8 文件管理

8.1 文件系统简介

文件系统

文件系统是指对存储器中文件、目录的管理，包括创建、删除、修改文件和目录，以及显示文件的内容等。

存储器

设备支持的存储器为Flash。

文件的命名规则

字符串形式，不支持空格，不区分大小写。文件名有两种表示方式：文件名、路径+文件名。

- 文件名

  如果直接使用文件名，则表示当前工作路径下的文件。文件名的长度范围是1～64。
- 路径+文件名

  格式为**drive + path + filename**，使用这种命名方式可以唯一的标识指定路径下的文件。文件名的长度范围是1～64，路径+文件名的总长度范围是1～160。

  drive是设备中的存储器，命名为**flash:**。

如果设备在堆叠情况下，**drive**的命名如下：

- flash：堆叠系统中主交换机Flash存储器根目录。
- 堆叠ID#flash：堆叠系统中某设备的Flash存储器根目录。

  例如：**slot2#flash:**是指堆叠ID为2的Flash卡。

path是指存储器中目录以及子目录，即路径。目录名使用的字符不可以是空格、“~”、“*”、“/”、“\”、“:”、“'”和“"”等字符，不区分大小写。

设备支持的路径可以是绝对路径也可以是相对路径。指定根目录（指定**drive**）的路径是绝对路径，相对路径有相对于根目录（即当前的存储器目录）的路径和相对于当前工作路径的路径，路径以“/”开头，则表示相对于根目录的路径。

- 若路径为“flash:/my/test/”，这是绝对路径。
- 若路径为“/selftest/”，表示根目录下的selftest目录，这是相对于根目录的相对路径。
- 若路径为“selftest/”，表示当前工作路径下的selftest目录，这是相对于当前工作路径的相对路径。

例如：**dir flash:/my/test/mytest.txt**，查看**flash:/my/test/**路径下的**mytest.txt**文件的信息，这是一种绝对路径。

如果用相对于根目录的路径，则可以使用命令：**dir /my/test/mytest.txt**。

如果用相对于当前工作路径的路径（若当前工作路径是**flash:/my/**），则使用命令**dir test/mytest.txt**。

说明

- 文件名在文件操作命令格式中统一用**filename**表示。
- 目录在文件操作命令中统一用**directory**表示，目录的格式即为**drive + path**。

8.2 设备支持的文件管理方式

设备在进行文件管理的过程中，可以分别充当服务器和客户端的角色：

- 设备作为服务器：可以从终端访问设备，实现对本设备文件的管理，以及与终端间的文件传输操作。
- 设备作为客户端访问其他设备（服务器）：可以实现管理其他设备上的文件，以及与其他设备间进行文件传输操作。

对于TFTP方式，设备只支持客户端功能；对于FTP、SFTP、SCP以及FTPS方式，设备均支持服务器与客户端功能。

各种文件管理方式的应用场景，优缺点如表8-1所示，用户可以根据需求选择其中一种方式。

表 8-1 文件管理方式

文件管理方式	应用场景	优点	缺点
直接登录系统	通过Console口、Telnet或STelnet方式登录设备，对存储器、目录和文件进行管理。特别是对存储器的操作需要通过此种方式。	对存储器、目录和文件的管理直接通过登录设备完成，方便快捷。	只是对本设备进行文件操作，无法进行文件的传输。
FTP（File Transfer Protocol）	适用于对网络安全性要求不是很高的文件传输场景中，广泛用于版本升级等业务中。	• 配置较简单，支持文件传输以及文件目录的操作。 • FTP可以在两个不同文件系统主机之间传输文件。 • 具有授权和认证功能。	明文传输数据，存在安全隐患。
TFTP（Trivial File Transfer Protocol）	在网络条件良好的实验室局域网中，可以使用TFTP进行版本的在线加载和升级。适用于客户端和服务器之间，不需要复杂交互的环境。	TFTP所占的内存要比FTP小。	• 设备只支持TFTP客户端功能。 • TFTP只支持文件传输，不支持交互。 • TFTP没有授权和认证，且是明文传输数据，存在安全隐患，易于网络病毒传输以及被黑客攻击。
SFTP（Secure File Transfer Protocol）	适用于网络安全性要求高的场景，目前被广泛用于日志下载、配置文件备份等业务中。	• 数据进行了严格加密和完整性保护，安全性高。 • 支持文件传输及文件目录的操作。 • 在设备上可以同时配置SFTP功能和普通FTP功能。（这一点与FTPS方式相比：FTPS是不可以同时提供FTPS和普通FTP功能的。）	配置较复杂。

