目 录

1 SSH

说明

仅 WX2500H-WiNet 系列不支持 slot 参数。

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。SSH 协议有两个版本，SSH1.x 和 SSH2.0（本文简称 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。

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，设备支持以下几种 SSH 应用。

- Secure Telnet：简称 Stelnet，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。
- Secure FTP：简称 SFTP，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。
- Secure Copy：简称 SCP，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。
- NETCONF over SSH：基于 SSH2，提供通过 SSH 连接给设备下发 NETCONF 指令的功能，使得用户可以安全登录到远程设备并直接进入到设备的 NETCONF 系统中进行配置和管理操作。设备仅支持作为 NETCONF over SSH 连接的服务器端。关于 NETCONF 系统的详细介绍，请参见“网络管理和监控配置指导”中的“NETCONF”。

目前，设备作为 Stelnet 服务器、SFTP 服务器、SCP 服务器时，支持 SSH2 和 SSH1 两个版本；设备作为 SSH 客户端时，只支持 SSH2 版本；设备作为 NETCONF over SSH 服务器端时，只支持 SSH2 版本。

1.1.1 SSH工作过程

本小节以SSH2 为例介绍SSH工作的过程，具体分为 表 1-1 所述的几个阶段。

表1-1 SSH 工作过程

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
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、SCP、NETCONF），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 该阶段，用户在客户端可以通过粘贴文本内容的方式执行命令，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：

- 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。
- 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、ECDSA、RSA 三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，如果合法，则发送消息请求客户端的数字签名；如果不合法，则直接发送失败消息；服务器收到客户端的数字签名之后，使用客户端的公钥对其进行解密，并根据计算结果返回认证成功或失败的消息。
- 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。
- 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。

关于 AAA 以及公钥相关内容的介绍请分别参考“安全配置指导”中的“AAA”和“公钥管理”。

说明

- 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。

1.2 配置SSH服务器

1.2.1 SSH服务器配置任务简介

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、ECDSA或RSA密钥对	必选	1.2.2
使能Stelnet服务器功能	仅对于Stelnet服务器必选	1.2.3
使能SFTP服务器功能	仅对于SFTP服务器必选	1.2.4
使能SCP服务器功能	仅对于SCP服务器必选	1.2.5
使能NETCONF over SSH服务器功能	仅对NETCONF over SSH服务器必选	1.2.6
配置SSH客户端登录时使用的用户线	仅对Stelnet客户端和NETCONF over SSH客户端必选	1.2.7
配置客户端的公钥	采用publickey、password-publickey或any认证方式时必选	1.2.8
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、password-publickey或any认证方式时必选 采用password认证方式时可选	1.2.9
配置SSH管理功能	可选	1.2.10

1.2.2 生成本地DSA、ECDSA或RSA密钥对

服务器端的 DSA、ECDSA 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，再使用该公钥对服务器发送的数字签名进行验证。

虽然一个客户端只会采用 DSA、ECDSA 或 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、ECDSA 和 RSA 三种密钥对。

- 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。SSH1 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 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。
- 生成 DSA 密钥对时，只生成一个主机密钥对。SSH1 不支持 DSA 算法。
- 生成 ECDSA 密钥对时，只生成一个主机密钥对。

服务器端生成本地 DSA、ECDSA 或 RSA 密钥对，需要注意的是：

- SSH 仅支持默认名称的本地 DSA、ECDSA 或 RSA 密钥对，不支持指定名称的本地 DSA、ECDSA 或 RSA 密钥对。关于密钥对生成命令的相关介绍请参见“安全命令参考”中的“公钥管理”。
- 生成 DSA 密钥对时，要求输入的密钥模数的长度必须小于 2048 比特。
- SSH 服务器只支持 secp256r1 类型的 ECDSA 密钥对，所以生成 SSH 服务器端密钥对时必须为 secp256r1 类型。

需要注意的是，如果服务器端不存在默认名称的本地 RSA 密钥对，则在服务器端执行 SSH 服务器相关命令行时（包括使能 Stelnet/SFTP/SCP/NETCONF over SSH 服务器、配置 SSH 用户、以及配置 SSH 服务器端的管理功能），系统会自动生成一个默认名称的本地 RSA 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、ECDSA或RSA密钥对	**public-key local create { dsa | ecdsa secp256r1 | rsa }**	缺省情况下，不存在任何DSA、ECDSA、RSA密钥对

1.2.3 使能Stelnet服务器功能

该配置任务用于使能设备上的 Stelnet 服务器功能，使客户端能采用 Stelnet 的方式登录到设备。

表1-4 使能 Stelnet 服务器功能

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

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，使客户端能采用 SFTP 的方式登录到设备。

设备作为 SFTP 服务器时，不支持 SSH1 版本的客户端发起的 SFTP 连接。

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**	缺省情况下，SFTP服务器处于关闭状态

1.2.5 使能SCP服务器功能

该配置任务用于使能设备上的 SCP 服务器功能，使客户端能采用 SCP 的方式登录到设备。

设备作为 SCP 服务器时，不支持 SSH1 版本的客户端发起的 SCP 连接。

表1-6 启动 SCP 服务器功能

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

1.2.6 使能NETCONF over SSH服务器功能

该配置任务用于使能设备上的 NETCONF over SSH 服务器功能，使得客户端能够使用支持 NETCONF over SSH 连接的客户端配置工具给设备下发 NETCONF 指令来实现对设备的访问。

设备作为 NETCONF over SSH 服务器时，不支持 SSH1 版本的客户端发起的 SSH 连接。

表1-7 启动 NETCONF over SSH 服务器功能

操作	命令	说明
进入系统视图	**system-view**	-
使能NETCONF over SSH服务器功能	**netconf ssh server enable**	缺省情况下，NETCONF over SSH服务器处于关闭状态 关于NETCONF over SSH服务器相关命令的详细介绍，请见“网络管理和监控命令参考”中的“NETCONF”

1.2.7 配置SSH客户端登录时使用的用户线

设备支持的 SSH 客户端根据不同的应用可分为：Stelnet 客户端、SFTP 客户端、SCP 客户端和 NETCONF over SSH 客户端。

- Stelnet 客户端和 NETCONF over SSH 客户端通过 VTY（Virtual Type Terminal，虚拟类型终端）用户线访问设备。因此，需要配置客户端登录时采用的 VTY 用户线，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。
- SFTP 客户端和 SCP 客户端不通过用户线访问设备，不需要配置登录时采用的 VTY 用户线。

表1-8 配置 SSH 客户端登录时使用的用户线

操作	命令	说明
进入系统视图	**system-view**	-
进入VTY用户线视图	**line vty** *number* [*ending-number*]	-
配置登录用户线的认证方式为**scheme**方式	**authentication-mode scheme**	缺省情况下，用户线认证为**password**方式 该命令的详细介绍，请参见“基础配置命令参考”中的“登录设备”

1.2.8 配置客户端的公钥

服务器在采用 publickey 方式验证客户端身份时，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，在采用 publickey、password-publickey 或 any 认证方式时，需要在服务器端配置客户端的 DSA、ECDSA 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、ECDSA 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：事先在客户端上通过显示命令或其它方式查看其公钥信息，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。

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。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（如 **public-key local export** 命令）显示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 服务器上配置的 SSH 客户端公钥数目建议不要超过 20 个。

表1-9 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*	-

操作	命令	说明
配置客户端的公钥	逐个字符输入或拷贝粘贴公钥内容	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，保存公钥数据时，将删除空格和回车符 具体介绍请参见“安全配置指导”中的“公钥管理”
退回系统视图	**peer-public-key end**	-

表1-10 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**	-
从公钥文件中导入远端客户端的公钥	**public-key peer** *keyname* **import sshkey** *filename*	-

1.2.9 配置SSH用户

本配置用于创建 SSH 用户，并指定 SSH 用户的服务类型、认证方式以及对应的客户端公钥或数字证书。SSH 用户的配置与服务器端采用的认证方式有关，具体如下：

- 如果服务器采用了 publickey 认证，则必须在设备上创建相应的 SSH 用户，以及同名的本地用户（用于下发授权属性：工作目录、用户角色）。
- 如果服务器采用了 password 认证，则必须在设备上创建相应的本地用户（适用于本地认证），或在远程服务器（如 RADIUS 服务器，适用于远程认证）上创建相应的 SSH 用户。这种情况下，并不需要通过本配置创建相应的 SSH 用户，如果创建了 SSH 用户，则必须保证指定了正确的服务类型以及认证方式。
- 如果服务器采用了 password-publickey 或 any 认证，则必须在设备上创建相应的 SSH 用户，以及在设备上创建同名的本地用户（适用于本地认证）或者在远程认证服务器上创建同名的 SSH 用户（如 RADIUS 服务器，适用于远程认证）。

配置 SSH 用户时，需要注意：

- SCP 或 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。通过 publickey 或 password-publickey 认证登录服务器的用户使用的工作目录均为对应的本地用户视图下为该用户设置的工作目录；通过 password 认证登录服务器的用户，使用的工作目录为通过 AAA 授权的工作目录。
- 通过 publickey 或 password-publickey 认证登录服务器的 SSH 用户将被授予对应的本地用户视图下指定的用户角色；通过 password 认证登录服务器的 SSH 用户将被授予远程 AAA 服务器或设备本地授权的用户角色。
- 对 SSH 用户配置的修改，不会影响已经登录的 SSH 用户，仅对新登录的用户生效。
- 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“1.2.8 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 SSH 用户可以成功通过认证，通过 **ssh user** 命令指定的 PKI 域中必须存在用于验证客户端证书的 CA 证书。

