<https://www.cnblogs.com/ambon/articles/5634933.html>

## 利用Azure作为远程 往外面的服务器

端口要打开，management的端口，防火墙端口，安装bitserver,要连的电脑装bitClient,配置s2c

## 

## 远程桌面

远程桌面采用的是一种类似TELNET的技术，他是从TELNET协议发展而来的。通俗的讲他就是图形化的TELNET.（他是一种C/S模式，客户机可以通过TELNET登录到高配置的服务器上，在服务器上运行程序）。

远程桌面很多用户都认为是从WIN2000 SERVER才开始引入的，实际上我们可以在WIN98甚至是DOS中看到他的身影。微软操作系统发展至今只有以下三个操作系统可以使用远程桌面功能，他们是WINDOWS 2000SERVER，WINDOWS XP和WINDOWS 2003。

远程连接接必须条件：

1. 作为远程桌面的服务器端（也就是你打算控制的电脑）
2. 作为远程桌面的客户端（也就是你打算用来控制服务器端的电脑）
3. 连接
4. 其它（在默认情况下，微软远程桌面连接将会分别在服务端和远程客户端使用的端口为3389端口，在设置NAT端口映射时，你可以将内网的3389端口映射在NAT服务器上的6666(也可以是其它没有被占用的数值)端口中，这样在远程客户端连接6666时就会连接到内网的3389端口）

摘自csdn：http://bbs.csdn.net/topics/330080637

问：两台没有独立IP的机器是怎么建立TCP连接的

TCP,UDP都可以的，不过一般来说，像这种多媒体传输，UDP是比较常用的  
楼主所说的 “没有独立的ip地址” ，我解释一下，NAT（网络地址映射）  
路由器都有这功能，它把内网机器的  IP:端口， 映射成外网的 IP:端口。  
  
但外网想通过路由访问内网的机器，路由是不同意的，这就要用到内网穿透，就是楼上各位说的“打洞”  
  
TCP 和 UDP 都可以 打洞的，不过TCP比较麻烦

[SSH和telnet的区别](http://blog.csdn.net/xd1103121507/article/details/7110059)

原文：http://blog.csdn.net/xd1103121507/article/details/7110059

简言之，SSH更安全！  
  
    使用Telnet这个用来访问远程计算机的TCP/IP协议以控制你的网络设备相当于在离开某个建筑时大喊你的用户名和口令。很快会有人进行监听，并且他们会利用你安全意识的缺乏。传统的网络服务程序如：ftp、pop和telnet在本质上都是不安全的，因为它们在网络上用明文传送口令和数据，别有用心的人非常容易就可以截获这些口令和数据。而且，这些服务程序的安全验证方式也是有其弱点的，就是很容易受到“中间人”（man-in-the-middle）这种方式的攻击。所谓“中间人”的攻击方式，就是“中间人”冒充真正的服务器接收你的传给服务器的数据，然后再冒充你把数据传给真正的服务器。服务器和你之间的数据传送被“中间人”一转手做了手脚之后，就会出现很严重的问题。  
　　SSH是替代Telnet和其他远程控制台管理应用程序的行业标准。SSH命令是加密的并以几种方式进行保密。   
　　在使用SSH的时候，一个数字证书将认证客户端(你的工作站)和服务器(你的网络设备)之间的连接，并加密受保护的口令。SSH1使用RSA加密密钥，SSH2使用数字签名算法(DSA)密钥保护连接和认证。加密算法包括Blowfish，数据加密标准(DES)，以及三重DES(3DES)。SSH保护并且有助于防止欺骗，“中间人”攻击，以及数据包监听。  
    通过使用SSH把所有传输的数据进行加密，这样“中间人”这种攻击方式就不可能实现了，而且也能够防止DNS和IP欺骗。还有一个额外的好处就是传输的数据是经过压缩的，所以可以加快传输的速度。SSH有很多功能，它既可以代替telnet，又可以为ftp、pop、甚至ppp提供一个安全的“通道”。

