目 录

1 SSH

1.1 SSH简介

SSH 是 Secure Shell（安全外壳）的简称，是一种在不安全的网络环境中，通过加密机制和认证机制，实现安全的远程访问以及文件传输等业务的网络安全协议。

SSH 协议采用了典型的客户端/服务器模式，并基于 TCP 协议协商建立用于保护数据传输的会话通道。设备既可以支持 SSH 服务器功能，接受多个 SSH 客户端的连接，也可以支持 SSH 客户端功能，允许用户通过设备与远程 SSH 服务器建立 SSH 连接。

目前，设备支持三种 SSH 应用：Stelnet、SFTP 和 SCP。

- Stelnet 是 Secure Telnet 的简称，可提供安全可靠的网络终端访问服务，使得用户可以安全登录到远程设备，且能保护远程设备不受诸如 IP 地址欺诈、明文密码截取等攻击。设备可支持 Stelnet 服务器、Stelnet 客户端功能。
- SFTP 是 Secure FTP 的简称，基于 SSH2，可提供安全可靠的网络文件传输服务，使得用户可以安全登录到远程设备上进行文件管理操作，且能保证文件传输的安全性。设备可支持 SFTP 服务器、SFTP 客户端功能。
- SCP 是 Secure Copy 的简称，基于 SSH2，可提供安全的文件复制功能。设备可支持 SCP 服务器、SCP 客户端功能。

SSH 协议有两个版本，SSH1 和 SSH2，两者互不兼容，SSH2 在性能和安全性方面比 SSH1 有所提高。

说明

目前，设备作为 SSH 服务器时，在非 FIPS 模式下支持 SSH2 和 SSH1 两个版本，在 FIPS 模式下只支持 SSH2 版本；设备作为 SSH 客户端时，只支持 SSH2 版本。

1.1.1 SSH工作过程

说明

本小节以 SSH2 为例介绍 SSH 工作的过程。

SSH服务器端与SSH客户端需要经历表 1-1所述的几个阶段的交互，才能实现SSH的安全连接，关于各阶段的详细介绍，请参见“SSH技术白皮书”。

表1-1 SSH 服务器端与客户端建立连接的几个阶段

阶段	说明
连接建立	SSH服务器在22号端口侦听客户端的连接请求，在客户端向服务器端发起连接请求后，双方建立一个TCP连接

阶段	说明
版本协商	双方通过版本协商确定最终使用的SSH版本号
算法协商	SSH支持多种算法，双方根据本端和对端支持的算法，协商出最终用于产生会话密钥的密钥交换算法、用于数据信息加密的加密算法、用于进行数字签名和认证的公钥算法，以及用于数据完整性保护的HMAC算法
密钥交换	双方通过DH（Diffie-Hellman Exchange）交换，动态地生成用于保护数据传输的会话密钥和用来标识该SSH连接的会话ID，并完成客户端对服务器端的身份认证
用户认证	SSH客户端向服务器端发起认证请求，服务器端对客户端进行认证
会话请求	认证通过后，SSH客户端向服务器端发送会话请求，请求服务器提供某种类型的服务（目前支持Stelnet、SFTP和SCP），即请求与服务器建立相应的会话
会话交互	会话建立后，SSH服务器端和客户端在该会话上进行数据信息的交互

说明

- 交互会话阶段，用户在客户端可以通过粘贴文本会话的方式执行命令，但文本会话不能超过 2000 字节，且粘贴的命令最好是同一视图下的命令，否则服务器可能无法正确执行该命令。
- 如果粘贴的文本会话超过 2000 字节，可以采用将配置文件通过 SFTP（Secure FTP，安全的 FTP）方式上传到服务器，利用新的配置文件重新启动的方式执行这些命令。

1.1.2 SSH认证方式

设备作为 SSH 服务器可提供以下四种对客户端的认证方式：

1. password认证

利用 AAA（Authentication、Authorization、Accounting，认证、授权和计费）对客户端身份进行认证。客户端向服务器发出 password 认证请求，将用户名和密码加密后发送给服务器；服务器将认证请求解密后得到用户名和密码的明文，通过本地认证或远程认证验证用户名和密码的合法性，并返回认证成功或失败的消息。

2. publickey认证

采用数字签名的方式来认证客户端。目前，设备上可以利用 DSA 和 RSA 两种公钥算法实现数字签名。客户端发送包含用户名、公钥和公钥算法（或者为携带公钥信息的数字证书）的 publickey 认证请求给服务器端。服务器对公钥进行合法性检查，如果不合法，则直接发送失败消息；否则，服务器利用数字签名对客户端进行认证，并返回认证成功或失败的消息。

该认证方式下，设备支持客户端采用不同的方式进行认证：

- 公钥认证：客户端直接提供用户的公钥信息给服务器，服务器对用户公钥进行合法性检查。
- 证书认证：客户端通过数字证书向服务器提供用户的公钥信息，服务器对用户数字证书进行合法性检查。目前，设备作为客户端不支持此类认证。

3. password-publickey认证

对于 SSH2 版本的客户端，要求同时进行 password 和 publickey 两种方式的认证，且只有两种认证均通过的情况下，才认为客户端身份认证通过；对于 SSH1 版本的客户端，只要通过其中任意一种认证即可。

4. any认证

不指定客户端的认证方式，客户端可采用 password 认证或 publickey 认证，且只要通过其中任何一种认证即可。

说明

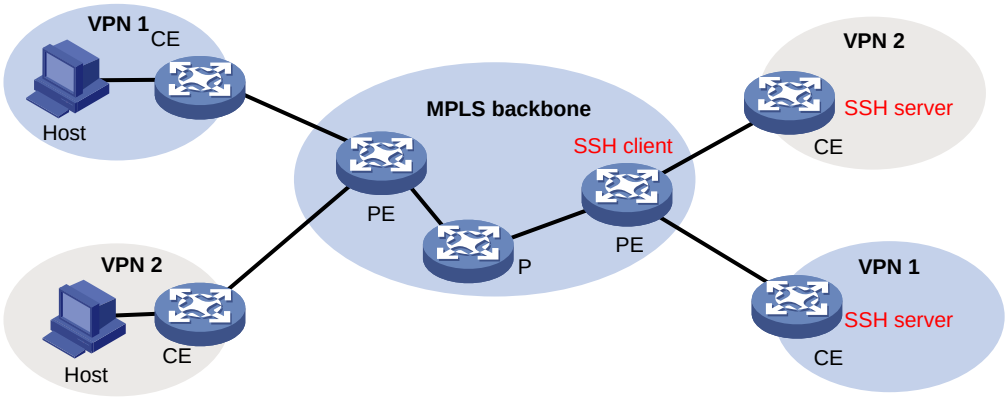
- 为便于描述，下文中提到的 publickey/password 认证方式是指涉及该认证方式的所有认证方式（publickey/password、password-publickey 和 any）。
- 客户端进行 password 认证时，如果远程认证服务器要求用户进行二次密码认证，则会在发送给服务器端的认证回应消息中携带一个提示信息，该提示信息被服务器端透传给客户端，由客户端输出并要求用户再次输入一个指定类型的密码，当用户提交正确的密码并成功通过认证服务器的验证后，服务器端才会返回认证成功的消息。
- SSH1 版本的 SSH 客户端不支持 AAA 服务器发起的二次密码认证。

1.1.3 SSH支持MPLS L3VPN

设备作为 SSH 客户端时，通过支持 MPLS L3VPN 功能，可以与位于 MPLS L3VPN 中的 SSH 服务器建立 SSH 连接。

如图 1-1所示，私网VPN 1 和VPN 2 中的用户通过PE接入MPLS骨干网，各VPN之间的业务相互隔离。在PE设备上开启SSH客户端功能后，通过MPLS L3VPN功能和SSH连接支持MPLS L3VPN功能，可以对各VPN中使能SSH服务器功能的CE设备进行访问，实现从PE设备到CE设备的安全登录和日志文件传输等功能。

图1-1 SSH 支持 VPN 多实例组网应用图



1.2 配置SSH服务器

1.2.1 SSH服务器配置任务简介

通过执行以下配置任务，可配置设备作为 Stelnet、SFTP 或 SCP 服务器。由于 Stelnet、SFTP 和 SCP 服务器功能的配置基本相同，因此除非特殊说明，本小节中使用 SSH 服务器作为 Stelnet、SFTP 和 SCP 服务器的统称。

表1-2 SSH 服务器配置任务简介

配置任务	说明	详细配置
生成本地DSA或RSA密钥	必选	1.2.2
使能SSH服务器功能	对于Stelnet、SFTP和SCP服务器均必选	1.2.3
使能SFTP服务器功能	仅对于SFTP服务器必选	1.2.4
配置SSH客户端登录时的用户界面	必选	1.2.5
配置客户端的公钥	采用publickey认证方式且客户端使用公钥认证时必选	1.2.6
配置认证客户端证书的PKI域	采用publickey认证方式且客户端使用证书认证时必选 该PKI域中必须保存了用于认证客户端证书的CA证书	请参见“安全配置指导”中的“PKI配置”
配置SSH用户	采用publickey认证方式时必选 其它情况下可选	1.2.7
配置SSH管理功能	可选	1.2.8

1.2.2 生成本地DSA或RSA密钥对

服务器端的 DSA 或 RSA 密钥对有两个用途，其一是用于在密钥交换阶段生成会话密钥和会话 ID，另外一个是客户端用它来对连接的服务器进行认证。客户端验证服务器身份时，首先判断服务器发送的公钥与本地保存的服务器公钥是否一致，确认服务器公钥正确后，再对服务器发送的该公钥计算出的数字签名进行验证。

虽然一个客户端只会采用 DSA 和 RSA 公钥算法中的一种来认证服务器，但是由于不同客户端支持的公钥算法不同，为了确保客户端能够成功登录服务器，建议在服务器上同时生成 DSA 和 RSA 两种密钥对。

表1-3 生成本地 DSA 或 RSA 密钥对

操作	命令	说明
进入系统视图	**system-view**	-
生成本地DSA或RSA密钥对	**public-key local create { dsa | rsa }**	必选 缺省情况下，不存在任何DSA和RSA密钥对