关于本地用户以及远程认证的相关配置请参见“安全配置指导”中的“AAA”。

表1-11 配置 SSH 用户

操作	命令	说明
进入系统视图	**system-view**	-
创建SSH用户，并指定SSH用户的服务类型和认证方式	**ssh user** *username* **service-type** { **all** | **netconf** | **scp** | **sftp** | **stelnet** } **authentication-type** { **password** | { **any** | **password-publickey** | **publickey** } **assign** { **pki-domain** *domain-name* | **publickey** *keyname* } }	SSH服务器上最多可以创建1024个SSH用户

1.2.10 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 服务器密钥对的最小更新间隔时间，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，可灵活设置最小更新间隔时间。
- 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。在 any 认证方式下，SSH 客户端通过 publickey 和 password 两种方式进行认证尝试的次数总和，不能超过配置的 SSH 连接认证尝试次数。
- 设置对 SSH 客户端的访问控制，使用 ACL 过滤向 SSH 服务器发起连接的 SSH 客户端。
- 设置 SSH 服务器向 SSH 客户端发送的报文的 DSCP 优先级。DSCP 携带在 IPv4 报文中的 ToS 字段和 IPv6 报文中的 Trafic class 字段，用来体现报文自身的优先等级，决定报文传输的优先程度。
- 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。
- 设置同时在线的最大 SSH 用户连接数。系统资源有限，当前在线 SSH 用户数超过设定的最大值时，系统会拒绝新的 SSH 连接请求。

表1-12 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**	缺省情况下，SSH服务器不兼容SSH1版本的客户端

操作	命令	说明
设置RSA服务器密钥对的最小更新间隔时间	**ssh server rekey-interval** *hours*	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*	缺省情况下，SSH用户的认证超时时间为60秒
设置SSH认证尝试的最大次数	**ssh server authentication-retries** *times*	缺省情况下，SSH连接认证尝试的最大次数为3次
设置对IPv4 SSH用户的访问控制	**ssh server acl** [**mac**] *acl-number*	缺省情况下，允许所有IPv4 SSH用户向设备发起SSH访问
设置对IPv6 SSH用户的访问控制	**ssh server ipv6 acl** { **ipv6** | **mac** } *acl-number*	缺省情况下，允许所有IPv6 SSH用户向设备发起SSH访问
设置Pv4 SSH服务器向SSH客户端发送的报文的DSCP优先级	**ssh server dscp** *dscp-value*	缺省情况下，IPv4 SSH报文的DSCP优先级为48
设置IPv6 SSH服务器向SSH客户端发送的报文的DSCP优先级	**ssh server ipv6 dscp** *dscp-value*	缺省情况下，IPv6 SSH报文的DSCP优先级为48
设置SFTP用户连接的空闲超时时间	**sftp server idle-timeout** *time-out-value*	缺省情况下，SFTP用户连接的空闲超时时间为10分钟
设置同时在线的最大SSH用户连接数	**aaa session-limit ssh** *max-sessions*	缺省的最大SSH用户连接数为32 该值的修改不会对已经在线的用户连接造成影响，只会对新的用户连接生效 关于该命令的详细介绍，请参见“安全命令参考”中的“AAA”

1.3 配置Stelnet客户端

1.3.1 Stelnet客户端配置任务简介

表1-13 Stelnet 客户端配置任务简介

配置任务	说明	详细配置
生成本地DSA、ECDSA或RSA密钥对	仅采用publickey、password-publickey或any认证方式时必选	1.3.2
配置Stelnet客户端发送SSH报文使用的源IP地址	可选	1.3.3
建立与Stelnet服务器端的连接	必选	1.3.4

1.3.2 生成本地DSA、ECDSA或RSA密钥对

客户端采用 publickey、password-publickey 或 any 认证方式时，需要生成本地密钥对。

客户端生成本地 DSA、ECDSA 或 RSA 密钥对，需要注意的是：

- SSH 仅支持默认名称的本地 DSA、ECDSA 或 RSA 密钥对，不支持指定名称的本地 DSA、ECDSA 或 RSA 密钥对。关于密钥对生成命令的相关介绍请参见“安全命令参考”中的“公钥管理”。
- 生成 DSA 密钥对时，要求输入的密钥模数的长度必须小于 2048 比特。
- SSH 客户端只支持 secp256r1 类型的 ECDSA 密钥对，所以生成 SSH 客户端密钥对时必须为 secp256r1 类型。

表1-14 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、ECDSA或RSA密钥对	**public-key local create** { **dsa** | **ecdsa secp256r1** | **rsa** }	缺省情况下，不存在任何DSA、ECDSA、RSA密钥对

1.3.3 配置Stelnet客户端发送SSH报文使用的源IP地址

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 接口的 IP 地址作为源 IP 地址。

表1-15 配置 Stelnet 客户端发送 SSH 报文使用的源 IP 地址

操作		命令	说明
进入系统视图		**system-view**	-
配置Stelnet客户端发送SSH报文使用的源IP地址	配置Stelnet客户端发送SSH报文使用的源IPv4地址	**ssh client source** { **interface** *interface-type interface-number* | **ip** *ip-address* }	二者必选其一 缺省情况下，IPv4 Stelnet客户端采用设备路由指定的SSH报文出接口主IP地址作为源IP地址；IPv6 Stelnet客户端采用设备自动选择的IPv4地址作为源IP地址
	配置Stelnet客户端发送SSH报文使用的源IPv6地址	**ssh client ipv6 source** { **interface** *interface-type interface-number* | **ipv6** *ipv6-address* }	

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等。

Stelnet 客户端访问服务器时，需要通过本地保存的服务器端的主机公钥来验证服务器的身份。设备作为 Stelnet 客户端时，默认支持首次认证，即当 Stelnet 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。

表1-16 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	**ssh2** *server* [*port-number*] [**identity-key** { **dsa** | **ecdsa** | **rsa** } | **prefer-compress zlib** | **prefer-ctos-cipher** { **3des-cbc** | **aes128-cbc** | **aes256-cbc** | **des-cbc** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** } | **prefer-kex** { **dh-group-exchange-sha1** | **dh-group1-sha1** | **dh-group14-sha1** } | **prefer-stoc-cipher** { **3des-cbc** | **aes128-cbc** | **aes256-cbc** | **des-cbc** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** }] * [**dscp** *dscp-value* | **escape** *character* | **public-key** *keyname* | **source** { **interface** *interface-type interface-number* | **ip** *ip-address* }] *	二者至少选其一 请在用户视图下执行本命令
	与IPv6 Stelnet服务器端建立连接	**ssh2 ipv6** *server* [*port-number*] [**-i** *interface-type interface-number*] [**identity-key** { **dsa** | **ecdsa** | **rsa** } | **prefer-compress zlib** | **prefer-ctos-cipher** { **3des-cbc** | **aes128-cbc** | **aes256-cbc** | **des-cbc** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** } | **prefer-kex** { **dh-group-exchange-sha1** | **dh-group1-sha1** | **dh-group14-sha1** } | **prefer-stoc-cipher** { **3des-cbc** | **aes128-cbc** | **aes256-cbc** | **des-cbc** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** }] * [**dscp** *dscp-value* | **escape** *character* | **public-key** *keyname* | **source** { **interface** *interface-type interface-number* | **ipv6** *ipv6-address* }] *	

1.4 配置SFTP客户端

1.4.1 SFTP客户端配置任务简介

表1-17 SFTP 客户端配置任务简介

配置任务	说明	详细配置
生成本地DSA、ECDSA或RSA密钥对	仅采用publickey、password-publickey或any认证方式时必选	1.4.2
配置SFTP客户端发送SFTP报文使用的源IP地址	可选	1.4.3
建立与SFTP服务器端的连接	必选	1.4.4
SFTP目录操作	可选	1.4.5
SFTP文件操作	可选	1.4.6
显示帮助信息	可选	1.4.7

配置任务	说明	详细配置
终止与SFTP服务器端的连接	可选	1.4.8

1.4.2 生成本地DSA、ECDSA或RSA密钥对

客户端采用 publickey、password-publickey 或 any 认证方式时，需要生成本地密钥对。

客户端生成本地 DSA、ECDSA 或 RSA 密钥对，需要注意的是：

- SSH 仅支持默认名称的本地 DSA、ECDSA 或 RSA 密钥对，不支持指定名称的本地 DSA、ECDSA 或 RSA 密钥对。关于密钥对生成命令的相关介绍请参见“安全命令参考”中的“公钥管理”。
- 生成 DSA 密钥对时，要求输入的密钥模数的长度必须小于 2048 比特。
- SSH 客户端只支持 secp256r1 类型的 ECDSA 密钥对，所以生成 SSH 客户端密钥对时必须为 secp256r1 类型。

表1-18 生成本地 DSA、ECDSA 或 RSA 密钥对

操作	命令	说明
进入系统视图	**system-view**	-
生成本地DSA、ECDSA或RSA密钥对	**public-key local create { dsa | ecdsa secp256r1 | rsa }**	缺省情况下，不存在任何DSA、ECDSA和RSA密钥对

1.4.3 配置SFTP客户端发送SFTP报文使用的源IP地址

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 接口的 IP 地址作为源 IP 地址。

表1-19 配置 SFTP 客户端发送 SFTP 报文使用的源 IP 地址

操作		命令	说明
进入系统视图		**system-view**	-
配置SFTP客户端发送SFTP报文使用的源IP地址	配置SFTP客户端发送SFTP报文使用的源IPv4地址	**sftp client source { ip** *ip-address* **| interface** *interface-type interface-number* **}**	二者必选其一 缺省情况下，IPv4客户端采用设备路由指定的SFTP报文的出接口主IP地址作为源IP地址；IPv6客户端采用设备自动选择的IPv6地址作为源IP地址
	配置SFTP客户端发送SFTP报文使用的源IPv6地址	**sftp client ipv6 source { ipv6** *ipv6-address* **| interface** *interface-type interface-number* **}**	

