login: Sun Sep 29 15:07:48 2019 from 1  
[root@VM_24_8_centos ~]#
```