文件管理方式	应用场景	优点	缺点
SCP（Secure Copy Protocol）	适用于网络安全性要求高，且文件上传下载效率高的场景。	• 数据进行了严格加密和完整性保护，安全性高。 • 客户端与服务器连接的同时完成文件的上传下载操作（即连接和拷贝操作使用一条命令完成），效率较高。	配置较复杂（与SFTP方式的配置非常类似），且不支持交互。
FTPS（FTP over SSL（Secure Sockets Layer））	适用于网络安全性要求高，且不提供普通FTP功能的场景。	利用数据加密、身份验证和消息完整性验证机制，为基于TCP可靠连接的应用层协议提供安全性保证。	• 配置较复杂，需要预先从CA处获得一套证书。 • 若配置FTPS服务，则普通的FTP服务功能必须关闭。

直接登录系统、FTP、TFTP方式，理解和配置都比较简单，下面主要介绍下另外几种文件管理方式。

SFTP 方式

SFTP是SSH协议的一部分，利用SSH协议提供的安全通道，使得远程用户可以安全地登录设备进行文件管理和文件传输等操作，为数据传输提供了更高的安全保障。同时，设备支持客户端的功能，用户可以从本地设备安全登录到远程SSH服务器上，进行文件的安全传输。

SSH提供的安全性主要有：

- 密文传输：在SSH连接建立初期，双方会通过协商的方式得出双方通信的加密算法和会话密钥，此后双方的通信就是以密文的方式进行，这样非法用户就很难窃取到合法用户的帐户信息。
- 支持基于公钥的认证：设备支持RSA、DSA和ECC三种公钥认证方式。
- 支持对服务器的认证：SSH协议可以通过验证服务器端公钥的方式来对服务器的身份进行认证，从而可以避免“伪服务器”方式的攻击。
- 支持对交互数据的校验：SSH协议支持对数据的完整性和真实性的校验，使用的校验方法是CRC(SSH1.5版本)和基于MD5的MAC算法(SSH2.0版本)。这样可以有效地防止类似于“中间人”的攻击。

SSH连接的建立过程：

1. 协商SSH版本号

   客户端与服务器通过发送的标识版本的字符串选择相互通讯所用的SSH协议版本。
2. 算法协商

   服务器和客户端进行密钥交换算法、加密算法、MAC算法协商的一个交互过程，用于后续的通讯过程。

3. 密钥交换

   根据前面算法协商过程中确定的密钥交换算法，服务器和客户端通过计算获得相同的会话密钥和会话ID。

4. 验证用户身份

   客户端向服务器发送用户身份信息。客户端将采用在服务器端配置的用户验证方式向服务器提出验证请求，直到验证通过或连接超时断开。

   服务器提供公钥认证和密码认证。

   - 在公钥（RSA、DSA和ECC三种）认证方式下，客户端必须生成RSA、DSA和ECC三种密钥对（包含公钥和私钥），并将公钥发送给服务器端。用户发起认证请求时，客户端随机生成一段由私钥加密的密文并发送给服务器，服务器利用客户端的公钥对其进行解密，解密成功就认为用户是可信的，对用户授予相应的访问权限。否则，中断连接。
   - 密码认证依靠AAA实现，与Telnet和FTP类似，支持本地数据库和远程RADIUS服务器验证，服务器对来自客户端的用户名与密码和预先配置的用户名与密码进行比较，如果完全匹配则验证通过。

