SSH原理了解：

<http://www.ruanyifeng.com/blog/2011/12/ssh_remote_login.html>

<http://www.ruanyifeng.com/blog/2011/12/ssh_port_forwarding.html>

<http://www.2cto.com/Article/201210/158972.html>

安装配置使用：

<http://blog.csdn.net/benkaoya/article/details/8127126>

<https://linux.cn/article-2933-1.html>

<http://blog.csdn.net/hitabc141592/article/details/8523184>

SSH只是一种协议，存在多种实现，既有商业实现，也有开源实现。本文针对的实现是OpenSSH，它是自由软件，应用非常广泛。

1. SSH主要用于计算机间的远程登录(加密)。

2. SSH的安装；(有服务端和客户端)

3. SSH的两种登录方式：

(1)口令登录

整个过程是这样的：

（1远程主机收到用户的登录请求，把自己的公钥发给用户。

（2用户使用这个公钥，将登录密码加密后，发送回来。

（3远程主机用自己的私钥，解密登录密码，如果密码正确，就同意用户登录。

当首次授权登录成功，远程主机的公钥被客户端接受以后，它就会被保存在客户端$HOME/.ssh/known\_hosts文件之中。下次再连接这台主机，系统就会认出它的公钥已经保存在本地了，从而跳过警告部分，直接提示输入密码。

每个SSH用户都有自己的known\_hosts文件，此外系统也有一个这样的文件，通常是/etc/ssh/ssh\_known\_hosts，保存一些对所有用户都可信赖的远程主机的公钥。

(2)公钥登录

注意：需要将客户端的~/.ssh/id\_rsa.pub文件中的公钥拷贝追加到服务端的.ssh/authorized\_keys文件末尾；

所谓"公钥登录"，原理很简单，就是用户将自己的公钥储存在远程主机上。登录的时候，远程主机会向用户发送一段随机字符串，用户用自己的私钥加密后，再发回来。远程主机用事先储存的公钥进行解密，如果成功，就证明用户是可信的，直接允许登录shell，不再要求密码。

(<http://www.2cto.com/Article/201210/158972.html>)

4.服务端和客户端的主程序和配置文件：

服务端主程序：/usr/sbin/sshd

客户端主程序：/usr/bin/ssh

服务端配置文件：/etc/ssh/sshd\_config

(可更改端口等，重启shhd服务生效)

客户端配置文件：~/.ssh/config或/etc/ssh/ssh\_config

(SSH登录使用的用户名、用户验证方式、端口等)

服务端配置文件示例：

/etc/ssh/sshd\_config：

# Package generated configuration file

# See the sshd(8) manpage for details

# What ports, IPs and protocols we listen for

Port 22

客户端配置文件示例：

~/.ssh/config：

host hr

  user root

  hostname 192.168.1.101

  port 22

  identityfile ~/.ssh/id\_rsa

host hj

  user root

  hostname 192.168.1.101

  port 22

  identityfile ~/.ssh/jiajia

~/.ssh/config：

Host <moblab\_server\_IPaddress>

CheckHostIP no

StrictHostKeyChecking no

IdentityFile %d/.ssh/testing\_rsa

Protocol 2

5.启动和查看服务：

service sshd start (或sudo /etc/init.d/ssh start) # 启动sshd

ps -aux | grep sshd #查看是否运行成功