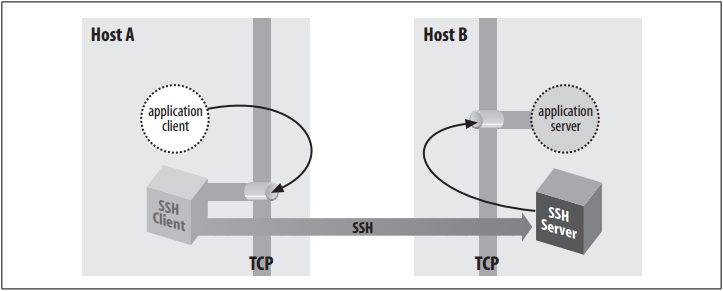
# SSH本地端口转发：

如果应用程序的客户端和 SSH 的客户端位于 SSH 隧道的同一侧，而应用程序的服务器和 SSH 服务器位于 SSH 隧道的另一侧，那么这种端口转发类型就是本地端口转发。



客户机：win10 ip:192.168.10.149

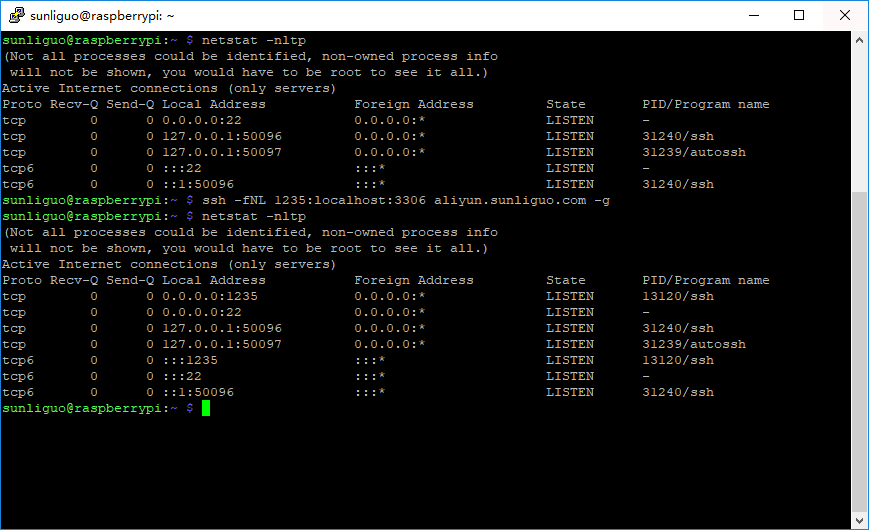
树莓派：linux ip:192.168.10.71 HostA

阿里云主机：linux aliyun.sunliguo.com 外网 HostB

实验目的：客户机访问阿里云主机上的mysql服务。阿里云主机默认只放开22端口。

方法一：

在树莓派上运行：



只会监听：127.0.0.1这个地址。

如果监听所有的端口，ssh -fNL \*:1235:localhost:3306 aliyun.sunliguo.com 或者是-g参数

sunliguo@raspberrypi:~ $ ssh -fNL 1235:localhost:3306 aliyun.sunliguo.com -g

现在在客户机上运行Navicat for mysql 连接 192.168.10.71 1235端口 就可以访问阿里云的mysql服务了。

下面两个命令和上面有什么不同？

sunliguo@raspberrypi:~ $ ssh -L 1234:aliyun.sunliguo.com:3306 -fN aliyun.sunliguo.com -g

sunliguo@raspberrypi:~ $ ssh -L 1234:127.0.0.1:3306 -fN aliyun.sunliguo.com -g

-L [bind\_address:]port:host:hostport

-L [bind\_address:]port:remote\_socket

-L local\_socket:host:hostport

-L local\_socket:remote\_socket

Specifies that connections to the given TCP port or Unix socket on the local (client) host are to be forwarded to the given host and port, or Unix socket, on the remote side.

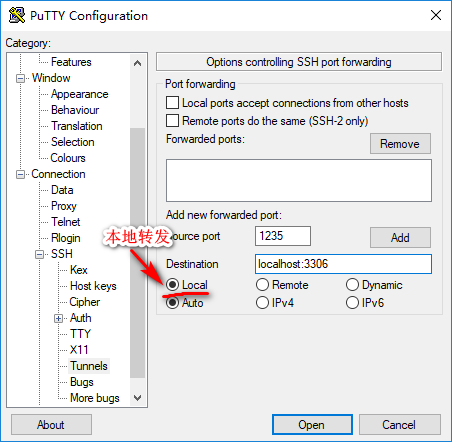
This works by allocating a socket to listen to either a TCP port on the local side, optionally bound to the specified bind\_address, or to a Unix socket. Whenever a connection is made to the local port or socket, the connection is forwarded over the secure channel, and a connection is made to either host port hostport, or the Unix socket remote\_socket, from the remote machine.