5. 请求会话

   认证完成后，客户端向服务器提交会话请求。服务器则进行等待，处理客户端的请求。

6. 交互会话

   会话申请成功后，连接进入交互会话模式。在这个模式下，数据在两个方向上双向传送。

说明

在进行SSH连接建立前，需要在服务器端生成本地密钥对（RSA密钥对、DSA密钥对和ECC密钥对），这个密钥对不仅用于生成会话密钥和会话ID，还用于客户端验证服务器身份，同时这也是配置SSH服务器的关键步骤。

SCP 方式

SCP也是SSH协议的一部分，是基于SSH协议的远程文件拷贝技术，实现文件的拷贝，包括上传和下载。SCP文件拷贝命令简单易用，提高了网络维护的效率。

FTPS 方式

FTPS将FTP和SSL（Secure Sockets Layer，安全套接层）结合，又称安全FTP。通过SSL对客户端身份和服务器进行验证，对传输的数据进行加密，SSL为普通FTP服务器提供了安全连接，从而很大程度上改善了普通FTP服务器安全性问题，实现了对设备上文件的安全管理。

配置此方式必须要了解的几个概念：

- CA（Certificate Authority）

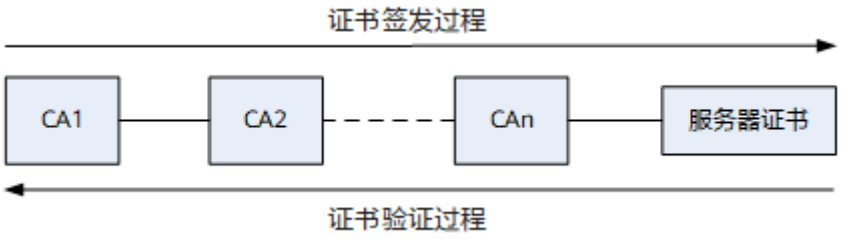
  CA是发放、管理、废除数字证书的机构。CA的作用是检查数字证书持有者身份的合法性，并签发数字证书（在证书上签字），以防证书被伪造或篡改，以及对证书和密钥进行管理。国际上被广泛信任的CA，被称之为根CA。根CA可授权其它CA为其下级CA。CA的身份也需要证明，而证明信息在信任证书机构文件中描述。

  例如：CA1作为最上级CA也叫根证书，签发下一级CA2证书，CA2又可以给它的下一级CA3签发证书，以此下去，最终由CAn签发服务器的证书。

如果服务器端的证书由CA3签发，则在客户端验证证书的过程从服务器端的证书有效性验证开始。先由CA3证书验证服务器端证书的有效性，如果通过则再由CA2证书验证CA3证书的有效性，最后由最上级CA1证书验证CA2证书的有效性。只有通过最上级CA证书即根证书的验证，服务器证书才会验证成功。

证书签发过程与证书验证过程如图8-1所示。

图 8-1 证书签发过程与证书验证过程示意图



- 数字证书

  数字证书实际上是存于计算机上的一个记录，是由CA签发的一个声明，证明证书主体（证书申请者拥有了证书后即成为证书主体）与证书中所包含的公钥的惟一对应关系。数字证书中包括证书申请者的名称及相关信息、申请者的公钥、签发数字证书的CA的数字签名及数字证书的有效期等内容。数字证书的作用使网上通信双方的身份得到了互相验证，提高了通信的可靠性。

  用户必须事先获取信息发送者的公钥证书，以便对信息进行解码认证，同时还需要CA发送给发送者的证书，以便用户验证发送者的身份。

- 证书撤销列表CRL（Certificate Revocation List）

  CRL由CA发布，它指定了一套证书发布者认为无效的证书。

  数字证书的寿命是有限的，但CA可通过证书撤销过程缩短证书的寿命。CRL指定的寿命通常比数字证书指定的寿命要短。由CA撤销数字证书，意味着CA在数字证书正常到期之前撤销允许使用密钥对的有关声明。在撤销证书到期后，CRL中的有关数据被删除，以缩短CRL列表的大小。

设备分别作为服务器和客户端的实现方式：

- 从用户终端访问作为FTP服务器的设备

  在作为FTP服务器的设备上部署SSL策略，加载数字证书并使能安全FTP服务器功能后，用户在终端通过支持SSL的FTP客户端软件访问安全FTP服务器，在终端与服务器之间实现文件的安全管理操作。

