

[cofftech](#): [opencv源码](#): [http://www.eyesourceco ...](http://www.eyesourceco...)

[opencv资料和文档](#)

[langke93](#): [wangzhengyi_nopass.key](#)这个怎么生成没写

[nginx搭建https服务器](#)

使用OpenVPN的桥接模式扩展内部局域网

1.背景

OpenVPN是一款高度可扩展的VPN软件，除了既有的将应用客户端安全接入服务器这一传统功能外，还可以让你无缝的接入一个远程的局域网，正如你身在该局域网一样，如果你不用OpenVPN，你将很难做到这一点。当然，你可以选择像IPSec这样的重量级VPN，但是你的生活从此将不再简单，你也可以使用拨号，连接到远程，但是你永远无法体验完全接入这种身临其境的感觉。

这就是OpenVPN的桥接功能，有了该功能，你将可以无限扩展局域网，你甚至可以将全世界连接在一个局域网内，每一个OpenVPN服务器都可以作为一个以太网桥存在，将局域网直接拉到很远的地方，距离再也不是问题。

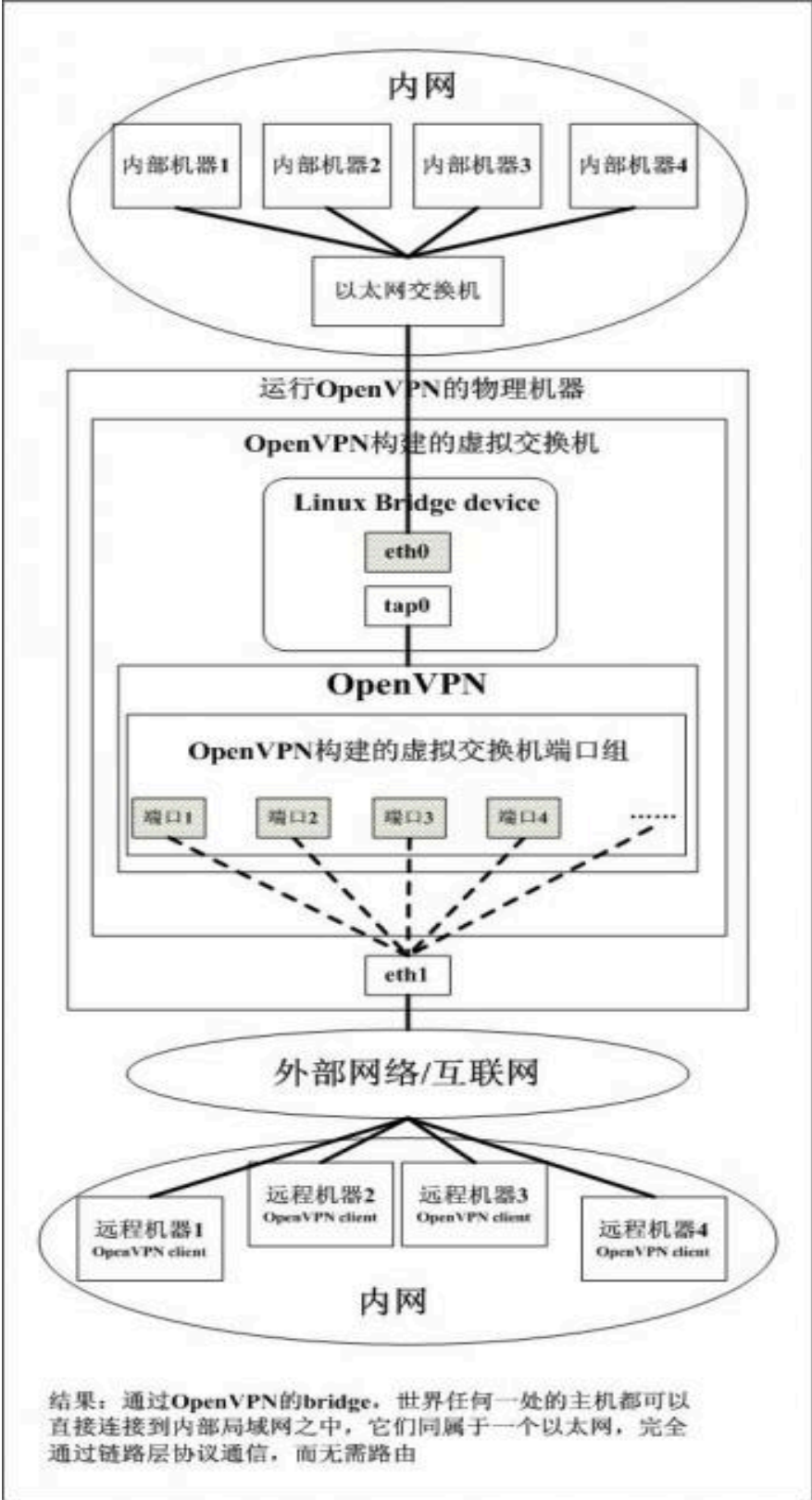
2.理论

OpenVPN有两种虚拟模式，一种是三层路由模式，另一种是桥接模式，我们常用的是路由模式，这种方式也是其它VPN软件经常使用的模式，毕竟我们使用VPN的目的是“安全的访问应用”而对于“安全的接入远程网络”的需求并不是很明显，但是一旦你需要安全接入远程网络，你就不得不需要路由这个大伙计，有时候这个伙计不是很友好，特别是网络部署很复杂的时候，这个时候，你会想什么，如果用一根很长很硬朗的线将远程的用户机器直接拉入内部网的一个交换机端口上将会怎么，甚好！幸运的是，OpenVPN可以为你提供这根线，稍显不幸的是，你还是需要做一些工作。

OpenVPN提供的桥接功能实现了上述的魔法，你只需要将其虚拟网卡模式配置成tap，然后将OpenVPN服务器打开的tap网卡加入到一个bridge，当然该bridge中起码还需要有一个物理网卡，该



物理网卡处于远程主机希望无缝接入的局域网之中。这很简单，下图展示了这个原理：



3.怎么做

如果你对这个主题很感兴趣，并且你已经很精通OpenVPN的桥接配置，那么下面的内容就不用看了，你的动作肯定比我快，但是如果你还没有配置过这个主题，我劝你还是看下去吧，因为如果你google的话，通篇都是在解释OpenVPN官网以及源码包中自带的那几个脚本，而那几个脚本是能让功能可用，但是对于理解整个过程帮助似乎不大，因此还是将问题分解开，一步一步做，对知其然甚有好处。

3.1.网络拓扑图：

略



3.2.创建一个网桥

brctl addbr br0

