* [前](https://stray.love/jiao-cheng/zerotier-zhong-jie-jiao-cheng%22%20%5Cl%20%22toc_0)
	+ [初阶方案](https://stray.love/jiao-cheng/zerotier-zhong-jie-jiao-cheng%22%20%5Cl%20%22toc_1)
	+ [正确的做法是什么？](https://stray.love/jiao-cheng/zerotier-zhong-jie-jiao-cheng%22%20%5Cl%20%22toc_2)
	+ [正式开始](https://stray.love/jiao-cheng/zerotier-zhong-jie-jiao-cheng%22%20%5Cl%20%22toc_3)
	+ [更进一步](https://stray.love/jiao-cheng/zerotier-zhong-jie-jiao-cheng%22%20%5Cl%20%22toc_4)
	+ [ZeroTier 的 Managed Routes 功能](https://stray.love/jiao-cheng/zerotier-zhong-jie-jiao-cheng%22%20%5Cl%20%22toc_5)
	+ [需要注意](https://stray.love/jiao-cheng/zerotier-zhong-jie-jiao-cheng%22%20%5Cl%20%22toc_6)
	+ [其他 FAQ](https://stray.love/jiao-cheng/zerotier-zhong-jie-jiao-cheng%22%20%5Cl%20%22toc_7)
* [后](https://stray.love/jiao-cheng/zerotier-zhong-jie-jiao-cheng%22%20%5Cl%20%22toc_8)

# 前

这篇中阶教程从这个网络拓扑图说起。



本文教大家如何通过 ZeroTier 让拓扑图中的 两台 PC、两台 Router、两台 Server、iPhone 之间可以互相访问。

## 初阶方案

如果读过初阶教程，那一定能想得到最容易的方法：在所有的设备上都安装 Zerotier 就可以实现互相访问的目的。但这也是最麻烦的方法，毕竟要在所有设备上安装 ZeroTier。

## 正确的做法是什么？

只需要在两台 Router上安装 ZeroTier 并正确配置 路由表 和 防火墙 即可。

## 正式开始

1. 在 Router1 上安装 Zerotier，并填写 network ID 加入 ZeroTier 网络
2. 假设 ZeroTier 为 Router1 分配的 IP 为 10.10.10.11
3. 在 ZeroTier 官网设置 Managed Routes 选项 如下图填写：



1. 点击加号，等待生效。
2. 配置 Router1 的防火墙（以 OPENWRT 路由器为例）

# 其中 zt0 是 ZeroTier 的物理接口，可以使用 zerotier-cli listnetworks 命令查看，其中 zt0 在其他平台可能是 其他名字

root@LEDE:~# zerotier-cli listnetworks

200 listnetworks <nwid> <name> <mac> <status> <type> <dev> <ZT assigned ips>

200 listnetworks xxxxxxxxx MarIxs xx:xx:xx:xx:xx:xx OK PRIVATE zt0 10.10.10.11/20

#配置防火墙

root@LEDE:~# iptables -I FORWARD -i zt0 -j ACCEPT

root@LEDE:~# iptables -I FORWARD -o zt0 -j ACCEPT

root@LEDE:~# iptables -t nat -I POSTROUTING -o zt0 -j MASQUERADE

1. 为了测试 iPhone 安装并运行 ZeroTier 并加入 ZeroTier 网络

如此 Router1 下的所有设备和 iPhone 可以互相访问了，也就是说 iPhone、Router1、PC1、Server1 任意两个之间都可以 ping 通。

比如在 iPhone 上 ping 10.10.10.11（Router1）、192.168.10.1（Router1）、192.168.10.100（PC1）、192.168.10.200（Server1） 都是没问题的。

## 更进一步

将 Router2 网络加入 ZeroTier，过程和 Router1 类似。

1. 在 Router2 上安装 Zerotier，并填写相同 network ID 加入 ZeroTier 网络
2. 假设 ZeroTier 为 Router2 分配的 IP 为 10.10.10.12
3. 在 ZeroTier 官网设置 Managed Routes 选项 如下图填写：



1. 点击加号，等待生效。
2. 配置 Router2 的防火墙（以 OPENWRT 路由器为例）

#其中 zt0 是 ZeroTier 的物理接口，可以使用 zerotier-cli listnetworks 命令查看，其中 zt0 在其他平台可能是 其他名字

root@LEDE:~# zerotier-cli listnetworks

200 listnetworks <nwid> <name> <mac> <status> <type> <dev> <ZT assigned ips>

200 listnetworks xxxxxxxxx MarIxs xx:xx:xx:xx:xx:xx OK PRIVATE zt0 10.10.10.12/20

#配置防火墙

root@LEDE:~# iptables -I FORWARD -i zt0 -j ACCEPT

root@LEDE:~# iptables -I FORWARD -o zt0 -j ACCEPT

root@LEDE:~# iptables -t nat -I POSTROUTING -o zt0 -j MASQUERADE

至此，拓扑图上的所有设备都可以互相访问了。而 Router1 和 Router2 所在的两个网络被无缝连接在了一起，如果两个网络在异地，那就是所谓的异地组网了。

## ZeroTier 的 Managed Routes 功能

按上面教程设置后， Managed Routes 如下图，对于熟悉路由表的朋友应该没什么难度，但对于对于网络了解很少的朋友可能会有些困难。

这里简单说明下：

* networks/bits：填写需要被访问的网段
* （lan）：网络中接入 ZeroTier 的设备被分配的 IP

所以前面的教程例子很容易理解了，以 Router1 为例：

* 需要被访问的是 Router1 下的设备，就是 Router1 的 lan IP 段，拓扑图上可以看出 Router1 lan IP 段为 192.168.10.1/24
* 这部分网络，接入 ZeroTier 的是 Router1 ，被分配的 IP 为 10.10.10.11
* 所以 networks/bits 为 192.168.10.1/24，（lan）为 10.10.10.11

用相同的思路分析 Router2 的网络，也能得到：networks/bits 为 192.168.5.1/24，（lan）为 10.10.10.12

ZeroTier 会根据你的设置，自动（智能）下发路由表到设备中，从而实现多个网段互联互通。感兴趣的朋友可以按照教程组网，然后查看设备上路由表。

## 需要注意

* **组网的多个局域网，IP 段不能冲突，**
	+ 如拓扑图中 Router1 192.168.10.1/24 和 Router2 192.168.5.1/24 是不冲突的。
* **防火墙的配置可能因设备而异**
	+ 主要的目的是放行 ZeroTier 的数据包和 SNAT 转换。