1.4.4 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等。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。

SFTP 客户端访问服务器时，需要通过本地保存的服务器端的主机公钥来验证服务器的身份。设备作为 SFTP 客户端时，默认支持首次认证，即当 SFTP 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。

表1-20 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	**sftp** *server* [*port-number*] [**identity-key** { **dsa** | **ecdsa** | **rsa** } | **prefer-compress zlib** | **prefer-ctos-cipher** { **3des-cbc** | **aes128-cbc** | **aes256-cbc** | **des-cbc** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** } | **prefer-kex** { **dh-group-exchange-sha1** | **dh-group1-sha1** | **dh-group14-sha1** } | **prefer-stoc-cipher** { **3des-cbc** | **aes128-cbc** | **aes256-cbc** | **des-cbc** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** }] * [**dscp** *dscp-value* | **public-key** *keyname* | **source** { **interface** *interface-type interface-number* | **ip** *ip-addres*}] *	二者至少选其一 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	**sftp ipv6** *server* [*port-number*] [**-i** *interface-type interface-number*] [**identity-key** { **dsa** | **ecdsa** | **rsa** } | **prefer-compress zlib** | **prefer-ctos-cipher** { **3des-cbc** | **aes128-cbc** | **aes256-cbc** | **des-cbc** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** } | **prefer-kex** { **dh-group-exchange-sha1** | **dh-group1-sha1** | **dh-group14-sha1** } | **prefer-stoc-cipher** { **3des-cbc** | **aes128-cbc** | **aes256-cbc** | **des-cbc** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** }] * [**dscp** *dscp-value* | **public-key** *keyname* | **source** { **interface** *interface-type interface-number* | **ipv6** *ipv6-addres*}] *	

1.4.5 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1-21 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1.4.4	-
改变远程SFTP服务器上的工作路径	**cd** [*remote-path*]	-

操作	命令	说明
返回到上一级目录	**cdup**	-
显示远程SFTP服务器上的当前工作目录	**pwd**	-
显示指定目录下的文件列表	**dir** [**-a** | **-l**] [*remote-path*]	**dir**和**ls**两条命令的作用相同
	ls [**-a** | **-l**] [*remote-path*]	
改变SFTP服务器上指定的目录的名字	**rename** *old-name new-name*	-
在远程SFTP服务器上创建新的目录	**mkdir** *remote-path*	-
删除SFTP服务器上指定的目录	**rmdir** *remote-path*	-

1.4.6 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、显示文件列表和删除文件。

表1-22 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1.4.4	-
改变SFTP服务器上指定的文件的名字	**rename** *old-name new-name*	-
从远程服务器上下载文件并存储在本地	**get** *remote-file* [*local-file*]	-
将本地的文件上传到远程SFTP服务器	**put** *local-file* [*remote-file*]	-
显示指定目录下的文件	**dir** [**-a** | **-l**] [*remote-path*]	**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*	**delete**和**remove**两条命令的功能相同
	remove *remote-file*	

1.4.7 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1-23 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1.4.4	-
显示SFTP客户端命令的帮助信息	**help**	二者选其一 **help**和？的功能相同
	？	

1.4.8 终止与SFTP服务器的连接

表1-24 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1.4.4	-
终止与SFTP服务器的连接，并退回用户视图	**bye**	三者选其一 **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 生成本地DSA或RSA密钥对

客户端采用 publickey、password-publickey 或 any 认证方式时，需要生成本地密钥对。

客户端生成本地 DSA 或 RSA 密钥对，需要注意的是：

- SSH 仅支持默认名称的本地 DSA、ECDSA 或 RSA 密钥对，不支持指定名称的本地 DSA、ECDSA 或 RSA 密钥对。关于密钥对生成命令的相关介绍请参见“安全命令参考”中的“公钥管理”。
- 生成 DSA 密钥对时，要求输入的密钥模数的长度必须小于 2048 比特。
- SSH 客户端只支持 secp256r1 类型的 ECDSA 密钥对，所以生成 SSH 客户端密钥对时必须为 secp256r1 类型。

表1-25 生成本地 DSA、ECDSA 或 RSA 密钥对

操作	命令	说明
进入系统视图	**system-view**	-
生成本地DSA、ECDSA或RSA密钥对	**public-key local create** { **dsa** | **ecdsa secp256r1** | **rsa** }	缺省情况下，不存在任何DSA、ECDSA和RSA密钥对

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。SCP 客户端访问服务器时，需要通过本地保存的服务器端的主机公钥来验证服务器的身份。设备作为 SCP 客户端时，默认支持首次认证，即当 SCP 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。

表1-26 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	与远程IPv4 SCP服务器建立连接，并进行文件传输	**scp** *server* [*port-number*] { **put** | **get** } *source-file-name* [*destination-file-name*] [**identity-key** { **dsa** | **ecdsa** | **rsa** } | **prefer-compress** **zlib** | **prefer-ctos-cipher** { **3des-cbc** | **aes128-cbc** | **aes256-cbc** | **des-cbc** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** } | **prefer-kex** { **dh-group-exchange-sha1** | **dh-group1-sha1** | **dh-group14-sha1** } | **prefer-stoc-cipher** { **3des-cbc** | **aes128-cbc** | **aes256-cbc** | **des-cbc** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** }] * [**public-key** *keyname* | **source** { **interface** *interface-type interface-number* | **ip** *ip-address* }] *	二者至少选其一 请在用户视图下执行此命令
	与远程IPv6 SCP服务器建立连接，并进行文件传输	**scp** **ipv6** *server* [*port-number*] [**-i** *interface-type interface-number*] { **put** | **get** } *source-file-name* [*destination-file-name*] [**identity-key** { **dsa** | **ecdsa** | **rsa** } | **prefer-compress** **zlib** | **prefer-ctos-cipher** { **3des-cbc** | **aes128-cbc** | **aes256-cbc** | **des-cbc** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** } | **prefer-kex** { **dh-group-exchange-sha1** | **dh-group1-sha1** | **dh-group14-sha1** } | **prefer-stoc-cipher** { **3des-cbc** | **aes128-cbc** | **aes256-cbc** | **des-cbc** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** }] * [**public-key** *keyname* | **source** { **interface** *interface-type interface-number* | **ipv6** *ipv6-address* }] *	

1.6 配置SSH2协议算法集

1.6.1 配置SSH2 协议密钥交换算法优先列表

该配置任务用来配置 SSH2 协议所能采用的密钥交换算法优先列表，该算法列表不影响 SSH1 会话。该密钥交换算法优先列表用于建立 Stelnet、SFTP、SCP 会话过程中 SSH 服务器和 SSH 客户端进行算法协商。

操作	命令	说明
进入系统视图	**system-view**	-
配置SSH2协议密钥交换算法优先列表	**ssh2 algorithm key-exchange { dh-group-exchange-sha1 | dh-group14-sha1 | dh-group1-sha1 } ***	缺省情况下，SSH2协议所采用的密钥交换算法优先列表为：**dh-group-exchange-sha1**、**dh-group14-sha1**、**dh-group1-sha1**

1.6.2 配置SSH2 协议主机签名算法优先列表

该配置任务用来配置 SSH2 协议所能采用的主机签名算法优先列表，该算法列表不影响 SSH1 会话。该算法优先列表用于建立 Stelnet、SFTP、SCP 会话过程中 SSH 服务器和 SSH 客户端进行算法协商。

操作	命令	说明
进入系统视图	**system-view**	-
配置SSH2协议主机签名算法优先列表	**ssh2 algorithm public-key { ecdsa | dsa | rsa } ***	缺省情况下，SSH2协议所采用的主机签名算法优先列表为：**ecdsa、dsa、rsa**

1.6.3 配置SSH2 协议加密算法优先列表

该配置任务用来配置 SSH2 协议所能采用的加密算法优先列表，该算法列表不影响 SSH1 会话。该加密算法优先列表用于建立 Stelnet、SFTP、SCP 会话过程中 SSH 服务器和 SSH 客户端进行算法协商。

操作	命令	说明
进入系统视图	**system-view**	-
配置SSH2协议加密算法优先列表	**ssh2 algorithm cipher { aes128-cbc | aes256-cbc | 3des-cbc | des-cbc } ***	缺省情况下，SSH2协议所采用的加密算法优先列表为：**aes128-cbc 、 aes256-cbc 、 3des-cbc des-cbc**

1.6.4 配置SSH2 协议MAC算法优先列表

该配置任务配置 SSH2 协议所能采用的 MAC 算法优先列表，该算法列表不影响 SSH1 会话。该 MAC 算法优先列表用于建立 Stelnet、SFTP、SCP 会话过程中 SSH 服务器和 SSH 客户端进行算法协商。

操作	命令	说明
进入系统视图	**system-view**	-
配置SSH2协议MAC算法优先列表	**ssh2 algorithm mac { sha1 | sha1-96 | md5 | md5-96 } ***	缺省情况下，SSH2协议所采用的密钥交换算法优先列表为：**sha1、sha1-96、md5、md5-96**

1.7 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1-27 SSH 显示和维护

操作	命令
显示SFTP客户端的源IP地址配置	**display sftp client source**
显示Stelnet客户端的源IP地址配置	**display ssh client source**
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** { **session** [**slot** *slot-number*] | **status** }
在SSH服务器端显示SSH用户信息	**display ssh user-information** [*username*]
显示本地密钥对中的公钥部分	**display public-key local** { **dsa** | **ecdsa** | **rsa** } **public** [**name** *publickey-name*]
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*]
显示设备上配置的SSH2协议使用的算法优先列表	**display ssh2 algorithm**