3.3.加入物理网卡到br0

将连入内部局域网的物理网卡加入br0

brctl addif br0 eth0

3.4.配置OpenVPN

在OpenVPN的配置文件中加入server-bridge [gw] [mask] [start-IP] [end-IP]

注意，start-IP到end-IP这几个IP地址不能和局域网内既有的地址相冲突，因为这些地址要分给远程机器了，而远程机器实际上已经通过OpenVPN接入到局域网内部了，而一个局域网内部，不能有两台机器的IP地址一样。

3.5.启动OpenVPN服务

按照常规的方式启动OpenVPN：openvpn --config server.cfg

然后将tap0加入到br0：brctl addif br0 tap0



请注意，这种桥接方式启动的OpenVPN服务器上的tap0虚拟网卡没有IP地址，因为整个过程没有IP层的内容。

3.6.在远程启动OpenVPN客户端

按照常规的方式启动OpenVPN客户端后，客户端将被分配到一个内网的地址，虽然它是从外部连接进来的。

3.7.测试

在远程OpenVPN客户端所在的机器上ping局域网内部的主机，然后查看arp表，内部局域网内的主机的mac地址已经到达了远程OpenVPN客户端所在的机器，它们属于一个局域网了。

分享到： 

[一个Linux虚拟机里面的Bridge设备引发的悲 ... | Windows系统下hosts文件工作原理](#)

2011-10-01 20:44

浏览 827

[评论\(0\)](#)

[查看更多](#)

评论

发表评论



[您还没有登录,请您登录后再发表评论](#)

相关推荐

[使用Cisco Packet Tracer实现两个局域网通信](#)

使用Cisco Packet Tracer实现两个局域网通信，亲自测试可以使用

[基于openvpn的web管理系统，前后端分离设计。](#)

基于openvpn的web管理系统，前后端分离设计。



[MedShakeEHR-Ansible:在Debian上自动安装Ansible的MedShakeEHR](#)

安装OpenVPN 保护OpenVPN 在局域网中安装Orthanc ? 先决条件 Ansible> 2.5 Ansible> 2.9 (用于SSH-sec角色) 在客户端计算机和服务器计算机之间已正确配置SSH身份验证。 安装 克隆项目并安装角色： gi...

[一款局域网共享的软件工具](#)

在IT领域，局域网共享软件工具是一种至关重要的应用，尤其在办公室或家庭网络环境中，它们使得用户能够方便地在连接在同一局域网内的设备之间分享文件、打印机和其他资源。"易共享"这款软件显然是针对这个需求而设...