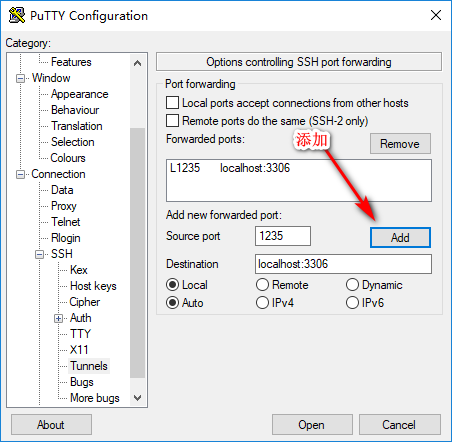
Port forwardings can also be specified in the configuration file. Only the superuser can forward privileged ports. IPv6 addresses can be specified by enclosing the address in square brackets.

By default, the local port is bound in accordance with the GatewayPorts setting. However, an explicit bind\_address may be used to bind the connection to a specific address. The bind\_address of “localhost” indicates that the listening port be bound for local use only, while an empty address or ‘\*’ indicates that the port should be available from all interfaces.

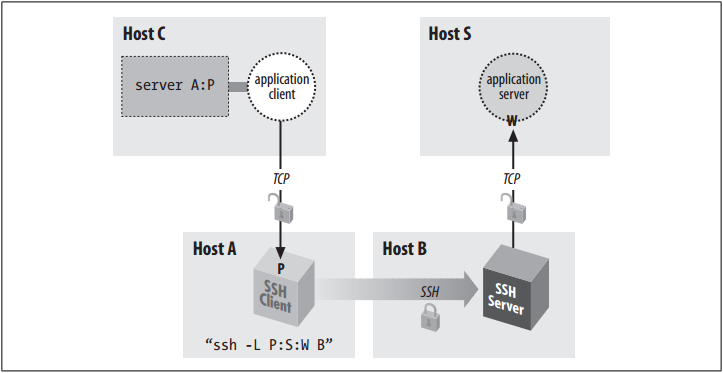
方法二：putty客户端

1:Connectio ->SSH->Tunnels 选中Local，Auto 。Source Port 添加本地要监听的端口，Destionation:添加 localhost:3306然后Add





最后登陆，mysql客户端访问本地的1235端口，就可以连接到aliyun的3306端口了。



上图中的场景可能更符合真实情况(此图来自互联网)。应用程序的客户端和 SSH 客户端分别位于 SSH 隧道同一侧的两台不同的主机上，而应用的服务器端和 SSH 服务器分别位于 SSH 隧道另一侧的两台不同的主机上。此时我们需要使用下面的命令：

$ ssh -g -L P:HostS:W HostB

应用 -g 选项后主机 A 不仅会监听 localhost 的 P 端口，还能够监听所有网络接口的 P 端口，所以主机 C 上的应用客户端就可以把消息发送到主机 A 的 P 端口。

接下来我们必须要介绍本地端口转发的命令格式了：

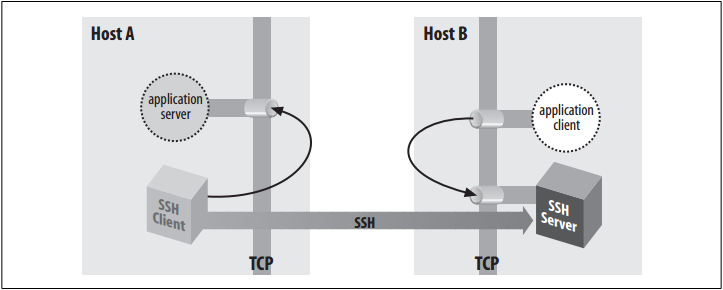
ssh -L <local port>:<remote host>:<remote port> <SSH server host>

SSH server host 是 SSH 服务器所在的主机， remote host 和 remote port 则分别指应用程序服务器所在主机和监听端口。如果 remote host 指定为 localhost 则认为应用程序服务器和 SSH 服务器在同一台主机上。