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”。

1.8 Stelnet典型配置举例

说明

请确保无线控制器和客户端路由可达。

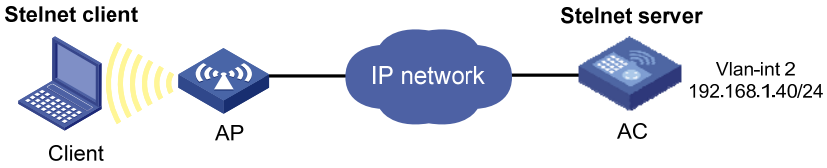
1.8.1 设备作为Stelnet服务器配置举例（password认证）

1. 组网需求

- 用户可以通过 Client 上运行的 Stelnet 客户端软件（SSH2 版本）安全地登录到 AC 上，并被授予用户角色 network-admin 进行配置管理；
- AC 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1-1 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。

```
<AC> system-view
[Switch] public-key local create rsa
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.....................++++++
.................++++++
..++++++++
............++++++++
Create the key pair successfully.
```

生成 DSA 密钥对。

```
[AC] public-key local create dsa
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.++++++++++++++++++++++++++++++++++++++++++++++++++*
........+......+.....+.................................+
...+.................+.........+...+.
Create the key pair successfully.
```

生成 ECDSA 密钥对。

```
[AC] public-key local create ecdsa secp256r1
Generating Keys...
.
Create the key pair successfully.
```

使能 Stelnet 服务器功能。

```
[AC] ssh server enable
```

配置 VLAN 接口 2 的 IP 地址，客户端将通过该地址连接 Stelnet 服务器。

```
[AC] interface vlan-interface 2
[AC-Vlan-interface2] ip address 192.168.1.40 255.255.255.0
```

```
[AC-Vlan-interface2] quit
```

设置 Stelnet 客户端登录用户线的认证方式为 AAA 认证。

```
[AC] line vty 0 15
[AC-line-vty0-15] authentication-mode scheme
[AC-line-vty0-15] quit
```

创建设备管理类本地用户 client001，并设置密码为明文 aabbcc，服务类型为 SSH，用户角色为 network-admin。

```
[AC] local-user client001 class manage
[AC-luser-manage-client001] password simple aabbcc
[AC-luser-manage-client001] service-type ssh
[AC-luser-manage-client001] authorization-attribute user-role network-admin
[AC-luser-manage-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）

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

(2) Stelnet 客户端建立与 Stelnet 服务器的连接

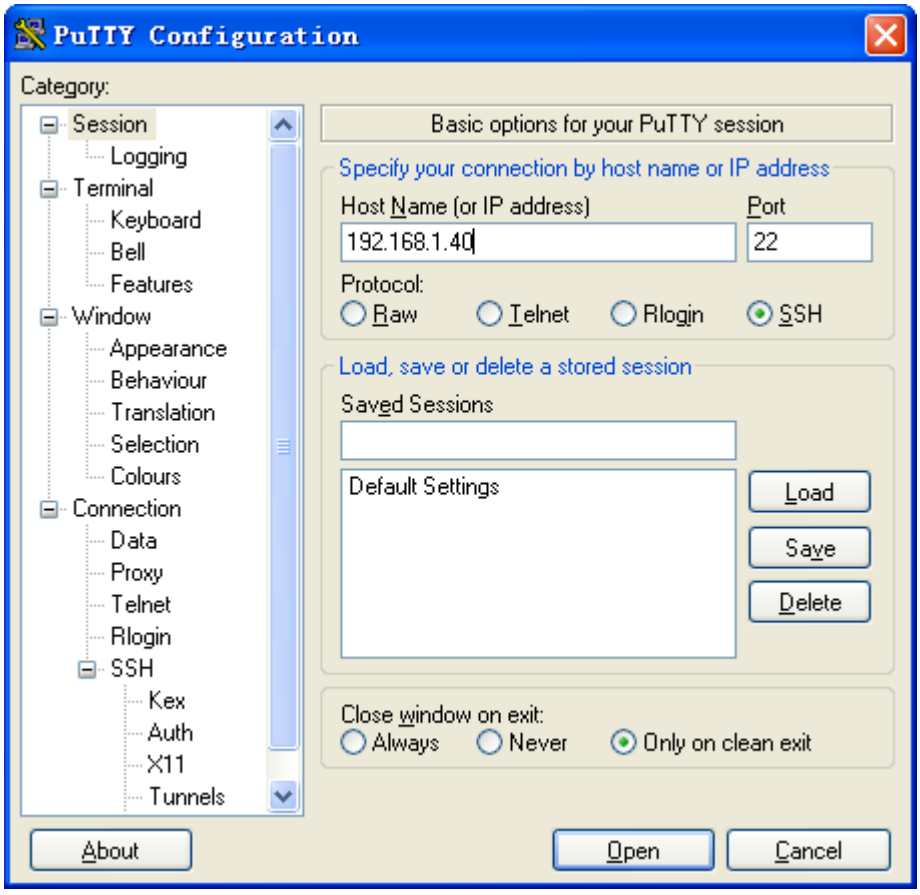
说明

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 服务器端的连接。

打开PuTTY.exe程序，出现如 图 1-2 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1-2 Stelnet 客户端配置界面



在 图 1-2 中，单击<Open>按钮。按提示输入用户名client001 及密码aabbcc，即可进入AC的配置界面。

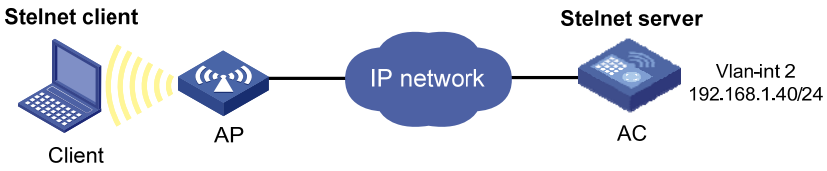
1.8.2 设备作为Stelnet服务器配置举例（publickey认证）

1. 组网需求

- 用户可以通过 Client 上运行的 Stelnet 客户端软件（SSH2 版本）安全地登录到 AC 上，并被授予用户角色 network-admin 进行配置管理；
- AC 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1-3 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，因此建议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

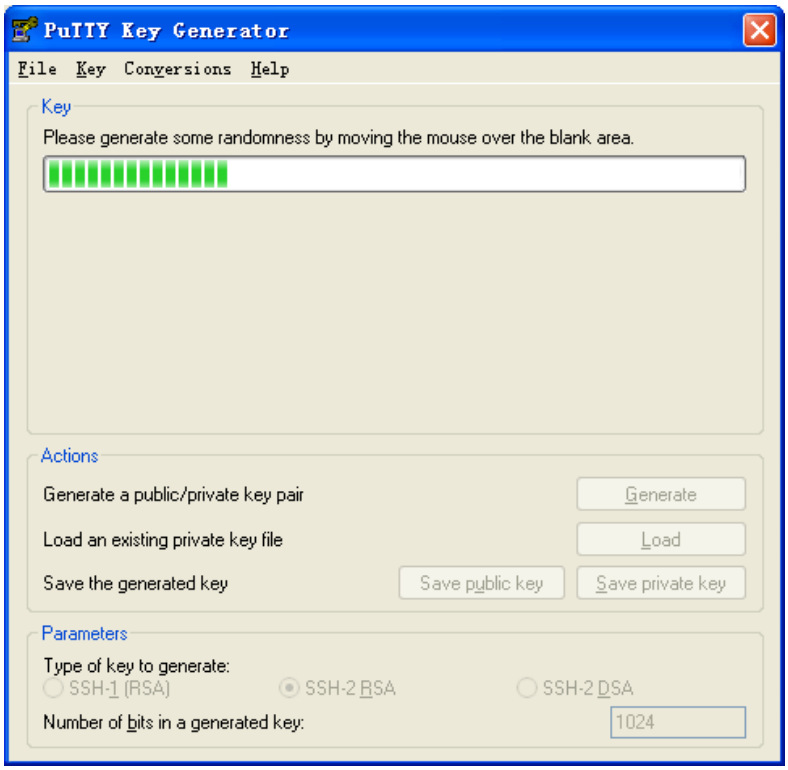
生成 RSA 密钥对。

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

图1-4 生成客户端密钥（步骤 1）

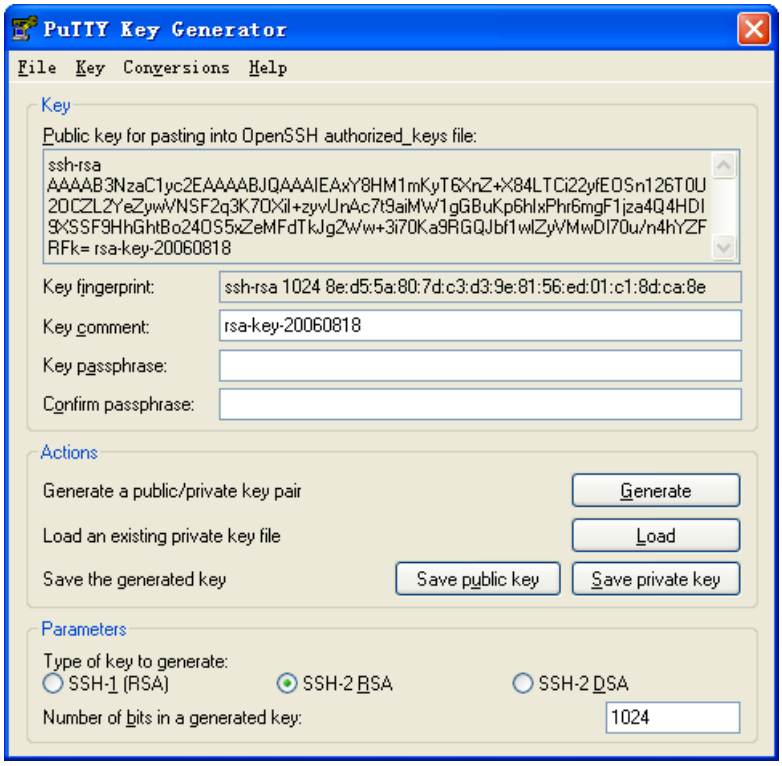
在产生密钥对的过程中需不停地移动鼠标，鼠标移动仅限于下图蓝色框中除绿色标记进程条外的地方，否则进程条的显示会不动，密钥对将停止产生，见 图 1-5。

图1-5 生成客户端密钥（步骤 2）



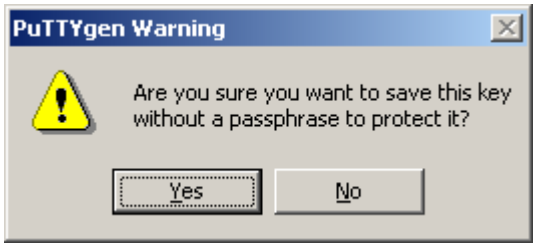
密钥对产生后，点击<Save public key>，输入存储公钥的文件名 key.pub，点击<保存>按钮。

图1-6 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1-7 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。

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

生成 DSA 密钥对。

