 首先，SSH软件包由两部分组成，一部分是服务器端软件包，另一部分是客户软件包。针对UNIX、Linux系统，这两个软件包是分开打包在两个不同的文件中的。在Windows 9x/NT/2000中，也分为两部分，不同之处在于，服务器软件包只能运行在Windows NT及Windows 2000 Server以上的版本中，而客户端SSH可以运行在所有的Windows系统中。此外，SSH还分为SSH1及SSH2两个版本，SSH1是一个完全免费的软件包，而SSH2在商业使用时则要付费。由其命名也可知SSH1是第一版，它的功能没有SSH2强大，但是，由于它是免费的，所以广泛地使用在很多网站中。SSH2中加入了很多功能，并且兼容SSH1服务器，可以对SSH1的客户端提供很好的服务支持。所以，如果你的系统中安装了SSH2，那就没有必要再安装SSH1软件包了。 UNIX/Linux下SSH2安装步骤 1.下载软件包，下载地址www.ssh.com，下载最新软件包SSH2，最好下载源程序软件包自己进行自行编译。 2.解压及安装： # tar -zxvf ssh2-2.4.0.tar.gz # cd ssh2-2.4.0 # ./configure # make #make install 安装完成。这一过程实际上将服务器软件包及客户端软件一起安装了，不必再次安装客户端软件包。 已编译好的二进制软件包以rpm格式存放在ftp://ftp.ssh.com/pub/ssh/rpm目录下。它是一个给非商业用户使用的软件包，软件包名称为：ssh-2.4.0-1.i386.rpm，其中包含了对X Window的支持，另一个不支持X Window的软件包为ssh- 2.4.0-1nox.i386.rpm，下载

后可以直接安装。安装程序将SSH2软件包安装在/usr/local/bin及 /usr/local/sbin下。 Windows NT上安装SSH 在NT及Windows 2000 Server环境下，可选择的服务器软件有：Vshell 、ssh2-2.4.0.win-server。 Vshell是由Van Dyke提供的一个可以在Windows NT/2000环境下提供SSH2服务器的软件包，其下载地址如下： //www.vandyke.com/download/index.html。另一个运行在Windows环境下的SSH服务器是 SSHWinServer.exe，可以直接从ftp://ftp.ssh.com/pub/ssh目录下下载。 Windows环境下的安装十分简单，本文不再多介绍。 与UNIX不同，在Windows环境下，需要分别安装服务器及客户端软件包。运行在Windows环境下的客户端软件，也可以从以上两个站点下载得到，文件名分别为SecureCRT及SSHWin-2.4.0-pl2。 关于密钥的准备工作 A.服务器端产生用户的自己的加密密钥及对外公开使用的公钥。在UNIX环境下，产生密钥的方法如下： -keygen 要求用户输入一个长的认证字串，这个字串的功能同password相当，但是，它更长，一般是在20个字符以内。再次输入相同的字串以确认输入的正确，之后，系统产生一对密钥及公钥。将公钥复制到本地，以便客户端对服务器发送的信息进行解密用。当然，如果你不复制，在第一次登录时，服务器会将它的公钥自动推给客户机，以便客户机能对服务器提供的信息进行解密识别。 B.客户端产生用户的加密密钥及公钥。客户端产生自己的密钥及公钥的方法与服务器端相同。而Windows环境下的一些支持SSH的客户端软件都采用自己生成的方法，具体情况各不相同，但是可以肯定的是所有的支持SSH的客户端都可以而且必须产生。以sshWin2.4为例说明如下： 打开选单：Edit→Settings→Globe settings

→User keys→Generate New keypairs，按照提示会自动产生新的密钥及公钥对。 最后，将客户机产生的公钥复制到服务端的主机上用户的目录中(在UNIX下应为/home/usrname/.ssh2目录中)。不同的版本的SSH对公钥及密钥的文件名有特定的要求，具体情况请阅读软件包中的安装说明。 启动SSH服务器 在UNIX/Linux环境下，服务器程序放置在/usr/local/sbin目录下，启动方法如下： # sshd # ps x 可以看到SSHD已经启动了。如果不希望每次重启动系统，都要手工运行启动SSHD，则可以自己写一个脚本，放置在init.d目录下，让系统启动后，自动执行SSHD服务的启动工作。或者直接在rc.local中加入一行/usr/local/sbin/sshd也可。 Windows NT/2000/下启动SSH2 Server，运行程序组中的start SSH2 Server即可。 使用SSH 客户端在UNIX/Linux系统中就是SSH，存放在/usr/local/bin目录下。其中有SSH1、SSH2、scp等客户端工具，使用SSH登录远程主机方法如下： host.ip.of.remote 如同使用Telnet一样，不同之处是要求用户输入认证字串，如果认证字串通过了认证，则用户直接登录成功；如果不成功，则是要求用户输入系统口令。口令认证成功后，用户也可以成功登录系统。从使用上看，与Telnet没有什么不同之处。而且有了SSH客户端软件，如果你要上传文件，不必向以前一样再开一个FTP窗口，再次认证，然后上传文件。使用SSH客户端自带的scp工具，就可以直接将文件上传到远端服务器上。使用方法如下： host1:dir/filename host2:/home/abc/filename 在Windows系统中，可供使用的SSH客户端有：SecurCRT，也即CRT的支持SSH的版本(下载地址： //www.vandyke.com/)，这是一个很好的支持SSH的远程终端，它同时支持SSH1及SSH2。用户可以根据

服务器端自由选择，让它支持相应的标准。另一个可供选择的是ssh.com提供的客户端，下载地址：ftp://ftp.ssh.com/pub/ssh/SSHWin-2.4.0-pl2.exe，这是新版本的SSH2客户端。另外，还有支持SSH的FTP客户端工具，其中sshwin-2.4中就有一个SSH Secure File Transfer Client，它可以用来在两个主机之间传输加密后的文件。也即scp的功能。配合SecureCRT的也有一个相应的支持SSH的FTP工具，其名称为：SecureFX，可以从www.vandyke.com/下载使用。由于种种原因，一些支持SSH的GUI客户端不一定会很好地支持以上各个服务器，大家可以自行组合以上工具，找到适合自己的工具。一般来说，在 UNIX下的客户端对各种服务器的支持是最好的。通常在选择服务器及客户端软件时，最好选择同一软件商的产品，这样不会出现不兼容的问题。需要补充的是，如果你既想使用SSH2又不想付费，那么一个可供选择的自由软件是Openssh，它是一个遵守GPL协议的软件包，同时支持 SSH1 及SSH2标准，是另一个被广泛使用的SSH软件包(可以从www.openssh.com下载)。Openssh的最新版本为Openssh- 2.5.1，提供全部源码。不过，在编译前，应仔细阅读其说明文件。编译过程中要用到zlib及openssl两个软件包，用户首先需要下载并安装它们，之后再编译openssh。具体过程请阅读软件包中的install文件。