说明

- **public-key local create** 命令的详细介绍请参见“安全命令参考”中的“公钥管理”。
- 通过 **public-key local create rsa** 命令生成 RSA 密钥对时，将同时生成两个密钥对——服务器密钥对和主机密钥对，二者都包括一个公钥和一个私钥。SSH1 中利用 SSH 服务器端的服务器公钥加密会话密钥，以保证会话密钥传输的安全；SSH2 中通过 DH 算法在 SSH 服务器和 SSH 客户端上生成会话密钥，不需要传输会话密钥，因此 SSH2 中没有利用服务器密钥对。
- 通过 **public-key local create dsa** 命令生成 DSA 密钥对时，只生成一个主机密钥对。
- SSH1 中不支持 DSA 算法。
- 在 FIPS 模式下，设备不支持 DSA 算法。

1.2.3 使能SSH服务器功能

该配置任务用于使能设备上的 SSH 服务器功能，使客户端能用 SSH 协议与服务器进行通信。

表1-4 使能 SSH 服务器功能

操作	命令	说明
进入系统视图	**system-view**	-
使能SSH服务器功能	**ssh server enable**	必选 缺省情况下，SSH服务器功能处于关闭状态

说明

设备作为 SCP 服务器时，同一时间只允许有一个 SCP 用户访问 SCP 服务器。

1.2.4 使能SFTP服务器功能

该配置任务用于使能设备上的 SFTP 服务器功能，使客户端能用 SFTP 的方式登录到服务器。

表1-5 启动 SFTP 服务器功能

操作	命令	说明
进入系统视图	**system-view**	-
使能SFTP服务器功能	**sftp server enable**	必选 缺省情况下，SFTP服务器处于关闭状态

说明

设备作为 SFTP 服务器时，同一时间只允许有一个用户访问 SFTP 服务器。

1.2.5 配置SSH客户端登录时使用的用户界面

SSH 客户端通过 VTY 用户界面访问设备。因此，需要配置 SSH 客户端登录时采用的 VTY 用户界面，使其支持 SSH 远程登录协议。配置将在客户端下次登录时生效。

表1-6 配置 SSH 客户端登录时使用的用户界面

操作	命令	说明
进入系统视图	**system-view**	-
进入VTY用户界面视图	**user-interface vty** *number* [*ending-number*]	-
配置登录用户界面的认证方式为**scheme**方式	**authentication-mode scheme**	必选 缺省情况下，用户界面认证为**password**方式
配置所在用户界面支持SSH协议	**protocol inbound** { **all** | **ssh** | **telnet** }	可选 缺省情况下，系统同时支持Telnet和SSH协议

说明

- **authentication-mode** 和 **protocol inbound** 命令的详细介绍，请参见“基础配置命令参考”中的“登录设备”。
- 配置用户界面支持 SSH 协议之前，必须首先配置登录用户界面的认证方式为 **scheme** 方式，否则 **protocol inbound** 命令会执行失败。

1.2.6 配置客户端的公钥

说明

本配置仅适用于 publickey 认证方式且客户端使用公钥认证的情况。

服务器在采用公钥验证客户端身份时，首先比较客户端发送的 SSH 用户名、主机公钥是否与本地配置的 SSH 用户名以及相应的客户端主机公钥一致，在确认用户名和客户端主机公钥正确后，对客户端发送的数字签名进行验证，该签名是客户端利用主机公钥对应的私钥计算出的。因此，需要在服务器端配置客户端的 DSA 或 RSA 主机公钥，并在客户端为该 SSH 用户指定与主机公钥对应的 DSA 或 RSA 主机私钥(若设备作为客户端，则在向服务器发起连接时通过指定公钥算法来实现)。

服务器端可以通过手工配置和从公钥文件中导入两种方式来配置客户端的公钥：

- 手工配置：事先在客户端上查看并记录客户端主机公钥的内容，然后采用手工输入的方式将客户端的公钥配置到服务器上。手工输入远端主机公钥时，可以逐个字符输入，也可以一次拷贝粘贴多个字符。这种方式要求手工输入或拷贝粘贴的主机公钥必须是未经转换的 DER（Distinguished Encoding Rules，特异编码规则）公钥编码格式。
- 从公钥文件中导入：事先将客户端的公钥文件保存到服务器上（例如，通过 FTP 或 TFTP，以二进制方式将客户端的公钥文件保存到服务器），服务器从本地保存的该公钥文件中导入客户端的公钥。导入公钥时，系统会自动将客户端公钥文件转换为 PKCS（Public Key Cryptography Standards，公共密钥加密标准）编码形式。

说明

- 手工配置客户端的公钥时，输入的主机公钥必须满足一定的格式要求。在设备作为客户端情况下，通过 **display public-key local public** 命令显示的公钥可以作为输入的公钥内容。通过其他方式查看到的公钥可能不满足格式要求，导致主机公钥保存失败。因此，建议选用从公钥文件导入的方式配置远端主机的公钥。
- SSH 服务器上最多可以配置 20 个 SSH 客户端的公钥。

表1-7 手工配置客户端的公钥

操作	命令	说明
进入系统视图	**system-view**	-
进入公钥视图	**public-key peer** *keyname*	-
进入公钥编辑视图	**public-key-code begin**	-
配置客户端的公钥	直接输入公钥内容	必选 在输入公钥内容时，字符之间可以有空格，也可以按回车键继续输入数据
退回公钥视图，并保存配置的主机公钥	**public-key-code end**	必选 退出公钥编辑视图时，系统自动保存配置的公钥密钥
退回系统视图	**peer-public-key end**	-

表1-8 从公钥文件中导入客户端的公钥

操作	命令	说明
进入系统视图	**system-view**	-
从公钥文件中导入SSH用户的公钥	**public-key peer** *keyname* **import sshkey** *filename*	必选

说明

关于客户端的公钥的配置介绍，请参见“安全配置指导”中的“公钥管理”。

1.2.7 配置SSH用户

说明

- 如果服务器采用 publickey 方式认证客户端，则必须通过本配置在设备上创建相应的 SSH 用户。
- 如果服务器采用 password 方式认证客户端，则必须将 SSH 用户的账号信息配置在设备（适用于本地认证）或者远程认证服务器（如 RADIUS 服务器，适用于远程认证）上，而并不要求通过本配置创建相应的 SSH 用户。如果通过本配置创建了相应的 SSH 用户，则必须保证指定正确的服务类型以及认证方式。关于本地及远程认证的相关配置请参见“安全配置指导”中的“AAA”。

本配置用于创建 SSH 用户，并指定 SSH 用户的服务类型、认证方式以及客户端的公钥或数字证书。除 password 认证方式外，其它认证方式下均需要指定客户端的公钥或证书。

- 对于使用公钥认证的SSH用户，服务器端必须指定客户端的公钥，且指定的公钥必须已经存在，公钥内容的配置请参见“1.2.6 配置客户端的公钥”。
- 对于使用证书认证的 SSH 用户，服务器端必须指定用于验证客户端证书的 PKI 域，PKI 域的配置请参见“安全配置指导”中的“PKI 域配置”。为保证合法的 SSH 用户可以成功通过认证，通过本命令指定的 PKI 域中必须存在用于验证其证书的 CA 证书。

表1-9 配置 SSH 用户

操作		命令	说明
进入系统视图		**system-view**	-
配置SSH用户	SSH用户的服务类型为**stelnet**	**ssh user** *username* **service-type stelnet authentication-type** { **password** | { **any** | **password-publickey** | **publickey** } **assign** { **pki-domain** *pkiname* | **publickey** *keyname* } }	根据服务类型选择其一
	SSH用户的服务类型为**all**、**scp**或**sftp**	**ssh user** *username* **service-type** { **all** | **scp** | **sftp** } **authentication-type** { **password** | { **any** | **password-publickey** | **publickey** } **assign** { **pki-domain** *pkiname* | **publickey** *keyname* } **work-directory** *directory-name* }	

说明

- SSH 服务器上最多可以创建 1024 个 SSH 用户。
- SSH1 不支持服务类型 **sftp** 和 **scp**，因此设备不支持 SSH1 版本的客户端发起的 SFTP 连接或 SCP 连接。
- SFTP 用户登录时使用的工作目录与用户使用的认证方式有关。只要是采用 publickey 认证方式的用户，使用的工作目录均为通过 **ssh user** 命令为该用户设置的工作目录；仅采用 password 认证方式的用户，使用的工作目录为通过 AAA 授权的工作目录。
- 只要是使用 publickey 认证方式的用户登录服务器后，可以访问的命令级别均为在用户界面上通过 **user privilege level** 命令配置的级别。
- 仅使用 password 认证方式的用户登录服务器后，用户可以访问的命令级别由 AAA 来授权。
- 对 SSH 用户配置的修改，对于已经登录的 SSH 用户不会生效，只在 SSH 用户下次登录时生效。

1.2.8 配置SSH管理功能

通过配置服务器上的 SSH 管理功能，可提高 SSH 连接的安全性。SSH 的管理功能包括：

- 设置 SSH 服务器是否兼容 SSH1 版本的客户端
- 设置 RSA 服务器密钥对的更新时间，此配置仅对 SSH 客户端版本为 SSH1 的用户有效，SSH 的核心是密钥的协商和传输，因此密钥的管理是非常重要的，可灵活设置更新时间间隔。
- 设置 SSH 用户认证的超时时间。为了防止不法用户建立起 TCP 连接后，不进行接下来的认证，而是空占着进程，妨碍其它合法用户的正常登录，可以设置验证超时时间，如果在规定的时间内没有完成认证就拒绝该连接。
- 设置 SSH 用户请求连接的认证尝试最大次数，限制登录的重试次数，防止非法用户对用户名和密码进行恶意地猜测和破解。
- 设置 SFTP 用户连接的空闲超时时间。当 SFTP 用户连接的空闲时间超过设定的阈值后，系统会自动断开此用户的连接，从而有效避免用户长期占用连接而不进行任何操作。

表1-10 配置 SSH 管理功能

操作	命令	说明
进入系统视图	**system-view**	-
设置SSH服务器兼容SSH1版本的客户端	**ssh server compatible-ssh1x enable**	可选 缺省情况下，SSH服务器兼容SSH1版本的客户端
设置RSA服务器密钥对的更新时间	**ssh server rekey-interval** *hours*	可选 缺省情况下，系统不更新RSA服务器密钥对
设置SSH用户的认证超时时间	**ssh server authentication-timeout** *time-out-value*	可选 缺省情况下，SSH用户的认证超时时间为60秒

操作	命令	说明
设置SSH认证尝试的最大次数	**ssh server authentication-retries** *times*	可选 缺省情况下，SSH连接认证尝试的最大次数为3次
设置SFTP用户连接的空闲超时时间	**sftp server idle-timeout** *time-out-value*	可选 缺省情况下，SFTP用户连接的空闲超时时间为10分钟