- 设备作为客户端访问FTP服务器

  在作为FTP客户端的设备上部署SSL策略并加载信任证书机构文件，检查证书持有者身份的合法性，以防证书被伪造或篡改。

8.3 管理本地文件

背景信息

须知

在对设备进行版本文件下载等文件操作过程中，请保持设备的正常供电。否则可能会引起文件损坏或文件系统损坏，从而造成设备存储介质损坏或设备不能正常启动等问题。

8.3.1 通过登录系统进行文件操作

前置任务

在配置通过登录系统进行文件操作之前，需完成以下任务：

- 终端与设备之间路由可达。
- 已从终端登录到设备。

配置流程

用户从终端登录到设备后，可以对存储器、目录及文件进行一系列操作。

以下各操作没有严格顺序，可根据需求选择一种或多种操作项目。

操作步骤

- **对目录进行操作**

表 8-2 目录操作

操作项目	命令	说明
查看当前所处的目录	**pwd**	-
改变当前所处的目录	**cd** *directory*	-
显示目录中的文件和子目录的列表	**dir** [**/all**] [*filename* | *directory* | **/all-filesystems**]	-
创建目录	**mkdir** *directory*	-

操作项目	命令	说明
删除目录	**rmdir** *directory*	• 被删除的目录必须为空目录。 • 目录被删除后，无法从回收站中恢复，原目录下被删除的文件也彻底从回收站中删除。

- **对文件进行操作**

表 8-3 文件操作

操作项目	命令	说明
显示文件的内容	**more** *filename* [*offset*] [**all**]	-
拷贝文件	**copy** *source-filename destination-filename*	• 在拷贝文件前，确保存储器有足够的空间。 • 若目标文件名与已经存在的文件名重名，将提示是否覆盖。
从HTTP服务器下载文件或上传文件到HTTP服务器	**copy** { *source-http-urlname destination-filename* | *source-filename destination-http-urlname* } [**username** *user-name* **password** *password*]	V200R013C00SPC500及之后版本支持。
从HTTPS服务器下载文件或上传文件到HTTPS服务器	**copy** { *source-https-urlname destination-filename* | *source-filename destination-https-urlname* } [**username** *user-name* **password** *password*] **ssl-policy** *ssl-policy*	V200R013C00SPC500及之后版本支持。
移动文件	**move** *source-filename destination-filename*	若目标文件名与已经存在的文件名重名，将提示是否覆盖。
重新命名文件	**rename** *old-name new-name*	-
压缩文件	**zip** *source-filename destination-filename*	-
解压缩文件	**unzip** *source-filename destination-filename*	-

操作项目	命令	说明
删除文件	**delete** [**/unreserved**] [**/quiet**] { *filename* | *devicename* }	此命令不能删除目录。 **须知** 如果使用参数**/unreserved**，则删除后的文件不可恢复。
恢复删除的文件	**undelete** { *filename* | *devicename* }	执行**delete**命令（不带**/unreserved**参数）后，文件将被放入回收站中。可以执行此命令恢复回收站中被删除的文件。
彻底删除回收站中的文件	**reset recycle-bin** [*filename* | *devicename*]	需要永久删除回收站中的文件时，可进行此操作。
进入系统视图	**system-view**	-
运行批处理文件	**execute** *batch-filename*	一次进行多项处理时，可进行此操作。编辑好的批处理文件要预先保存在设备的存储器中。

说明

当对文件执行操作命令时，若出现错误提示信息“Cannot xxx, because it may be locked or no lock available.”，请等待一段时间后再执行该命令。若多次执行命令后仍出现该提示，请联系技术支持人员处理。

- **对存储器进行操作**

当某存储器上的文件系统出现异常时，终端会给出提示信息，建议修复异常。

当文件系统的异常无法修复或者确认不再需要存储器上的所有数据时，可格式化存储器。格式化会清空存储器中的所有文件和目录。

须知

格式化存储器，会导致数据无法恢复，请慎用。

表 8-4 存储器的操作

操作项目	命令	说明
修复文件系统异常的存储器	**fixdisk** *drive*	执行此命令后，如果仍然收到系统建议修复的信息，则表示存储器可能已经损坏。
格式化存储器	**format** *drive*	如果执行此命令后，存储器仍然不可用，则可能是物理原因导致的存储器不可用。