```
[AC] public-key local create dsa
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.++++++++++++++++++++++++++++++++++++++++++++++++++*
........+......+.....+.................................+
...+.................+.........+...+
Create the key pair successfully.
```

生成 ECDSA 密钥对。

```
[AC] public-key local create ecdsa secp256r1
Generating Keys...
.
Create the key pair successfully.
```

使能 Stelnet 服务器功能。

```
[AC] ssh server enable
```

配置 VLAN 接口 2 的 IP 地址，客户端将通过该地址连接 Stelnet 服务器。

```
[AC] interface vlan-interface 2
[AC-Vlan-interface2] ip address 192.168.1.40 255.255.255.0
[AC-Vlan-interface2] quit
```

设置 Stelnet 客户端登录用户线的认证方式为 AAA 认证。

```
[AC] line vty 0 15
[AC-line-vty0-15] authentication-mode scheme
[AC-line-vty0-15] quit
```

从文件 key.pub 中导入远端的公钥，并命名为 switchkey。

```
[AC] public-key peer ACkey import sshkey key.pub
```

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

```
[AC] ssh user client002 service-type stelnet authentication-type publickey assign publickey
ackey
```

创建设备管理类本地用户 client002，并设置服务类型为 SSH，用户角色为 network-admin。

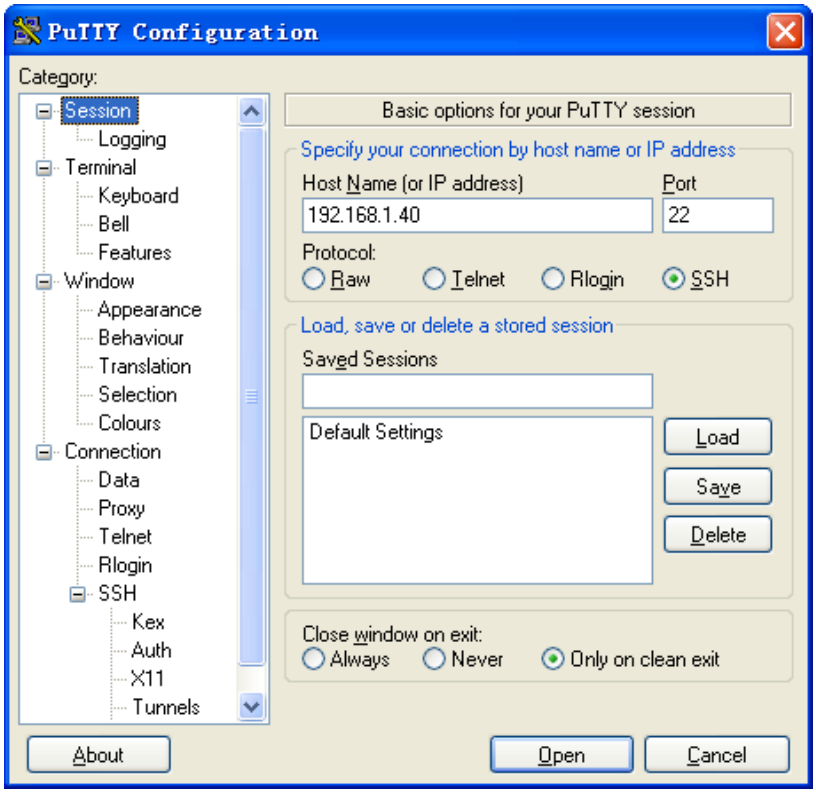
```
[AC] local-user client002 class manage
[AC-luser-manage-client002] service-type ssh
[AC-luser-manage-client002] authorization-attribute user-role network-admin
[AC-luser-manage-client002] quit
```

(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。

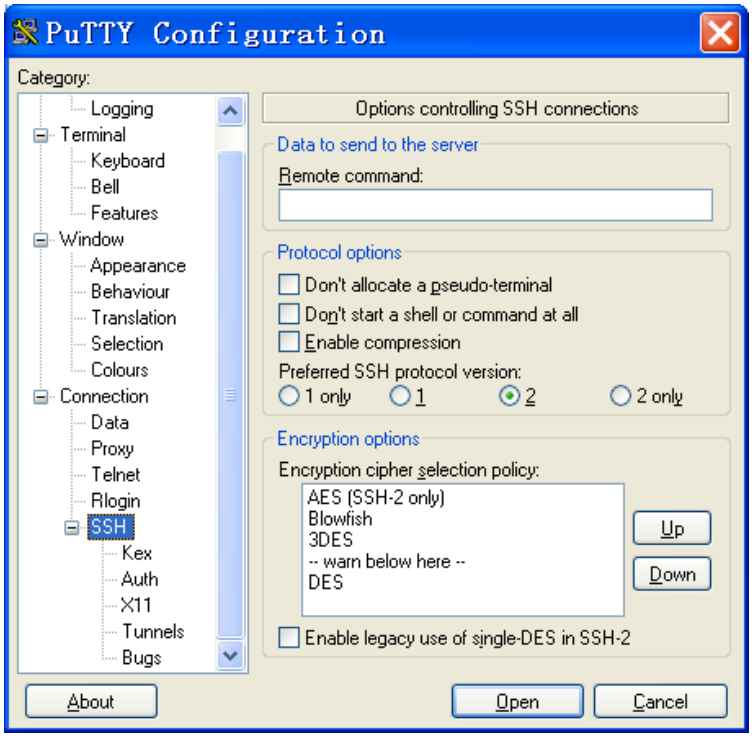
打开PuTTY.exe程序，出现如 图 1-8 所示的客户端配置界面。在“Host Name（or IP address）”文本框中输入Stelnet服务器的IP地址为 192.168.1.40。

图1-8 Stelnet 客户端配置界面



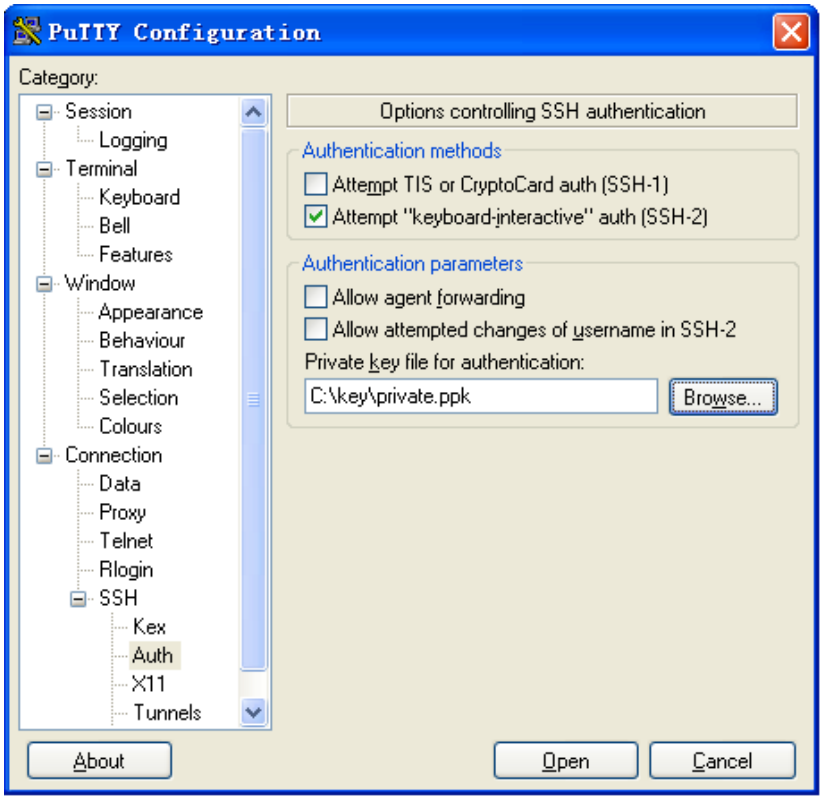
单击左侧导航栏“Connection->SSH”，出现如 图 1-9 的界面。选择“Preferred SSH protocol version”为 “2”。

图1-9 Stelnet 客户端配置界面



单击左侧导航栏“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



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

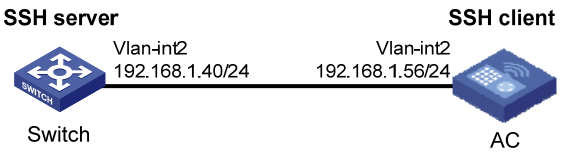
1.8.3 设备作为Stelnet客户端配置举例（password认证）

1. 组网需求

- 配置 AC 作为 Stelnet 客户端，用户能够通过 AC 安全地登录到 Switch 上，并被授予用户角色 network-admin 进行配置管理。
- Switch 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 Switch 上。

2. 组网图

图1-11 设备作为 Stelnet 客户端配置组网图



3. 配置步骤

(1) 配置 Stelnet 服务器

生成 RSA 密钥对。