说明

SSH 客户端通过 publickey 和 password 两种方式进行认证尝试的次数总和，不能超过 **ssh server authentication-retries** 命令配置的 SSH 连接认证尝试次数。

1.3 配置Stelnet客户端

1.3.1 Stelnet客户端配置任务简介

表1-11 SSH 客户端配置任务简介

配置任务	说明	详细配置
为Stelnet客户端指定源IP地址或源接口	可选	1.3.2
配置SSH客户端是否支持首次认证	可选	1.3.3
建立与Stelnet服务器端的连接	必选	1.3.4

1.3.2 为Stelnet客户端指定源IP地址或源接口

Stelnet 客户端与 Stelnet 服务器通信时，缺省采用路由决定的源 IP 地址作为发送报文的源地址。如果使用本配置指定了源 IP 地址或源接口，则采用该地址与服务器进行通信。为保证 Stelnet 客户端与 Stelnet 服务器通信链路的可达性，以及增加认证业务对 SFTP 客户端的可管理性，通常建议指定 Loopback 接口作为源接口。

表1-12 为 Stelnet 客户端指定源 IP 地址或源接口

操作		命令	说明
进入系统视图		**system-view**	-
为Stelnet客户端指定源IP地址或源接口	为Stelnet客户端指定源IPv4地址或源接口	**ssh client source** { **interface** *interface-type interface-number* | **ip** *ip-address* }	二者必选其一 缺省情况下，客户端用设备路由指定的接口地址访问Stelnet服务器
	为Stelnet客户端指定源IPv6地址或源接口	**ssh client ipv6 source** { **interface** *interface-type interface-number* | **ipv6** *ipv6-address* }	

1.3.3 配置SSH客户端是否支持首次认证

设备作为 SSH 客户端和服务器端连接时，将根据是否支持首次认证决定，在本地没有配置服务器端的主机公钥时，是否仍然信任服务器并继续访问该服务器：

- 如果支持首次认证，则当 SSH 客户端首次访问服务器，而客户端没有配置服务器端的主机公钥时，用户可以选择继续访问该服务器，并在客户端保存该主机公钥；当用户下次访问该服务器时，就以保存的主机公钥来认证该服务器。首次认证在比较安全的网络环境中可以简化客户端的配置，但由于该方式下客户端完全相信服务器公钥的正确性，因此存在一定的安全隐患。
- 如果不支持首次认证，则当客户端没有配置服务器端的主机公钥时，客户端将拒绝访问该服务器。用户必须事先将要访问的服务器端的主机公钥配置在本地，同时指定要连接的服务器端的主机公钥名称，以便客户端对连接的服务器进行认证。

1. 配置SSH客户端支持首次认证

表1-13 配置 SSH 客户端支持首次认证

操作	命令	说明
进入系统视图	**system-view**	-
设置SSH客户端支持首次认证	**ssh client first-time enable**	可选 缺省情况下，客户端支持首次认证

2. 配置SSH客户端不支持首次认证

如果配置 SSH 客户端不支持首次认证，则需要在客户端配置服务器端的主机公钥，并为要连接的服务器指定主机公钥名称。

表1-14 配置 SSH 客户端不支持首次认证

操作	命令	说明
进入系统视图	**system-view**	-
设置SSH客户端不支持首次认证	**undo ssh client first-time**	必选 缺省情况下，客户端支持首次认证
配置服务器端的主机公钥	请参见“1.2.6 配置客户端的公钥”	必选 在客户端配置服务器端主机公钥的方法，与在服务器端配置客户端公钥的方法相同
在客户端上指定要连接的服务器端的主机公钥名称	**ssh client authentication server** *server* **assign publickey** *keyname*	必选

1.3.4 建立与Stelnet服务器的连接

该配置任务用来启动 Stelnet 客户端程序，与远程 Stelnet 服务器建立连接，并指定公钥算法、首选加密算法、首选 HMAC 算法和首选密钥交换算法。

表1-15 建立与 Stelnet 服务器的连接

操作		命令	说明
与Stelnet服务器端建立连接	与IPv4 Stelnet服务器端建立连接	• 在非 FIPS 模式下： **ssh2** *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] [**identity-key** { **dsa** | **rsa** } | **prefer-compress** { **zlib** | **zlib-openssh** } | **prefer-ctos-cipher** { **3des** | **aes128** | **des** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** } | **prefer-kex** { **dh-group-exchange** | **dh-group1** | **dh-group14** } | **prefer-stoc-cipher** { **3des** | **aes128** | **des** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** }] * • 在 FIPS 模式下： **ssh2** *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] [**identity-key rsa** | **prefer-ctos-cipher** { **aes128** | **aes256** } | **prefer-ctos-hmac** { **sha1** | **sha1-96** } | **prefer-kex dh-group14** | **prefer-stoc-cipher** { **aes128** | **aes256** } | **prefer-stoc-hmac** { **sha1** | **sha1-96** }] *	二者必选其一 请在用户视图下执行本命令
	与IPv6 Stelnet服务器端建立连接	• 在非 FIPS 模式下： **ssh2 ipv6** *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] [**identity-key** { **dsa** | **rsa** } | **prefer-compress** { **zlib** | **zlib-openssh** } | **prefer-ctos-cipher** { **3des** | **aes128** | **des** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** } | **prefer-kex** { **dh-group-exchange** | **dh-group1** | **dh-group14** } | **prefer-stoc-cipher** { **3des** | **aes128** | **des** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** }] * • 在 FIPS 模式下： **ssh2 ipv6** *server* [*port-number*] [**identity-key rsa** | **prefer-ctos-cipher** { **aes128** | **aes256** } | **prefer-ctos-hmac** { **sha1** | **sha1-96** } | **prefer-kex dh-group14** | **prefer-stoc-cipher** { **aes128** | **aes256** } | **prefer-stoc-hmac** { **sha1** | **sha1-96** }] *	

1.4 配置SFTP客户端

1.4.1 SFTP客户端配置任务简介

表1-16 SFTP 客户端配置任务简介

配置任务	说明	详细配置
为SFTP客户端指定源IP地址或源接口	可选	1.4.2
配置SSH客户端是否支持首次认证	可选	1.3.3
建立与SFTP服务器端的连接	必选	1.4.3
SFTP目录操作	可选	1.4.4
SFTP文件操作	可选	1.4.5
显示帮助信息	可选	1.4.6
中止与SFTP服务器端的连接	可选	1.4.7

1.4.2 为SFTP客户端指定源IP地址或源接口

SFTP 客户端与 SFTP 服务器通信时，缺省采用路由决定的源 IP 地址作为发送报文的源地址。如果使用本配置指定了源 IP 地址或源接口，则采用该地址与服务器进行通信。为保证 SFTP 客户端与 SFTP 服务器通信链路的可达性，以及增加认证业务对 SFTP 客户端的可管理性，通常建议指定 Loopback 接口作为源接口。

表1-17 为 SFTP 客户端指定 IP 地址或源接口

操作		命令	说明
进入系统视图		**system-view**	-
为SFTP客户端指定源IP地址或源接口	为SFTP客户端指定源IPv4地址或源接口	**sftp client source** { **interface** *interface-type interface-number* | **ip** *ip-address* }	二者必选其一 缺省情况下，客户端用设备路由指定的接口地址访问SFTP服务器
	为SFTP客户端指定源IPv6地址或源接口	**sftp client ipv6 source** { **interface** *interface-type interface-number* | **ipv6** *ipv6-address* }	

1.4.3 建立与SFTP服务器的连接

该配置任务用来启动 SFTP 客户端程序，与远程 SFTP 服务器建立连接，并指定公钥算法、首选加密算法、首选 HMAC 算法和首选密钥交换算法。SFTP 客户端与服务器成功建立连接之后，用户即可进入到服务器端上的 SFTP 客户端视图下进行目录、文件等操作。

表1-18 建立与 SFTP 服务器端的连接

操作		命令	说明
与SFTP服务器建立连接，并进入SFTP客户端视图	与IPv4 SFTP服务器建立连接，并进入SFTP客户端视图	• 在非 FIPS 模式下： **sftp** *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] [**identity-key** { **dsa** | **rsa** } | **prefer-compress** { **zlib** | **zlib-openssh** } | **prefer-ctos-cipher** { **3des** | **aes128** | **des** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** } | **prefer-kex** { **dh-group-exchange** | **dh-group1** | **dh-group14** } | **prefer-stoc-cipher** { **3des** | **aes128** | **des** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** }] * • 在 FIPS 模式下： **sftp** *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] [**identity-key rsa** | **prefer-ctos-cipher** { **aes128** | **aes256** } | **prefer-ctos-hmac** { **sha1** | **sha1-96** } | **prefer-kex dh-group14** | **prefer-stoc-cipher** { **aes128** | **aes256** } | **prefer-stoc-hmac** { **sha1** | **sha1-96** }] *	二者必选其一 请在用户视图下执行此命令
	与IPv6 SFTP服务器建立连接，并进入SFTP客户端视图	• 在非 FIPS 模式下： **sftp ipv6** *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] [**identity-key** { **dsa** | **rsa** } | **prefer-compress** { **zlib** | **zlib-openssh** } | **prefer-ctos-cipher** { **3des** | **aes128** | **des** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** } | **prefer-kex** { **dh-group-exchange** | **dh-group1** | **dh-group14** } | **prefer-stoc-cipher** { **3des** | **aes128** | **des** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** }] * • 在 FIPS 模式下： **sftp ipv6** *server* [*port-number*] [**identity-key rsa** | **prefer-ctos-cipher** { **aes128** | **aes256** } | **prefer-ctos-hmac** { **sha1** | **sha1-96** } | **prefer-kex dh-group14** | **prefer-stoc-cipher** { **aes128** | **aes256** } | **prefer-stoc-hmac** { **sha1** | **sha1-96** }] *	

1.4.4 SFTP目录操作

SFTP 目录操作包括：改变或显示当前的工作路径、显示指定目录下的文件或目录信息、改变服务器上指定的文件夹的名字、创建或删除目录等操作。

表1-19 SFTP 目录操作

操作	命令	说明
进入SFTP客户端视图	具体命令请参考1.4.3	-
改变远程SFTP服务器上的工作路径	**cd** [*remote-path*]	可选
返回到上一级目录	**cdup**	可选
显示远程SFTP服务器上的当前工作目录	**pwd**	可选
显示指定目录下的文件列表	**dir** [**-a** | **-l**] [*remote-path*]	可选