在结束本地端口转发之前还需要介绍另外两个选项，它们是 f 和 N。上面的命令在创建隧道的同时登录到远程主机，一般情况下我们不需要这个登录。况且一旦这个登录退出，隧道也会随之关闭。我们更期望的是能够创建在后台运行的隧道，这时就需要添加 f 和 N 选项。

**SSH远程端口转发**

如果应用程序的客户端和 SSH 的服务器位于 SSH 隧道的同一侧，而应用程序的服务器和 SSH 的客户端位于 SSH 隧道的另一侧，那么这种端口转发类型就是远程端口转发。



所以，区分本地端口转发和远程端口转发主要是看 SSH 客户端与应用程序的哪一部分在 SSH 隧道的同一侧！远程端口转发的命令格式为：

ssh -R <local port>:<remote host>:<remote port> <SSH server host>

其它的细节两者基本也是一样的。但是远程端口转发不支持 -g 参数，这让我们很难实现类似下面的用例：

内网中主机 A 上运行 Jenkins 服务器监听本机 8080 端口，并运行 SSH 客户端。

外网中的主机 B 上运行 SSH 服务器。

希望可以通过远程端口转发的方式在主机 A 和 B 之间建立隧道，  
然后外网的 Bitbucket 等代码管理服务可以通过 Webhook 的方式访问主机 B 从而触发 Jenkins 服务器中的 Build。

这个问题的根源在于我们执行下面的远程端口转发命令后：

$ ssh -R 18080:localhost:8080 HostB

主机 B 只能监听 localhost 的 18080 端口：

IMG_256

如何让 HostB 监听本机所有网络接口的 18080 端口呢？ 需要通过修改 SSH 服务器的配置来实现这个功能！在 SSH 服务器的配置文件 /etc/ssh/sshd\_config 中添加一行：

GatewayPorts yes

保存后重启 SSH 服务器，然后重新建立隧道：

IMG_257

此时主机 B 已经可以接受外部 webhook 的调用了。

实验背景介绍：

树莓派：ip 192.168.10.71 在办公室内网

阿里云公网：aliyun.sunliguo.com

家中：移动，无公网ip

实验目的：需要在家中内网中访问。

在树莓派上运行：

autossh -NfR 1234:localhost:22 [sunliguo@aliyun.sunliguo.com](mailto:sunliguo@aliyun.sunliguo.com)

或者

ssh -NfR 1234:192.168.10.71:22 [sunliguo@aliyun.sunliguo.com](mailto:sunliguo@aliyun.sunliguo.com)

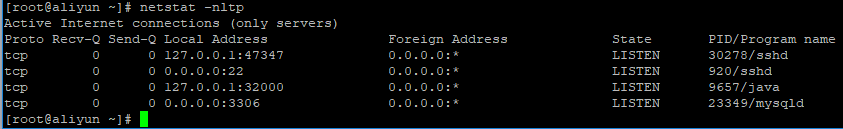
-R [bind\_address:]port:host:hostport

Bind\_address 默认绑定127.0.0.1

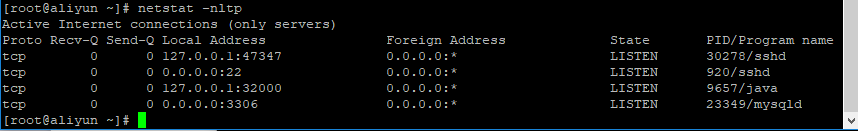
Port 如果指定为0的话，随机绑定，然后返回。

树莓派上执行：





阿里云上显示：



-R [bind\_address:]port:host:hostport

Specifies that the given port on the remote (server) host is to be forwarded to the given host and port on the local side. This works by allocating a socket to listen to port on the remote side, and whenever a connection is made to this port, the connection is forwarded over the secure channel, and a connection is made to host port hostport from the local machine.

Port forwardings can also be specified in the configuration file. Privileged ports can be forwarded only when logging in as root on the remote machine. IPv6 addresses can be specified by enclosing the address in square braces or using an alternative syntax: [bind\_address/]host/port/hostport.

By default, the listening socket on the server will be bound to the loopback interface only. This may be overridden by specifying a bind\_address. An empty bind\_address, or the address ‘\*’, indicates that the remote socket should listen on all interfaces. Specifying a remote bind\_address will only succeed if the server’s GatewayPorts option is enabled (see sshd\_config(5)).

If the port argument is ‘0’, the listen port will be dynamically allocated on the server and reported to the client at run time.