```
<Switch> system-view
```

```
[Switch] public-key local create rsa
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.....................++++++
.................++++++
..++++++++
............++++++++
Create the key pair successfully.
```

生成 DSA 密钥对。

```
[Switch] public-key local create dsa
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.++++++++++++++++++++++++++++++++++++++++++++++++*
........+......+.....+................................+
...+.................+.........+...+
Create the key pair successfully.
```

生成 ECDSA 密钥对。

```
[Switch] public-key local create ecdsa secp256r1
Generating Keys...
.
Create the key pair successfully.
```

使能 Stelnet 服务器功能。

```
[Switch] ssh server enable
```

配置 VLAN 接口 2 的 IP 地址，客户端将通过该地址连接 Stelnet 服务器。

```
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] ip address 192.168.1.40 255.255.255.0
[Switch-Vlan-interface2] quit
```

设置 Stelnet 客户端登录用户线的认证方式为 AAA 认证。

```
[Switch] line vty 0 15
[Switch-line-vty0-15] authentication-mode scheme
[Switch-line-vty0-15] quit
```

创建设备管理类本地用户 client001，并设置密码为明文 aabbcc，服务类型为 SSH，用户角色为 network-admin。

```
[Switch] local-user client001 class manage
[Switch-luser-manage-client001] password simple aabbcc
[Switch-luser-manage-client001] service-type ssh
[Switch-luser-manage-client001] authorization-attribute user-role network-admin
[Switch-luser-manage-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）

```
[Switch] 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 VLAN 接口 2 的 IP 地址。

```
<AC> system-view
[AC] interface vlan-interface 2
[AC-Vlan-interface2] ip address 192.168.1.56 255.255.255.0
[AC-Vlan-interface2] quit
[AC] quit
```

- 客户端本地没有服务器端的主机公钥，首次与服务器建立连接

建立到服务器 192.168.1.40 的 SSH 连接，选择在不认证服务器的情况下继续访问服务网，并在客户端保存服务器端的本地公钥。

```
<AC> ssh2 192.168.1.40
Username: client001
Press CTRL+C to abort.
Connecting to 192.168.1.40 port 22.
The server is not authenticated. Continue? [Y/N]:y
Do you want to save the server public key? [Y/N]:y
client001@192.168.1.40's password:

Enter a character ~ and a dot to abort.

************************************************************************
* Copyright (c) 2004-2017 New H3C Technologies Co., Ltd. All rights reserved.*
* Without the owner's prior written consent,                           *
* no decompiling or reverse-engineering shall be allowed.              *
************************************************************************

<Switch>
```

输入正确的密码之后，即可成功登录到 Switch 上。由于选择在本地保存服务器端的主机公钥，下次用户登录 Switch 时直接输入正确密码即可成功登录。

- 客户端配置服务器端的主机公钥后，与服务器建立连接

在客户端配置 SSH 服务器端的主机公钥。在公钥视图输入服务器端的主机公钥，即在服务器端通过 **display public-key local dsa public** 命令显示的公钥内容。

```
[AC] public-key peer key1
Enter public key view. Return to system view with "peer-public-key end" command.
[AC-pkey-public-key-key1]308201B73082012C06072A8648CE3804013082011F0281810
0D757262C4584C44C211F18BD96E5F0
[AC-pkey-public-key-key1]61C4F0A423F7FE6B6B85B34CEF72CE14A0D3A5222FE08CECE
65BE6C265854889DC1EDBD13EC8B274
[AC-pkey-public-key-key1]DA9F75BA26CCB987723602787E922BA84421F22C3C89CB9B0
6FD60FE01941DDD77FE6B12893DA76E
[AC-pkey-public-key-key1]EBC1D128D97F0678D7722B5341C8506F358214B16A2FAC4B3
68950387811C7DA33021500C773218C
[AC-pkey-public-key-key1]737EC8EE993B4F2DED30F48EDACE915F0281810082269009E
14EC474BAF2932E69D3B1F18517AD95
[AC-pkey-public-key-key1]94184CCDFCEAE96EC4D5EF93133E84B47093C52B20CD35D02
```

```
492B3959EC6499625BC4FA5082E22C5
[AC-pkey-public-key-key1]B374E16DD00132CE71B020217091AC717B612391C76C1FB2E
88317C1BD8171D41ECB83E210C03CC9
[AC-pkey-public-key-key1]B32E810561C21621C73D6DAAC028F4B1585DA7F42519718CC
9B09EEF0381840002818000AF995917
[AC-pkey-public-key-key1]E1E570A3F6B1C2411948B3B4FFA256699B3BF871221CC9C5D
F257523777D033BEE77FC378145F2AD
[AC-pkey-public-key-key1]D716D7DB9FCABB4ADBF6FB4FDB0CA25C761B308EF53009F71
01F7C62621216D5A572C379A32AC290
[AC-pkey-public-key-key1]E55B394A217DA38B65B77F0185C8DB8095522D1EF044B465E
8716261214A5A3B493E866991113B2D
[AC-pkey-public-key-key1]485348
[AC-pkey-public-key-key1] peer-public-key end
[AC] quit
```

建立到服务器 192.168.1.40 的 SSH 连接，并指定服务器端的主机公钥。

```
<AC> ssh2 192.168.1.40 public-key key1
Username: client001
Press CTRL+C to abort.
Connecting to 192.168.1.40 port 22.
client001@192.168.1.40's password:
Enter a character ~ and a dot to abort.

******************************************************************************
* Copyright (c) 2004-2017 New H3C Technologies Co., Ltd. All rights reserved.*
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************

<Switch>
```

输入正确的密码之后，即可成功登录到 Switch B 上。

- 客户端本地已有服务器端的主机公钥，直接与服务器建立连接

```
<AC> ssh2 192.168.1.40
Username: client001
Press CTRL+C to abort.
Connecting to 192.168.1.40 port 22.
client001@192.168.1.40's password:
Enter a character ~ and a dot to abort.

******************************************************************************
* Copyright (c) 2004-2017 New H3C Technologies Co., Ltd. All rights reserved.*
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************

<Switch>
```

输入正确的密码之后，即可成功登录到 Switch B 上。

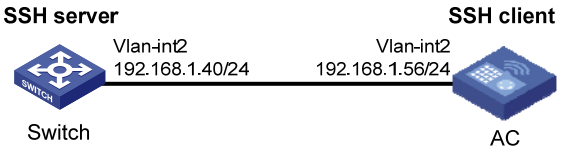
1.8.4 设备作为Stelnet客户端配置举例（publickey认证）

1. 组网需求

- 配置 AC 作为 Stelnet 客户端，用户能够通过 AC 安全地登录到 Switch 上，并被授予用户角色 network-admin 进行配置管理。
- Switch 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，因此需要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 VLAN 接口 2 的 IP 地址。

```
<AC> system-view
[AC] interface vlan-interface 2
[AC-Vlan-interface2] ip address 192.168.1.56 255.255.255.0
[AC-Vlan-interface2] quit
```

生成 DSA 密钥对。

```
[AC] public-key local create dsa
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.++++++++++++++++++++++++++++++++++++++++++++++++++*
........+......+.....+.....................................+
...+.................+..........+...+
Create the key pair successfully.
```

将生成的 DSA 主机公钥导出到指定文件 key.pub 中。

```
[AC] public-key local export dsa ssh2 key.pub
[AC] 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。

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

生成 DSA 密钥对。

```
[Switch] public-key local create dsa
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.++++++++++++++++++++++++++++++++++++++++++++++++++*
........+......+.....+.....................................+
...+.................+.........+...+
Create the key pair successfully.
```

生成 ECDSA 密钥对。

```
[Switch] public-key local create ecdsa secp256r1
Generating Keys...
.
Create the key pair successfully.
```

使能 Stelnet 服务器功能。

```
[Switch] ssh server enable
```

配置 VLAN 接口 2 的 IP 地址，客户端将通过该地址连接 SSH 服务器。

```
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] ip address 192.168.1.40 255.255.255.0
[Switch-Vlan-interface2] quit
```

设置 Stelnet 客户端登录用户线的认证方式为 AAA 认证。

```
[Switch] line vty 0 15
[Switch-line-vty0-15] authentication-mode scheme
[Switch-line-vty0-15] quit
```

从文件 key.pub 中导入远端的公钥，并命名为 ackey。

```
[Switch] public-key peer ackey import sshkey key.pub
```

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

```
[Switch] ssh user client002 service-type stelnet authentication-type publickey assign
publickey ackey
```

创建设备管理类本地用户 client002，并设置服务类型为 SSH，用户角色为 network-admin。

```
[Switch] local-user client002 class manage
[Switch-luser-manage-client002] service-type ssh
[Switch-luser-manage-client002] authorization-attribute user-role network-admin
[Switch-luser-manage-client002] quit
```