操作	命令	说明
	ls [**-a** | **-l**] [*remote-path*]	**dir**和**ls**两条命令的作用相同
改变SFTP服务器上指定的目录的名字	**rename** *oldname newname*	可选
在远程SFTP服务器上创建新的目录	**mkdir** *remote-path*	可选
删除SFTP服务器上指定的目录	**rmdir** *remote-path*&<1-10>	可选

1.4.5 SFTP文件操作

SFTP 文件操作包括：改变文件名、下载文件、上传文件、显示文件列表、删除文件。

表1-20 SFTP 文件操作

操作	命令	说明
进入SFTP客户端视图	具体命令请参考1.4.3	-
改变SFTP服务器上指定的文件的名字	**rename** *old-name new-name*	可选
从远程服务器上下载文件并存储在本地	**get** *remote-file* [*local-file*]	可选
将本地的文件上传到远程SFTP服务器	**put** *local-file* [*remote-file*]	可选
显示指定目录下的文件	**dir** [**-a** | **-l**] [*remote-path*]	可选 **dir**和**ls**两条命令的作用相同
	ls [**-a** | **-l**] [*remote-path*]	
删除SFTP服务器上指定的文件	**delete** *remote-file*&<1-10>	可选 **delete**和**remove**两条命令的功能相同
	remove *remote-file*&<1-10>	

1.4.6 显示帮助信息

本配置用于显示命令的帮助信息，如命令格式、参数配置等。

表1-21 显示客户端命令的帮助信息

操作	命令	说明
进入SFTP客户端视图	具体命令请参考1.4.3	-
显示SFTP客户端命令的帮助信息	**help** [**all** | *command-name*]	必选

1.4.7 终止与SFTP服务器的连接

表1-22 终止与 SFTP 服务器的连接

操作	命令	说明
进入SFTP客户端视图	具体命令请参考1.4.3	-
终止与SFTP服务器的连接，并退回用户视图	**bye**	三者必选其一 **bye**，**exit**和**quit**三条命令的功能相同
	exit	
	quit	

1.5 配置SCP客户端

1.5.1 SCP客户端配置任务简介

表1-23 SCP 客户端配置任务简介

配置任务	说明	详细配置
配置SSH客户端是否支持首次认证	可选	1.3.3
与远程SCP服务器传输文件	必选	1.5.2

1.5.2 与远程SCP服务器传输文件

该配置任务用来启动 SCP 客户端程序，与远程 SCP 服务器建立连接，并进行安全的文件传输操作。

表1-24 与远程 SCP 服务器传输文件

操作		命令	说明
与远程SCP服务器建立连接，并进行文件传输	向远程SCP服务器上传文件	非FIPS模式下： **scp** [**ipv6**] *server* [*port-number*] **put** *source-file-path* [*destination-file-path*] [**identity-key** { **dsa** | **rsa** } | **prefer-compress** { **zlib** | **zlib-openssh** } | **prefer-ctos-cipher** { **3des** | **aes128** | **des** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** } | **prefer-kex** { **dh-group-exchange** | **dh-group1** | **dh-group14** } | **prefer-stoc-cipher** { **3des** | **aes128** | **des** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** }] * FIPS模式下： **scp** [**ipv6**] *server* [*port-number*] **put** *source-file-path* [*destination-file-path*] [**identity-key rsa** | **prefer-compress** { **zlib** | **zlib-openssh** } | **prefer-ctos-cipher** { **aes128** | **aes256** } | **prefer-ctos-hmac** { **sha1** | **sha1-96** } | **prefer-kex dh-group14** | **prefer-stoc-cipher** { **aes128** | **aes256** } | **prefer-stoc-hmac** { **sha1** | **sha1-96** }] *	二者必选其一

操作		命令	说明
	从远程SCP服务器下载文件	非FIPS模式下： **scp** [**ipv6**] *server* [*port-number*] **get** *source-file-path* [*destination-file-path*] [**identity-key** { **dsa** | **rsa** } | **prefer-compress** { **zlib** | **zlib-openssh** } | **prefer-ctos-cipher** { **3des** | **aes128** | **des** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** } | **prefer-kex** { **dh-group-exchange** | **dh-group1** | **dh-group14** } | **prefer-stoc-cipher** { **3des** | **aes128** | **des** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** }] * FIPS模式下： **scp** [**ipv6**] *server* [*port-number*] **get** *source-file-path* [*destination-file-path*] [**identity-key rsa** | **prefer-compress** { **zlib** | **zlib-openssh** } | **prefer-ctos-cipher** { **aes128** | **aes256** } | **prefer-ctos-hmac** { **sha1** | **sha1-96** } | **prefer-kex dh-group14** | **prefer-stoc-cipher** { **aes128** | **aes256** } | **prefer-stoc-hmac** { **sha1** | **sha1-96** }] *	

1.6 SSH显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令，可以显示配置后 SSH 的运行情况，通过查看显示信息验证配置的效果。

表1-25 SSH 显示和维护

操作	命令
显示当前为SFTP客户端设置的源IP地址或者源接口	**display sftp client source** [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示当前为Stelnet客户端设置的源IP地址或者源接口	**display ssh client source** [**|** { **begin** | **exclude** | **include** } *regular-expression*]
在SSH服务器端显示该服务器的状态信息或会话信息	**display ssh server** { **status** | **session** } [**|** { **begin** | **exclude** | **include** } *regular-expression*]
在SSH客户端显示客户端保存的服务器端的主机公钥和服务器的对应关系	**display ssh server-info** [**|** { **begin** | **exclude** | **include** } *regular-expression*]
在SSH服务器端显示SSH用户信息	**display ssh user-information** [*username*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示本地密钥对中的公钥部分	**display public-key local** { **dsa** | **rsa** } **public** [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示保存在本地的远端主机的公钥信息	**display public-key peer** [**brief** | **name** *publickey-name*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

说明

display public-key local 和 **display public-key peer** 命令的详细介绍请参见“安全命令参考”中的“公钥管理”。

1.7 Stelnet典型配置举例

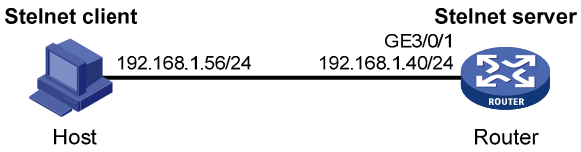
1.7.1 设备作为Stelnet服务器配置举例（password认证）

1. 组网需求

- 用户可以通过 Host 上运行的 Stelnet 客户端软件（SSH2 版本）安全地登录到 Router 上进行配置管理；
- Router 采用 password 认证方式对 Stelnet 客户端进行认证，客户端的用户名和密码保存在本地。

2. 组网图

图1-2 设备作为 Stelnet 服务器配置组网图



3. 配置步骤

(1) 配置 Stelnet 服务器

生成 RSA 密钥对。

```
<Router> system-view
[Router] public-key local create rsa
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
It will take a few minutes.
Press CTRL+C to abort.
Input the bits of the modulus[default = 1024]:
Generating Keys...
++++++++++++++++++++++++
++++++++++++++++++++++++
+++++
+++++
```

生成 DSA 密钥对。

```
[Router] public-key local create dsa
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
It will take a few minutes.
Press CTRL+C to abort.
```

```
Input the bits of the modulus[default = 1024]:
Generating Keys...
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
++++++++++++++++++++++++++++++++
```

使能 SSH 服务器功能。

```
[Router] ssh server enable
```

配置接口 GigabitEthernet3/0/1 的 IP 地址，客户端将通过该地址连接 Stelnet 服务器。

```
[Router] interface gigabitethernet 3/0/1
[Router-GigabitEthernet3/0/1] ip address 192.168.1.40 255.255.255.0
[Router-GigabitEthernet3/0/1] quit
```

设置 Stelnet 客户端登录用户界面的认证方式为 AAA 认证。

```
[Router] user-interface vty 0 4
[Router-ui-vty0-4] authentication-mode scheme
```

设置 Router 上远程用户登录协议为 SSH。

```
[Router-ui-vty0-4] protocol inbound ssh
[Router-ui-vty0-4] quit
```

创建本地用户 client001，密码为 aabbcc，服务类型为 SSH。

```
[Router] local-user client001
[Router-luser-client001] password simple aabbcc
[Router-luser-client001] service-type ssh
[Router-luser-client001] quit
```

配置 SSH 用户 client001 的服务器类型为 Stelnet，认证方式为 password 认证。（此步骤可以不配置）

```
[Router] ssh user client001 service-type stelnet authentication-type password
```

(2) Stelnet 客户端建立与 Stelnet 服务器的连接

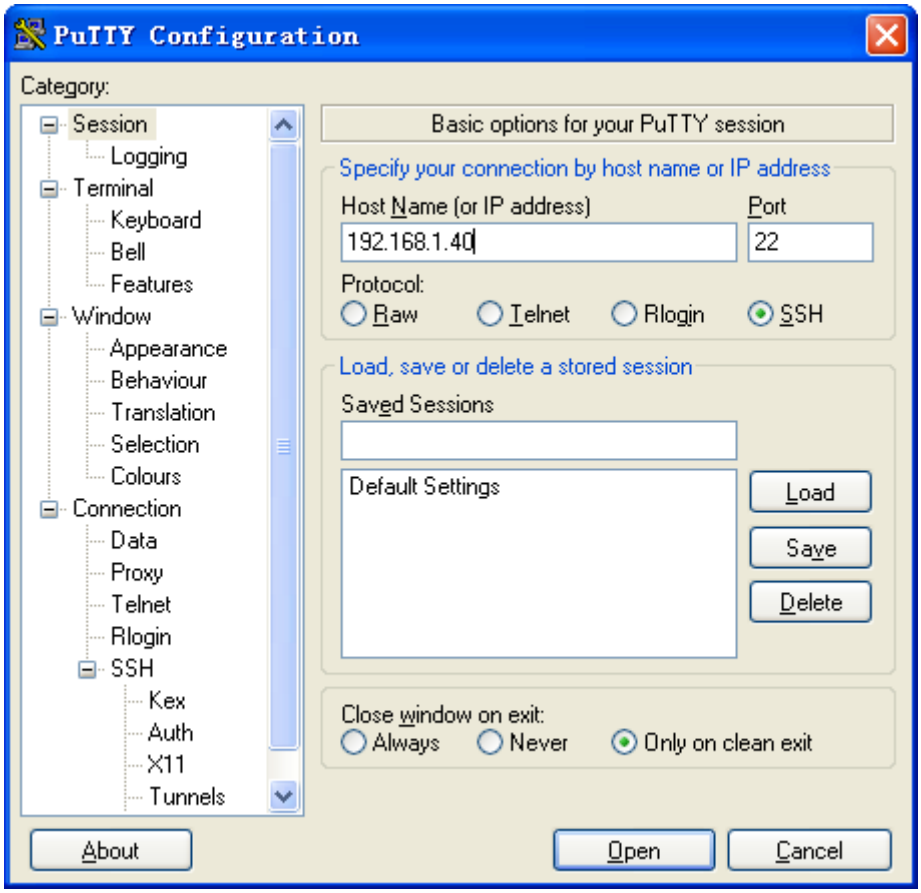
说明

Stelnet 客户端软件有很多，例如 PuTTY、OpenSSH 等。本文中仅以客户端软件 PuTTY0.58 为例，说明 Stelnet 客户端的配置方法。

建立与 Stelnet 服务器的连接。

打开PuTTY.exe程序，出现如图 1-3所示的客户端配置界面。在“Host Name（or IP address）”文本框中输入Stelnet服务器的IP地址为 192.168.1.40。

图1-3 Stelnet 客户端配置界面



在图 1-3中，单击<Open>按钮。按提示输入用户名client001 及密码aabbcc，即可进入Router的配置界面。

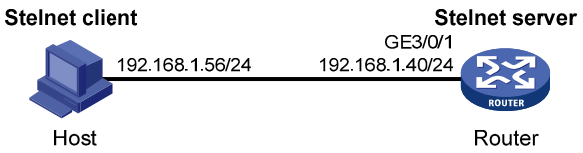
1.7.2 设备作为Stelnet服务器配置举例（publickey认证）

1. 组网需求

- 用户可以通过 Host 上运行的 Stelnet 客户端软件（SSH2 版本）安全地登录到 Router 上进行配置管理；
- Router 采用 publickey 认证方式对 Stelnet 客户端进行认证，使用的公钥算法为 RSA。

2. 组网图

图1-4 设备作为 Stelnet 服务器配置组网图



3. 配置步骤

说明

- 在服务器的配置过程中需要指定客户端的公钥信息，因此需要首先完成客户端密钥对的配置，再进行服务器的配置。
- 客户端软件有很多，例如 PuTTY、OpenSSH 等。本文中仅以客户端软件 PuTTY0.58 为例，说明 Stelnet 客户端的配置方法。

(1) 配置 Stelnet 客户端

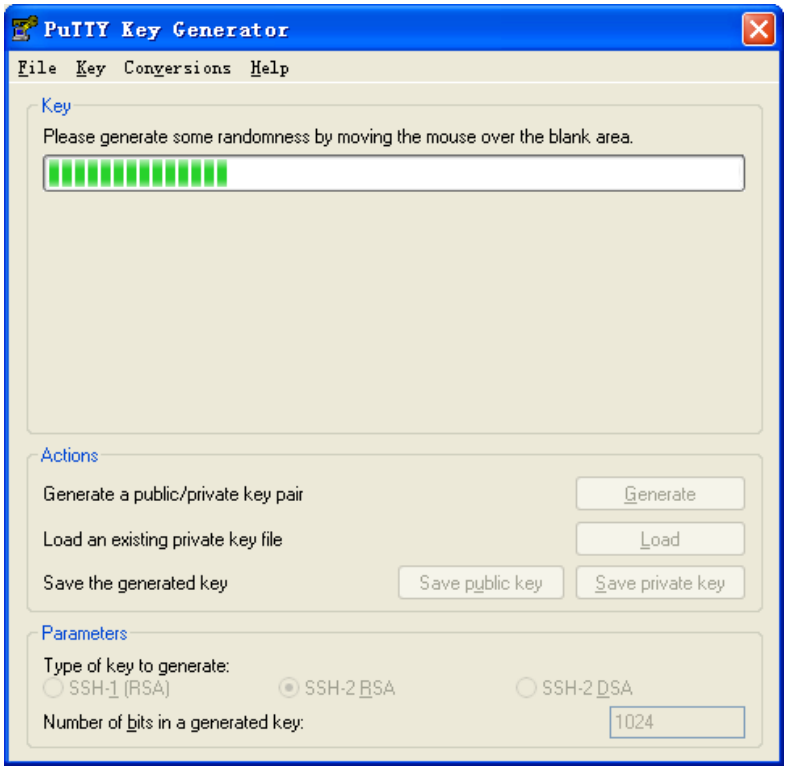
生成 RSA 密钥对。

运行 PuTTYGen.exe，在参数栏中选择“SSH-2 RSA”，点击<Generate>，产生客户端密钥对。

图1-5 生成客户端密钥（步骤 1）

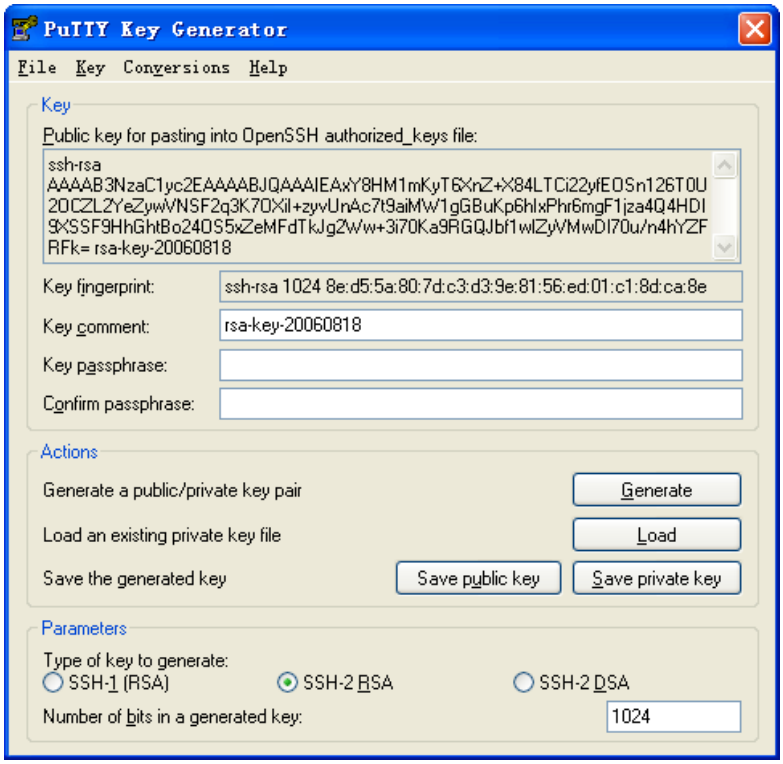
在产生密钥对的过程中需不停地移动鼠标，鼠标移动仅限于下图蓝色框中除绿色标记进程条外的地方，否则进程条的显示会不动，密钥对将停止产生，见图 1-6。

图1-6 生成客户端密钥（步骤 2）



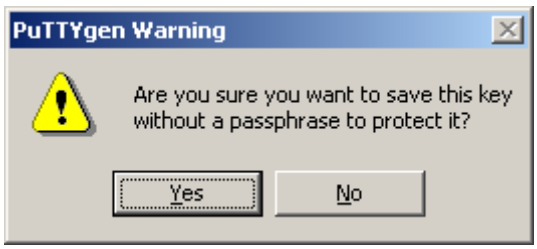
密钥对产生后，点击<Save public key>，输入存储公钥的文件名 key.pub，点击<保存>按钮。

图1-7 生成客户端密钥（步骤 3）



点击<Save private key>存储私钥，弹出警告框，提醒是否保存没做任何保护措施的私钥，点击<Yes>，输入私钥文件名为 private.ppk，点击保存。

图1-8 生成客户端密钥（步骤 4）



客户端生成密钥对后，需要将保存的公钥文件 key.pub 通过 FTP/TFTP 方式上传到服务器，具体过程略。

(2) 配置 Stelnet 服务器

生成 RSA 密钥对。

```
<Router> system-view
[Router] public-key local create rsa
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
It will take a few minutes.
Press CTRL+C to abort.
Input the bits of the modulus[default = 1024]:
Generating Keys...
++++++++++++++++++++++++
++++++++++++++++++++++
+++++
+++++
```

生成 DSA 密钥对。

```
[Router] public-key local create dsa
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
It will take a few minutes.
Press CTRL+C to abort.
Input the bits of the modulus[default = 1024]:
Generating Keys...
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
++++++++++++++++++++++++++++++++++
```

使能 SSH 服务器功能。

```
[Router] ssh server enable
```

配置接口 GigabitEthernet3/0/1 的 IP 地址，客户端将通过该地址连接 Stelnet 服务器。

```
[Router] interface gigabitethernet 3/0/1
[Router-GigabitEthernet3/0/1] ip address 192.168.1.40 255.255.255.0
[Router-GigabitEthernet3/0/1] quit
```

设置 Stelnet 客户端登录用户界面的认证方式为 AAA 认证。

```
[Router] user-interface vty 0 4
```

```
[Router-ui-vty0-4] authentication-mode scheme
```

设置 Router 上远程用户登录协议为 SSH。

```
[Router-ui-vty0-4] protocol inbound ssh
[Router-ui-vty0-4] quit
```

从文件 key.pub 中导入远端的公钥，并命名为 ClientKey。

```
[Router] public-key peer ClientKey import sshkey key.pub
```

设置 SSH 用户 client002 的认证方式为 publickey，并指定公钥为 ClientKey。

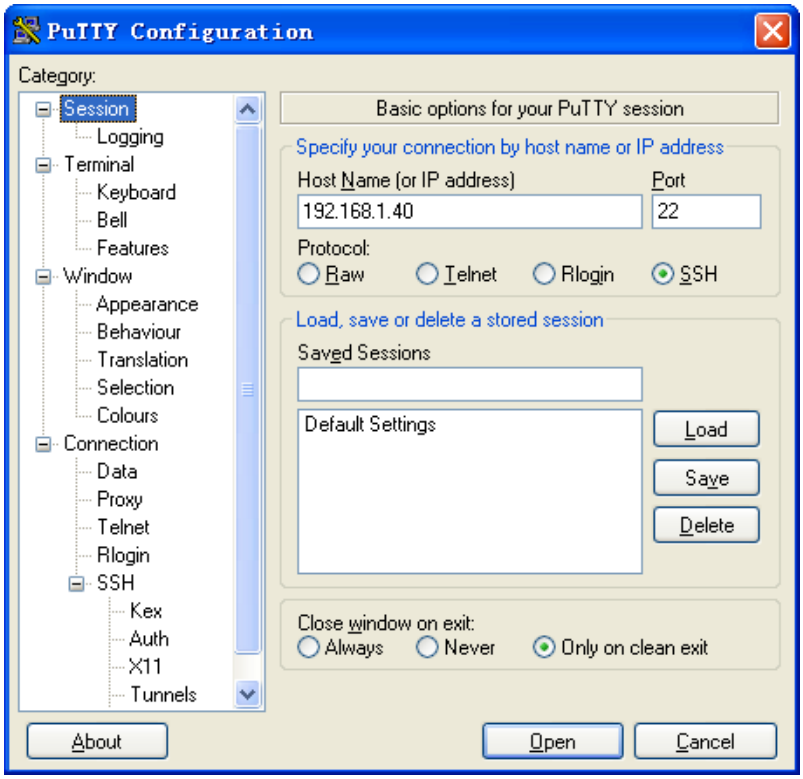
```
[Router] ssh user client002 service-type stelnet authentication-type publickey assign
publickey ClientKey
```