(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。

```
<AC> ssh2 192.168.1.40
Username: client002
Press CTRL+C to abort.
Connecting to 192.168.1.40 port 22.
The server is not authenticated. Continue? [Y/N]:y
Do you want to save the server public key? [Y/N]:n
Enter a character ~ and a dot to abort.

******************************************************************************
* Copyright (c) 2004-2017 New H3C Technologies Co., Ltd. All rights reserved.*
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************

<Switch>
```

由于本地未保存服务器端的主机公钥，因此在选择继续访问服务器之后，即可成功登录到 Switch B 上。

1.9 SFTP典型配置举例

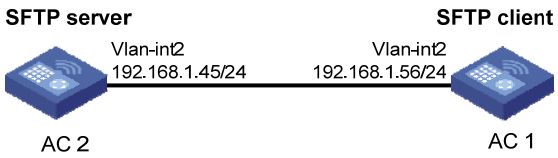
1.9.1 设备作为SFTP服务器配置举例（password认证）

1. 组网需求

- AC 1 和 AC 2 之间建立 SSH 连接，AC 1 作为 SFTP 客户端登录到 AC 2，，并被授予用户角色 network-admin 进行文件管理和文件传送等操作；
- AC 2 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。

```
<AC2> system-view
```

```
[AC2] public-key local create rsa
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.....................++++++
.................++++++
..++++++++
............++++++++
Create the key pair successfully.
```

生成 DSA 密钥对。

```
[AC2] public-key local create dsa
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.++++++++++++++++++++++++++++++++++++++++++++++++*
........+......+.....+.................................+
...+.................+.........+...+
Create the key pair successfully.
```

生成 ECDSA 密钥对。

```
[AC2] public-key local create ecdsa secp256r1
Generating Keys...
.
Create the key pair successfully.
```

启动 SFTP 服务器。

```
[AC2] sftp server enable
```

配置 VLAN 接口 2 的 IP 地址，客户端将通过该地址连接 SSH 服务器。

```
[AC2] interface vlan-interface 2
[AC2-Vlan-interface2] ip address 192.168.1.45 255.255.255.0
[AC2-Vlan-interface2] quit
```

创建设备管理类本地用户 client002，并设置密码为明文 aabbcc，服务类型为 SSH，用户角色为 network-admin，工作目录为 cfa0:/。

```
[AC2] local-user client002 class manage
[AC2-luser-manage-client002] password simple aabbcc
[AC2-luser-manage-client002] service-type ssh
[AC2-luser-manage-client002] authorization-attribute user-role network-admin
work-directory cfa0:/
[AC2-luser-manage-client002] quit
```

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

```
[AC2] 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。

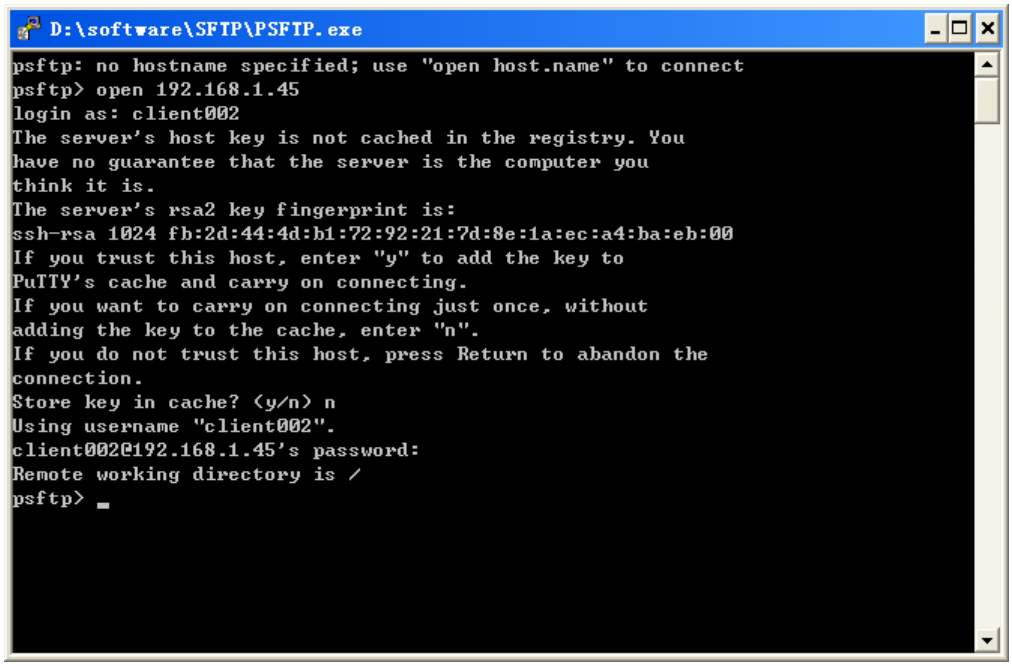
建立与 SFTP 服务器的连接。

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



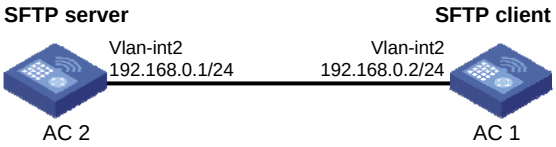
1.9.2 设备作为SFTP客户端配置举例（publickey认证）

1. 组网需求

- 配置 AC 1 作为 SFTP 客户端，用户能够通过 AC 1 安全地登录到 AC 2 上，并被授予用户角色 network-admin 进行文件管理和文件传送等操作。
- AC 2 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 VLAN 接口 2 的 IP 地址。

```
<AC1> system-view
[AC1] interface vlan-interface 2
[AC1-Vlan-interface2] ip address 192.168.0.2 255.255.255.0
[AC1-Vlan-interface2] quit
```

生成 RSA 密钥对。

```
[AC1] public-key local create rsa
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.....................++++++
.................++++++
..++++++++
............++++++++
Create the key pair successfully.
```

将生成的 RSA 主机公钥导出到指定文件 pubkey 中。

```
[AC1] public-key local export rsa ssh2 pubkey
[AC1] 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。

```
<AC2> system-view
[AC2] public-key local create rsa
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
```

```
Input the modulus length [default = 1024]:
Generating Keys...
.....................++++++
...................++++++
..++++++++
............++++++++
Create the key pair successfully.
```

生成 DSA 密钥对。

```
[AC2] public-key local create dsa
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.++++++++++++++++++++++++++++++++++++++++++++++++*
........+......+.....+.....................................+
...+.................+.........+...+
Create the key pair successfully.
```

生成 ECDSA 密钥对。

```
[AC2] public-key local create ecdsa secp256r1
Generating Keys...
.
Create the key pair successfully.
```

启动 SFTP 服务器。

```
[AC2] sftp server enable
```

配置 VLAN 接口 2 的 IP 地址，客户端将通过该地址连接 SSH 服务器。

```
[AC2] interface vlan-interface 2
[AC2-Vlan-interface2] ip address 192.168.0.1 255.255.255.0
[AC2-Vlan-interface2] quit
```

从文件 pubkey 中导入远端的公钥，并命名为 switchkey。

```
[AC2] public-key peer switchkey 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 switchkey。

```
[AC2] ssh user client001 service-type sftp authentication-type publickey assign publickey
switchkey
```

创建设备管理类本地用户 client001，并设置服务类型为 SSH，用户角色为 network-admin，工作目录为 cfa0:/。

```
[AC2] local-user client001 class manage
[AC2-luser-manage-client001] service-type ssh
[AC2-luser-manage-client001] authorization-attribute user-role network-admin
work-directory cfa0:/
[AC2-luser-manage-client001] quit
```

(3) SFTP 客户端建立与 SFTP 服务器端的连接

与远程 SFTP 服务器建立连接，进入 SFTP 客户端视图。

```
<AC1> sftp 192.168.0.1 identity-key rsa
Username: client001
Press CTRL+C to abort.
```

```
Connecting to 192.168.0.1 port 22.
The server is not authenticated. Continue? [Y/N]:y
Do you want to save the server public key? [Y/N]:n
sftp>
```

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> dir -l
-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> delete z
Removing /z
sftp> dir -l
-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> mkdir new1
sftp> dir -l
-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> rename new1 new2
sftp> dir -l
-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> get pubkey2 public
Fetching / pubkey2 to public
/pubkey2                                    100% 225     1.4KB/s   00:00
```

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> put pu puk
Uploading pu to / puk
sftp> dir -l
-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>
```

退出 SFTP 客户端视图。

```
sftp> quit
<AC1>
```

1.10 SCP典型配置举例

1.10.1 SCP文件传输配置举例（password认证）

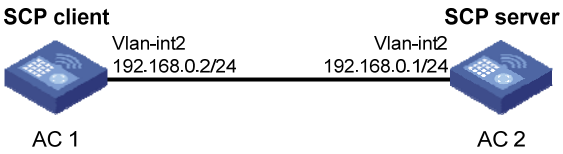
1. 组网需求

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

- 用户能够通过 Switch A 安全地安全地登录到 Switch B 上，并被授予用户角色 network-admin 与 Switch B 进行文件传输。
- Switch 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 Switch 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

生成 RSA 密钥对。

```
<AC2> system-view
[AC2] public-key local create rsa
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.....................++++++
.................++++++
..++++++++
............++++++++
Create the key pair successfully.
```

生成 DSA 密钥对。

```
[AC2] public-key local create dsa
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.++++++++++++++++++++++++++++++++++++++++++++++++++*
........+......+.....+.....................................+
...+.................+..........+...+.
Create the key pair successfully.
```

生成 ECDSA 密钥对。

```
[AC2] public-key local create ecdsa secp256r1
Generating Keys...
.
Create the key pair successfully.
```

使能 SCP 服务器功能。