(3) Stelnet 客户端建立与 Stelnet 服务器的连接

指定私钥文件，并建立与 Stelnet 服务器的连接。

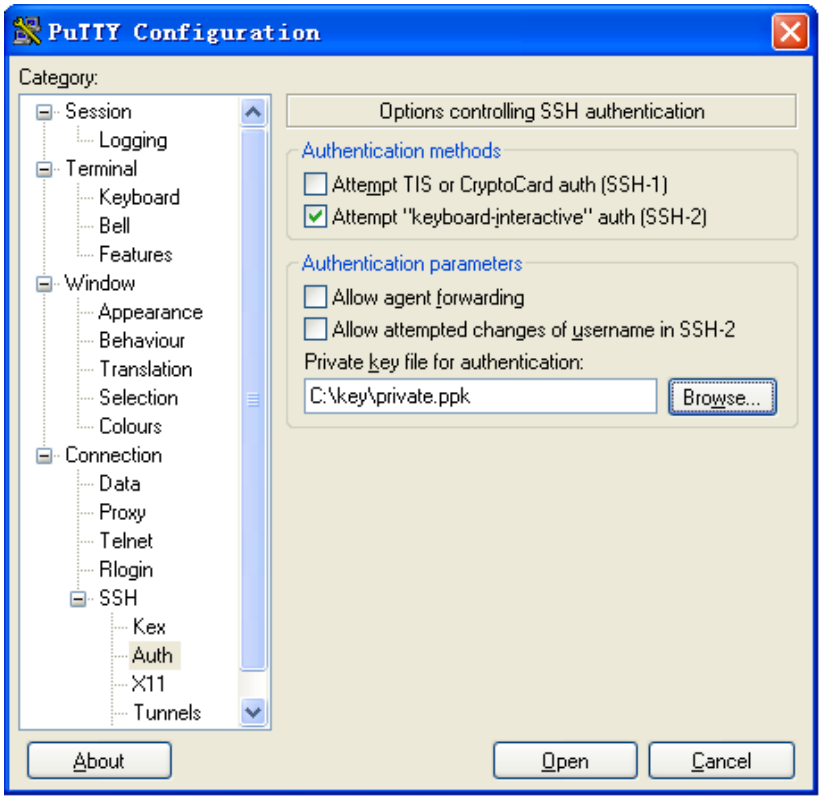
打开PuTTY.exe程序，出现如图 1-9所示的客户端配置界面。在“Host Name（or IP address）”文本框中输入Stelnet服务器的IP地址为 192.168.1.40。

图1-9 Stelnet 客户端配置界面（步骤 1）



单击左侧导航树“Connection->SSH”下面的“Auth”（认证），出现如图 1-10的界面。单击<Browse…>按钮，弹出文件选择窗口。选择与配置到服务器端的公钥对应的私钥文件private.ppk。

图1-10 Stelnet 客户端配置界面（步骤 2）



如图 1-10，单击<Open>按钮。按提示输入用户名client002，即可进入Router的配置界面。

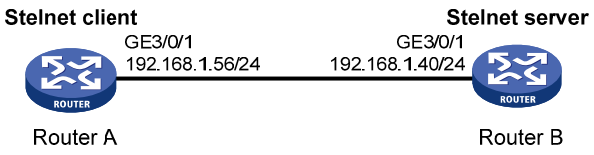
1.7.3 设备作为Stelnet客户端配置举例（password认证）

1. 组网需求

- 配置 Router A 作为 Stelnet 客户端，用户能够通过 Router A 安全地登录到 Router B 上进行配置管理。
- Router B 作为 Stelnet 服务器采用 password 认证方式对 Stelnet 客户端进行认证，客户端的用户名和密码保存在 Router B 上。

2. 组网图

图1-11 设备作为 Stelnet 客户端的 password 认证配置组网图



3. 配置步骤

(1) 配置 Stelnet 服务器

生成 RSA 密钥对。

```
<RouterB> system-view
```

```
[RouterB] public-key local create rsa
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
It will take a few minutes.
Press CTRL+C to abort.
Input the bits of the modulus[default = 1024]:
Generating Keys...
++++++++++++++++++++++++
++++++++++++++++++++++++
+++++
+++++
```

生成 DSA 密钥对。

```
[RouterB] public-key local create dsa
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
It will take a few minutes.
Press CTRL+C to abort.
Input the bits of the modulus[default = 1024]:
Generating Keys...
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
++++++++++++++++++++++++++++++++
```

使能 SSH 服务器功能。

```
[RouterB] ssh server enable
```

配置接口 GigabitEthernet3/0/1 的 IP 地址，客户端将通过该地址连接 Stelnet 服务器。

```
[RouterB] interface gigabitethernet 3/0/1
[RouterB-GigabitEthernet3/0/1] ip address 192.168.1.40 255.255.255.0
[RouterB-GigabitEthernet3/0/1] quit
```

设置 Stelnet 客户端登录用户界面的认证方式为 AAA 认证。

```
[RouterB] user-interface vty 0 4
[RouterB-ui-vty0-4] authentication-mode scheme
```

设置 Router B 上远程用户登录协议为 SSH。

```
[RouterB-ui-vty0-4] protocol inbound ssh
[RouterB-ui-vty0-4] quit
```

创建本地用户 client001，密码为 aabbcc，服务类型为 SSH。

```
[RouterB] local-user client001
[RouterB-luser-client001] password simple aabbcc
[RouterB-luser-client001] service-type ssh
[RouterB-luser-client001] quit
```

配置 SSH 用户 client001 的服务类型为 Stelnet，认证方式为 password 认证。（此步骤可以不配置）

```
[RouterB] ssh user client001 service-type stelnet authentication-type password
```

(2) Stelnet 客户端建立与 Stelnet 服务器的连接

配置接口 GigabitEthernet3/0/1 的 IP 地址。

```
<RouterA> system-view
[RouterA] interface gigabitethernet 3/0/1
[RouterA-GigabitEthernet3/0/1] ip address 192.168.1.56 255.255.255.0
```

```
[RouterA-GigabitEthernet3/0/1] quit
[RouterA] quit
```

- 如果客户端支持首次认证，则可以直接与服务器建立连接。

建立到服务器 192.168.1.40 的 SSH 连接。

```
<RouterA> ssh2 192.168.1.40
Username: client001
Trying 192.168.1.40 ...
Press CTRL+K to abort
Connected to 192.168.1.40 ...

The Server is not authenticated. Continue? [Y/N]:y
Do you want to save the server public key? [Y/N]:n
Enter password:
```

输入正确的密码之后，即可成功登录到 Router B 上。

- 如果客户端不支持首次认证，则需要进行如下配置。

配置客户端不支持首次认证。

```
[RouterA] undo ssh client first-time
```

在客户端配置服务器端的主机公钥。在公钥编辑视图输入服务器端的主机公钥，由于客户端缺省采用 DSA 主机公钥认证服务器，因此这里输入的是在服务器端通过 **display public-key local dsa public** 命令显示的公钥内容。

```
[RouterA] public-key peer key1
[RouterA-pkey-public-key] public-key-code begin
[RouterA-pkey-key-code]308201B73082012C06072A8648CE3804013082011F0281810
0D757262C4584C44C211F18BD96E5F0
[RouterA-pkey-key-code]61C4F0A423F7FE6B6B85B34CEF72CE14A0D3A5222FE08CECE
65BE6C265854889DC1EDBD13EC8B274
[RouterA-pkey-key-code]DA9F75BA26CCB987723602787E922BA84421F22C3C89CB9B0
6FD60FE01941DDD77FE6B12893DA76E
[RouterA-pkey-key-code]EBC1D128D97F0678D7722B5341C8506F358214B16A2FAC4B3
68950387811C7DA33021500C773218C
[RouterA-pkey-key-code]737EC8EE993B4F2DED30F48EDACE915F0281810082269009E
14EC474BAF2932E69D3B1F18517AD95
[RouterA-pkey-key-code]94184CCDFCEAE96EC4D5EF93133E84B47093C52B20CD35D02
492B3959EC6499625BC4FA5082E22C5
[RouterA-pkey-key-code]B374E16DD00132CE71B020217091AC717B612391C76C1FB2E
88317C1BD8171D41ECB83E210C03CC9
[RouterA-pkey-key-code]B32E810561C21621C73D6DAAC028F4B1585DA7F42519718CC
9B09EEF0381840002818000AF995917
[RouterA-pkey-key-code]E1E570A3F6B1C2411948B3B4FFA256699B3BF871221CC9C5D
F257523777D033BEE77FC378145F2AD
[RouterA-pkey-key-code]D716D7DB9FCABB4ADBF6FB4FDB0CA25C761B308EF53009F71
01F7C62621216D5A572C379A32AC290
[RouterA-pkey-key-code]E55B394A217DA38B65B77F0185C8DB8095522D1EF044B465E
8716261214A5A3B493E866991113B2D
[RouterA-pkey-key-code]485348
[RouterA-pkey-key-code] public-key-code end
[RouterA-pkey-public-key] peer-public-key end
```

指定服务器 192.168.1.40 对应的主机公钥名称为 key1。

```
[RouterA] ssh client authentication server 192.168.1.40 assign publickey key1
[RouterA] quit
```

建立到服务器 192.168.1.40 的 SSH 连接。

```
<RouterA> ssh2 192.168.1.40
Username: client001
Trying 192.168.1.40
Press CTRL+K to abort
Connected to 192.168.1.40...
Enter password:
```

输入正确的密码之后，即可成功登录到 Router B 上。

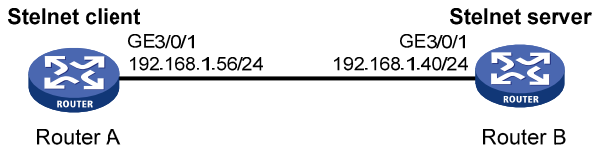
1.7.4 设备作为Stelnet客户端配置举例（publickey认证）

1. 组网需求

- 配置 Router A 作为 Stelnet 客户端，用户能够通过 Router A 安全地登录到 Router B 上进行配置管理。
- Router B 作为 Stelnet 服务器采用 publickey 认证方式对 Stelnet 客户端进行认证，使用的公钥算法为 DSA。

2. 组网图

图1-12 设备作为 Stelnet 客户端配置组网图



3. 配置步骤

说明

在服务器的配置过程中需要指定客户端的公钥信息，因此建议首先完成客户端密钥对的配置，再进行服务器的配置。

(1) 配置 Stelnet 客户端

配置接口 GigabitEthernet3/0/1 的 IP 地址。

```
<RouterA> system-view
[RouterA] interface gigabitethernet 3/0/1
[RouterA-GigabitEthernet3/0/1] ip address 192.168.1.56 255.255.255.0
[RouterA-GigabitEthernet3/0/1] quit
```

生成 DSA 密钥对。

```
[RouterA] public-key local create dsa
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
```

```
It will take a few minutes.
Press CTRL+C to abort.
Input the bits of the modulus[default = 1024]:
Generating Keys...
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
++++++++++++++++++++++++++++++++++
```

将生成的 DSA 主机公钥导出到指定文件 key.pub 中。

```
[RouterA] public-key local export dsa ssh2 key.pub
[RouterA] quit
```

客户端生成密钥对后，需要将保存的公钥文件 key.pub 通过 FTP/TFTP 方式上传到服务器，具体过程略。

(2) 配置 Stelnet 服务器

生成 RSA 密钥对。

```
<RouterB> system-view
[RouterB] public-key local create rsa
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
It will take a few minutes.
Press CTRL+C to abort.
Input the bits of the modulus[default = 1024]:
Generating Keys...
++++++++++++++++++++++++
++++++++++++++++++++++
+++++
+++++
```

生成 DSA 密钥对。

```
[RouterB] public-key local create dsa
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
It will take a few minutes.
Press CTRL+C to abort.
Input the bits of the modulus[default = 1024]:
Generating Keys...
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
++++++++++++++++++++++++++++++++++
```

使能 SSH 服务器功能。

```
[RouterB] ssh server enable
```

配置接口 GigabitEthernet3/0/1 的 IP 地址，客户端将通过该地址连接 Stelnet 服务器。

```
[RouterB] interface gigabitethernet 3/0/1
[RouterB-GigabitEthernet3/0/1] ip address 192.168.1.40 255.255.255.0
[RouterB-GigabitEthernet3/0/1] quit
```

设置 Stelnet 客户端登录用户界面的认证方式为 AAA 认证。

```
[RouterB] user-interface vty 0 4
[RouterB-ui-vty0-4] authentication-mode scheme
```

设置 Router B 上远程用户登录协议为 SSH。

```
[RouterB-ui-vty0-4] protocol inbound ssh
```

设置用户能访问的命令级别为 3。

```
[RouterB-ui-vty0-4] user privilege level 3
[RouterB-ui-vty0-4] quit
```

从文件 key.pub 中导入远端的公钥，并命名为 ClientKey。

```
[RouterB] public-key peer ClientKey import sshkey key.pub
```

设置 SSH 用户 client002 的认证方式为 publickey，并指定公钥为 ClientKey。

```
[RouterB] ssh user client002 service-type stelnet authentication-type publickey assign
publickey ClientKey
```

(3) Stelnet 客户端建立与 Stelnet 服务器的连接

建立到服务器 192.168.1.40 的 SSH 连接。

```
<RouterA> ssh2 192.168.1.40
Username: client002
Trying 192.168.1.40 ...
Press CTRL+K to abort
Connected to 192.168.1.40 ...

The Server is not authenticated. Continue? [Y/N]:y
Do you want to save the server public key? [Y/N]:n
```

之后，即可成功登录到 Router B 上。

1.8 SFTP典型配置举例

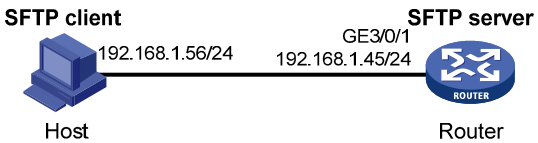
1.8.1 设备作为SFTP服务器配置举例（password认证）

1. 组网需求

- 用户可以通过 Host 上运行的 SFTP 客户端软件安全地登录到 Router 上进行文件管理和文件传送操作；
- Router 采用 password 认证方式对 SFTP 客户端进行认证，客户端的用户名和密码保存在本地。

2. 组网图

图1-13 设备作为 SFTP 服务器配置组网图



3. 配置步骤

(1) 配置 SFTP 服务器

生成 RSA 密钥对。

```
<Router> system-view
[Router] public-key local create rsa
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
```

```
It will take a few minutes.
Press CTRL+C to abort.
Input the bits of the modulus[default = 1024]:
Generating Keys...
++++++++++++++++++++++++
++++++++++++++++++++++++
+++++
+++++
```

生成 DSA 密钥对。

```
[Router] public-key local create dsa
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
It will take a few minutes.
Press CTRL+C to abort.
Input the bits of the modulus[default = 1024]:
Generating Keys...
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
++++++++++++++++++++++++++++++++
```

使能 SSH 服务器功能。

```
[Router] ssh server enable
```

启动 SFTP 服务器。

```
[Router] sftp server enable
```

配置接口 GigabitEthernet3/0/1 的 IP 地址，客户端将通过该地址连接 SSH 服务器。

```
[Router] interface gigabitethernet 3/0/1
[Router-GigabitEthernet3/0/1] ip address 192.168.1.45 255.255.255.0
[Router-GigabitEthernet3/0/1] quit
```

设置 SFTP 客户端登录用户界面的认证方式为 AAA 认证。

```
[Router] user-interface vty 0 4
[Router-ui-vty0-4] authentication-mode scheme
```

设置 Router 上远程用户登录协议为 SSH。

```
[Router-ui-vty0-4] protocol inbound ssh
[Router-ui-vty0-4] quit
```

创建本地用户 client002，密码为 aabbcc，服务类型为 SSH。

```
[Router] local-user client002
[Router-luser-client002] password simple aabbcc
[Router-luser-client002] service-type ssh
[Router-luser-client002] quit
```

配置 SSH 用户认证方式为 password，服务类型为 SFTP。

```
[Router] ssh user client002 service-type sftp authentication-type password
```

(2)　SFTP 客户端建立与 SFTP 服务器的连接

说明

- SFTP 客户端软件有很多，本文中仅以客户端软件 PuTTY0.58 中的 PSFTP 为例，说明 SFTP 客户端的配置方法。
- PSFTP 只支持 password 认证，不支持 publickey 认证。

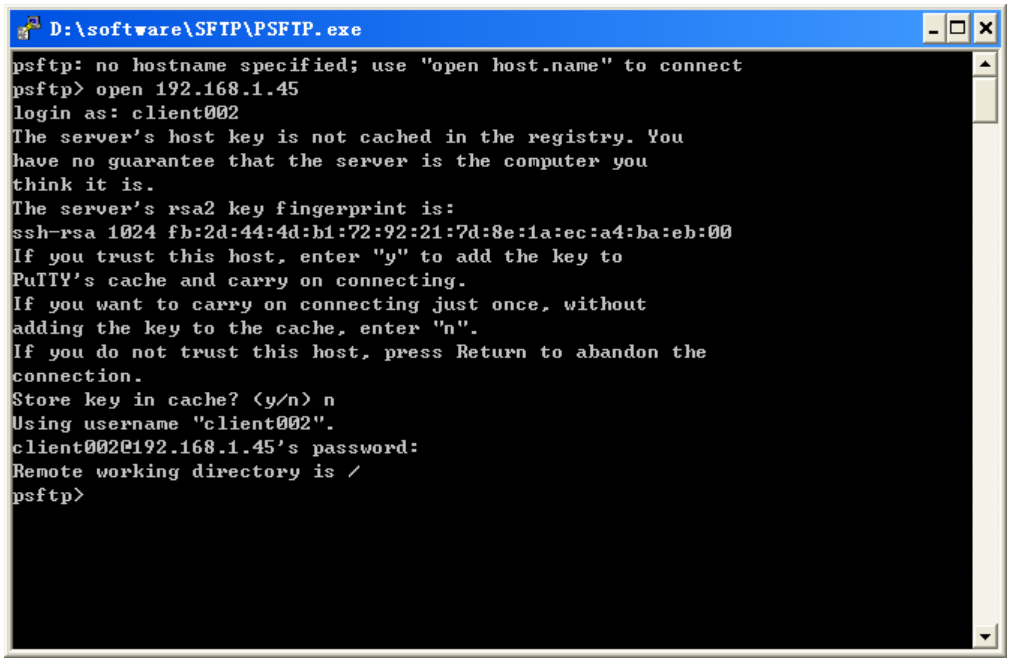
建立与 SFTP 服务器的连接。

打开psftp.exe程序，出现如图 1-14所示的客户端配置界面。输入如下命令：

```
open 192.168.1.45
```

根据提示输入用户名 client002、密码 aabbcc，即可登录 SFTP 服务器。

图1-14 SFTP 客户端登录界面



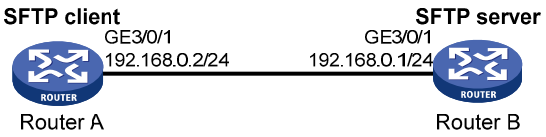
1.8.2 设备作为SFTP客户端配置举例（publickey认证）

1. 组网需求

- 配置 Router A 作为 SFTP 客户端，用户能够通过 Router A 安全地登录到 Router B 上进行文件管理和文件传送等操作。
- Router B 作为 SFTP 服务器采用 publickey 认证方式对 SFTP 客户端进行认证，使用的公钥算法为 RSA。

2. 组网图

图1-15 设备作为 SFTP 客户端配置组网图



3. 配置步骤

说明

在服务器的配置过程中需要指定客户端的公钥信息，因此建议首先完成客户端密钥对的配置，再进行服务器的配置。

(1) 配置 SFTP 客户端

配置接口 GigabitEthernet3/0/1 的 IP 地址。

```
<RouterA> system-view
[RouterA] interface gigabitethernet 3/0/1
[RouterA-GigabitEthernet3/0/1] ip address 192.168.0.2 255.255.255.0
[RouterA-GigabitEthernet3/0/1] quit
```