```
[AC2] scp server enable
```

配置接口 VLAN 接口 2 的 IP 地址，客户端将通过该地址连接 SCP 服务器。

```
[AC2] interface vlan-interface 2
[AC2-Vlan-interface2] ip address 192.168.0.1 255.255.255.0
[AC2-Vlan-interface2] quit
```

创建设备管理类本地用户 client001，并设置密码为明文 aabbcc，服务类型为 SSH。

```
[AC2] local-user client001 class manage
[AC2-luser-manage-client001] password simple aabbcc
[AC2-luser-manage-client001] service-type ssh
[AC2-luser-manage-client001] authorization-attribute user-role network-admin
[AC2-luser-manage-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）

```
[AC2] ssh user client001 service-type scp authentication-type password
```

(2) 配置 SCP 客户端

配置接口 VLAN 2 的 IP 地址。

```
<AC1> system-view
[AC1] interface vlan-interface 2
[AC1-Vlan-interface2] ip address 192.168.0.2 255.255.255.0
[AC1-Vlan-interface2] quit
[AC1] 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。

```
<AC1> scp 192.168.0.1 get remote.bin local.bin
Username: client001
Press CTRL+C to abort.
Connecting to 192.168.0.1 port 22.
The server is not authenticated. Continue? [Y/N]:y
Do you want to save the server public key? [Y/N]:n
client001@192.168.0.1's password:
```

```
remote.bin                                    100% 2875     2.8KB/s   00:00
```

1.11 NETCONF over SSH典型配置举例

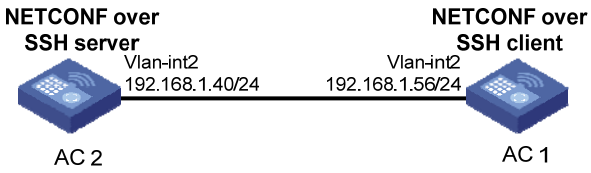
1.11.1 NETCONF over SSH配置举例（password认证）

1. 组网需求

- 用户可以通过AC 1上运行的支持NETCONF over SSH连接的SSH客户端软件（SSH2版本）安全地登录到 AC 2 上，并被授予用户角色 network-admin 进行配置管理。
- AC 2 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。
- 用户登录时的登录用户名为 client001，密码为 aabbcc。

2. 组网图

图1-17 设备作为 NETCONF over SSH 服务器配置组网图



3. 配置步骤

生成 RSA 密钥对。

```
<AC2> system-view
[AC2] public-key local create rsa
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.......................++++++
...................++++++
..++++++++
............++++++++
Create the key pair successfully.
```

生成 DSA 密钥对。

```
[AC2] public-key local create dsa
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.++++++++++++++++++++++++++++++++++++++++++++++++*
........+......+.....+.....................................+
...+.................+..........+...+.
Create the key pair successfully.
```

生成 ECDSA 密钥对。

```
[AC2] public-key local create ecdsa secp256r1
Generating Keys...
.
Create the key pair successfully.
```

使能 NETCONF over SSH 服务器功能。

```
[AC2] netconf ssh server enable
```

配置 VLAN 接口 2 的 IP 地址，客户端将通过该地址连接 NETCONF over SSH 服务器。

```
[AC2] interface vlan-interface 2
[AC2-Vlan-interface2] ip address 192.168.1.40 255.255.255.0
[AC2-Vlan-interface2] quit
```

设置 NETCONF over SSH 客户端登录用户线的认证方式为 AAA 认证。

```
[AC2] line vty 0 15
[AC2-line-vty0-15] authentication-mode scheme
[AC2-line-vty0-15] quit
```

创建设备管理类本地用户 client001，并设置密码为明文 aabbcc，服务类型为 SSH，用户角色为 network-admin。

```
[AC2] local-user client001 class manage
[AC2-luser-manage-client001] password simple aabbcc
[AC2-luser-manage-client001] service-type ssh
[AC2-luser-manage-client001] authorization-attribute user-role network-admin
[AC2-luser-manage-client001] quit
```

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

```
[AC2] ssh user client001 service-type netconf authentication-type password
```

4. 验证配置

用户通过支持 NETCONF over SSH 连接的客户端软件与 AC 2 建立 NETCONF over SSH 连接之后，可直接进入 AC 2 的 NETCONF 配置模式。

打开支持 NETCONF over SSH 登录方式的客户端软件，本文以 NetConf Browser 2015（Version3.1）工具为例。

在菜单栏中选择“File> Connect…”。

- “NETCONF version”选择“1.0”。
- “Host”文本框处输入设备 IP“192.168.100.49”。
- “Port”文本框处输入“830”。
- “Username”文本框处输入“client001”。
- 单击“Connect”按钮完成设置。

图1-18 通过 NetConf Browser 连接设备

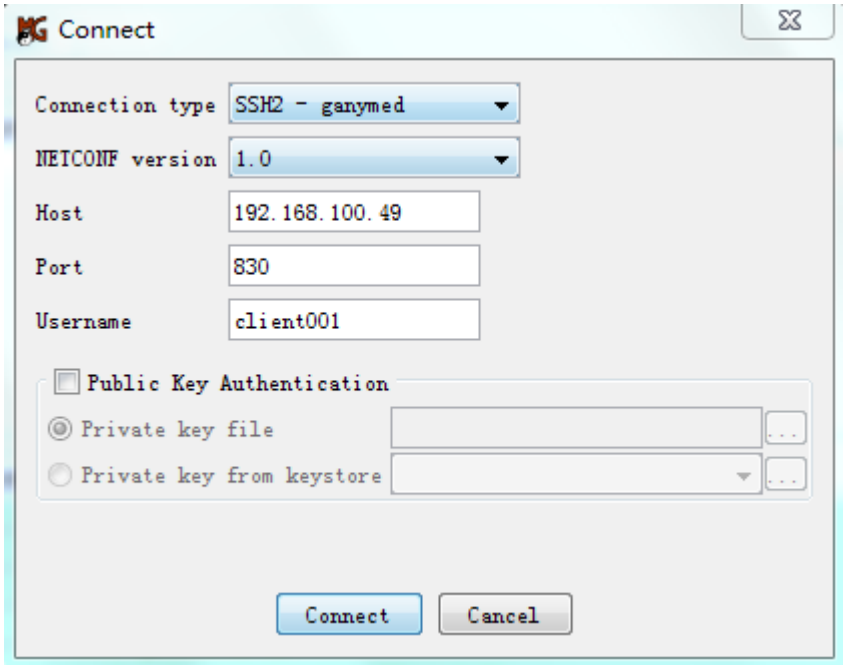


图1-19 输入密码：aabbcc。

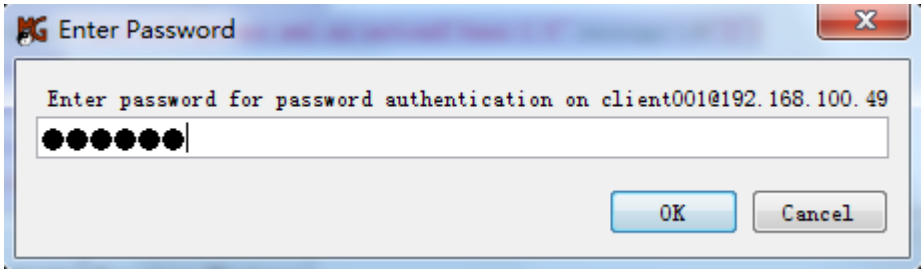
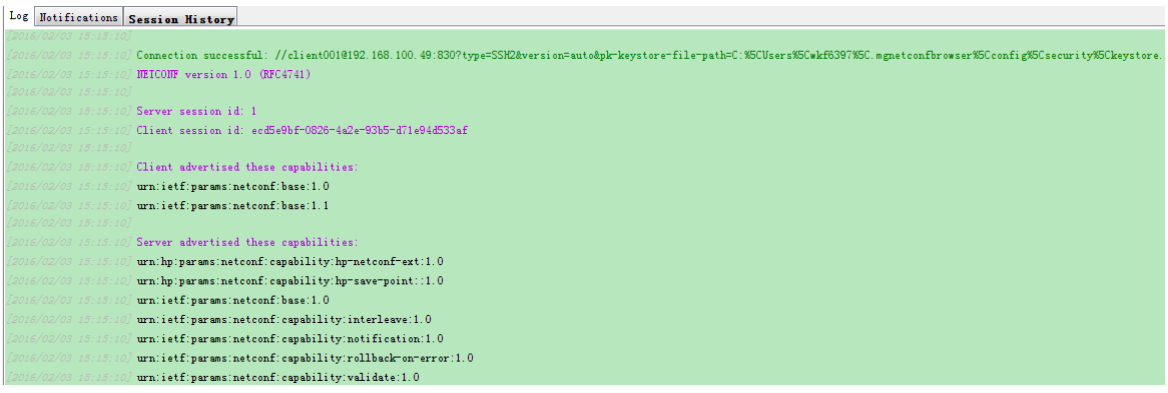


图1-20 登录成功



与 Device 建立 NETCONF over SSH 连接之后，直接进入 Device 的 NETCONF 配置模式。用户登录时获得 network-admin 权限，例如：

在 NetConf Browser 的“Command XML”区域输入以下信息，并点击 Send：

```
<get-sessions/>
```

在“Output XML”区域显示 NETCONF 用户的会话信息。

```
<?xml version="1.0" encoding="utf-8"?>
<rpc-reply xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="2">
  <get-sessions>
    <Session>
      <SessionID>1</SessionID>
      <Line>vty1</Line>
      <UserName>client001</UserName>
      <Since>2016-02-03T15:05:30</Since>
      <LockHeld>false</LockHeld>
    </Session>
  </get-sessions>
</rpc-reply>
```