生成 RSA 密钥对。

```
[RouterA] public-key local create rsa
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
It will take a few minutes.
Press CTRL+C to abort.
Input the bits of the modulus[default = 1024]:
Generating Keys...
++++++++++++++++++++++++
++++++++++++++++++++++++
+++++
+++++
```

将生成的 RSA 主机公钥导出到指定文件 pubkey 中。

```
[RouterA] public-key local export rsa ssh2 pubkey
[RouterA] quit
```

客户端生成密钥对后，需要将保存的公钥文件 pubkey 通过 FTP/TFTP 方式上传到服务器，具体过程略。

(2) 配置 SFTP 服务器

生成 RSA 密钥对。

```
<RouterB> system-view
[RouterB] public-key local create rsa
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
It will take a few minutes.
```

```
Press CTRL+C to abort.
Input the bits of the modulus[default = 1024]:
Generating Keys...
++++++++++++++++++++++++
++++++++++++++++++++++++
+++++
+++++
```

生成 DSA 密钥对。

```
[RouterB] public-key local create dsa
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
It will take a few minutes.
Press CTRL+C to abort.
Input the bits of the modulus[default = 1024]:
Generating Keys...
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
++++++++++++++++++++++++++++++++++
```

使能 SSH 服务器功能。

```
[RouterB] ssh server enable
```

启动 SFTP 服务器。

```
[RouterB] sftp server enable
```

配置接口 GigabitEthernet3/0/1 的 IP 地址，客户端将通过该地址连接 SFTP 服务器。

```
[RouterB] interface gigabitethernet 3/0/1
[RouterB-GigabitEthernet3/0/1] ip address 192.168.0.1 255.255.255.0
[RouterB-GigabitEthernet3/0/1] quit
```

设置 SFTP 客户端登录用户界面的认证方式为 AAA 认证。

```
[RouterB] user-interface vty 0 4
[RouterB-ui-vty0-4] authentication-mode scheme
```

设置 Router B 上远程用户登录协议为 SSH。

```
[RouterB-ui-vty0-4] protocol inbound ssh
[RouterB-ui-vty0-4] quit
```

从文件 pubkey 中导入远端的公钥，并命名为 RouterKey。

```
[RouterB] public-key peer RouterKey import sshkey pubkey
```

设置 SSH 用户 client001 的服务类型为 SFTP，认证方式为 publickey，并指定公钥为 RouterKey，工作目录为 cfa0:/。

```
[RouterB] ssh user client001 service-type sftp authentication-type publickey assign
publickey RouterKey work-directory cfa0:/
```

(3) SFTP 客户端建立与 SFTP 服务器的连接

与远程 SFTP 服务器建立连接，进入 SFTP 客户端视图。

```
<RouterA> sftp 192.168.0.1 identity-key rsa
Input Username: client001
Trying 192.168.0.1 ...
Press CTRL+K to abort
Connected to 192.168.0.1 ...

The Server is not authenticated. Continue? [Y/N]:y
```

```
Do you want to save the server public key? [Y/N]:n

sftp-client>
```
显示服务器的当前目录，删除文件 z，并检查此文件是否删除成功。
```
sftp-client> dir
-rwxrwxrwx   1 noone    nogroup      1759 Aug 23 06:52 config.cfg
-rwxrwxrwx   1 noone    nogroup       225 Aug 24 08:01 pubkey2
-rwxrwxrwx   1 noone    nogroup       283 Aug 24 07:39 pubkey
drwxrwxrwx   1 noone    nogroup         0 Sep 01 06:22 new
-rwxrwxrwx   1 noone    nogroup       225 Sep 01 06:55 pub
-rwxrwxrwx   1 noone    nogroup         0 Sep 01 08:00 z
sftp-client> delete z
The following File will be deleted:
/z
Are you sure to delete it? [Y/N]:y
This operation may take a long time.Please wait...

File successfully Removed
sftp-client> dir
-rwxrwxrwx   1 noone    nogroup      1759 Aug 23 06:52 config.cfg
-rwxrwxrwx   1 noone    nogroup       225 Aug 24 08:01 pubkey2
-rwxrwxrwx   1 noone    nogroup       283 Aug 24 07:39 pubkey
drwxrwxrwx   1 noone    nogroup         0 Sep 01 06:22 new
-rwxrwxrwx   1 noone    nogroup       225 Sep 01 06:55 pub
```
新增目录 new1，并检查新目录是否创建成功。
```
sftp-client> mkdir new1
New directory created
sftp-client> dir
-rwxrwxrwx   1 noone    nogroup      1759 Aug 23 06:52 config.cfg
-rwxrwxrwx   1 noone    nogroup       225 Aug 24 08:01 pubkey2
-rwxrwxrwx   1 noone    nogroup       283 Aug 24 07:39 pubkey
drwxrwxrwx   1 noone    nogroup         0 Sep 01 06:22 new
-rwxrwxrwx   1 noone    nogroup       225 Sep 01 06:55 pub
drwxrwxrwx   1 noone    nogroup         0 Sep 02 06:30 new1
```
将目录名 new1 更名为 new2，并查看是否更名成功。
```
sftp-client> rename new1 new2
File successfully renamed
sftp-client> dir
-rwxrwxrwx   1 noone    nogroup      1759 Aug 23 06:52 config.cfg
-rwxrwxrwx   1 noone    nogroup       225 Aug 24 08:01 pubkey2
-rwxrwxrwx   1 noone    nogroup       283 Aug 24 07:39 pubkey
drwxrwxrwx   1 noone    nogroup         0 Sep 01 06:22 new
-rwxrwxrwx   1 noone    nogroup       225 Sep 01 06:55 pub
drwxrwxrwx   1 noone    nogroup         0 Sep 02 06:33 new2
```
从服务器上下载文件 pubkey2 到本地，并更名为 public。
```
sftp-client> get pubkey2 public
Remote  file:/pubkey2 --->  Local file: public
```

```
Downloading file successfully ended
```

将本地文件 pu 上传到服务器上，更名为 puk，并查看上传是否成功。

```
sftp-client> put pu puk
Local file:pu --->  Remote file: /puk
Uploading file successfully ended
sftp-client> dir
-rwxrwxrwx   1 noone    nogroup      1759 Aug 23 06:52 config.cfg
-rwxrwxrwx   1 noone    nogroup       225 Aug 24 08:01 pubkey2
-rwxrwxrwx   1 noone    nogroup       283 Aug 24 07:39 pubkey
drwxrwxrwx   1 noone    nogroup         0 Sep 01 06:22 new
drwxrwxrwx   1 noone    nogroup         0 Sep 02 06:33 new2
-rwxrwxrwx   1 noone    nogroup       283 Sep 02 06:35 pub
-rwxrwxrwx   1 noone    nogroup       283 Sep 02 06:36 puk
sftp-client>
```

退出 SFTP 客户端视图。

```
sftp-client> quit
Bye
Connection closed.
<RouterA>
```

1.9 SCP文件传输配置举例

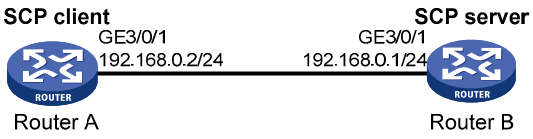
1. 组网需求

如下图所示，Router A 作为 SCP 客户端，Router B 作为 SCP 服务器。现有如下具体需求：

- 用户能够通过 Router A 安全地与 Router B 进行文件传输。
- Router B 采用 password 认证对 SCP 客户端进行认证，客户端的用户名和密码保存在 Router B 上。

2. 组网图

图1-16 SCP 文件传输配置组网图



3. 配置步骤

(1) 配置 SCP 服务器

```
<RouterB> system-view
[RouterB] public-key local create rsa
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
It will take a few minutes.
Press CTRL+C to abort.
Input the bits of the modulus[default = 1024]:
Generating Keys...
```

```
++++++++++++++++++++++++
++++++++++++++++++++++
+++++
+++++
```

生成 DSA 密钥对。

```
[RouterB] public-key local create dsa
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
It will take a few minutes.
Press CTRL+C to abort.
Input the bits of the modulus[default = 1024]:
Generating Keys...
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
++++++++++++++++++++++++++++++++
```

使能 SSH 服务器功能。

```
[RouterB] ssh server enable
```

配置接口 GigabitEthernet3/0/1 的 IP 地址，客户端将通过该地址连接 SCP 服务器。

```
[RouterB] interface gigabitethernet 3/0/1
[RouterB-GigabitEthernet3/0/1] ip address 192.168.0.1 255.255.255.0
[RouterB-GigabitEthernet3/0/1] quit
```

设置 Stelnet 客户端登录用户界面的认证方式为 AAA 认证。

```
[RouterB] user-interface vty 0 4
[RouterB-ui-vty0-4] authentication-mode scheme
```

设置 Router B 上远程用户登录协议为 SSH。

```
[RouterB-ui-vty0-4] protocol inbound ssh
[RouterB-ui-vty0-4] quit
```

创建本地用户 client001，密码为 aabbcc，服务类型为 SSH。

```
[RouterB] local-user client001
[RouterB-luser-client001] password simple aabbcc
[RouterB-luser-client001] service-type ssh
[RouterB-luser-client001] quit
```

配置 SSH 用户 client001 的服务类型为 scp，认证方式为 password 认证。（此步骤可以不配置）

```
[RouterB] ssh user client001 service-type scp authentication-type password
```

(2) 配置 SCP 客户端

配置 GigabitEthernet3/0/1 接口的 IP 地址。

```
<RouterA> system-view
[RouterA] interface gigabitethernet 3/0/1
[RouterA-GigabitEthernet3/0/1] ip address 192.168.0.2 255.255.255.0
[RouterA-GigabitEthernet3/0/1] quit
[RouterA] quit
```

(3) SCP 客户端从 SCP 服务器下载文件

与远程 SCP 服务器建立连接，并下载远端的 remote.bin 文件，下载到本地后更名为 local.bin。

```
<RouterA> scp 192.168.0.1 get remote.bin local.bin
Username: client001
Trying 192.168.0.1 ...
```

```
Press CTRL+K to abort
Connected to 192.168.0.1 ...

The Server is not authenticated. Continue? [Y/N]:y
Do you want to save the server public key? [Y/N]:n
Enter password:
18471 bytes transfered in 0.001 seconds.
```