- **配置文件系统提示方式**

  当在设备上进行操作时，系统可以给予提示或警示信息（特别是对于可能导致数据丢失或破坏的操作）。如果需要修改系统对文件操作的提醒方式时，可以进行配置文件系统提示方式的操作。

  表 8-5 配置文件系统提示方式

操作步骤	命令	说明
进入系统视图	**system-view**	-
配置文件系统提示方式	**file prompt { alert | quiet }**	缺省情况下，提示方式为**alert**。 **须知** 如果将文件操作的提醒方式设置为**quiet**，则对由于用户误操作（比如删除文件操作）而导致数据丢失的情况不作提示，请慎用。

----结束

8.3.2 通过 FTP 进行文件操作

前置任务

在通过FTP进行文件操作之前，需完成以下任务：

- 终端与设备之间路由可达。
- 终端支持FTP客户端软件。

配置流程

须知

使用FTP协议存在安全风险，建议使用SFTP V2、SCP或FTPS方式进行文件操作。

从V200R020C00版本开始，当需要授权客户可以登录服务器时，必须执行命令指定服务器端的源接口或源地址。

通过FTP进行文件操作的配置流程如表8-6所示。

表 8-6 通过 FTP 进行文件操作的配置流程

序号	配置任务名称	配置任务说明	配置流程说明
1	配置FTP服务器功能及参数	包括FTP服务器的使能及参数配置：端口号、源地址、超时断连时间。	序号1、2、3之间没有严格的配置顺序。

序号	配置任务名称	配置任务说明	配置流程说明
2	配置FTP本地用户	包括配置本地用户的服务类型、用户级别及FTP用户的授权目录等。	
3	（可选）配置FTP访问控制	包括配置ACL规则及FTP基本访问控制列表，提高FTP访问的安全性。	
4	用户通过FTP访问设备	从终端通过FTP访问设备。	-

缺省配置

表 8-7 缺省配置

参数	缺省值
FTP服务器功能	关闭
端口号	21
FTP用户	没有创建本地用户

操作步骤

- **配置FTP服务器功能及参数**

  表 8-8 配置 FTP 服务器功能及参数

操作步骤	命令	说明
进入系统视图	**system-view**	-
（可选）指定FTP服务器端口号	**ftp** [**ipv6**] **server port** *port-number*	缺省情况下，FTP服务器端口号是21。 如果配置了新的端口号，FTP服务器端先断开当前已经建立的所有FTP连接，然后使用新的端口号开始尝试连接。这样可以有效防止攻击者对FTP服务标准端口的访问。

操作步骤	命令	说明
指定FTP服务器的源地址	• **ftp server-source** { **-a** *source-ip-address* | **-i** *interface-type interface-number* } • **ftp ipv6 server-source -a** *ipv6_address* [**vpn-instance** *vpn_name*]	缺省情况下，未指定FTP服务器的源地址。 配置了服务器的源地址后，登录服务器时，所输入的服务器地址必须与该命令中配置的一致，否则无法成功登录。
使能FTP服务器	**ftp** [**ipv6**] **server enable**	缺省情况下，设备的FTP服务器功能是关闭的。
（可选）配置FTP连接空闲时间	**ftp** [**ipv6**] **timeout** *minutes*	缺省情况下，连接空闲时间为10分钟。 在设定的时间内，如果FTP连接始终处于空闲状态时，系统将自动断开FTP连接。
（可选）设置FTP服务器支持的最大会话数	**ftp** [**ipv6**] **server max-sessions** *max-sessions-number*	缺省情况下，FTP服务器支持的最大会话数是5。

说明

- 如果变更端口号前FTP服务已经启动，则不能变更成功。需执行**undo ftp** [**ipv6**] **server**命令关闭FTP服务，再进行端口号变更。
- 当客户端与设备之间的文件操作结束后，请执行**undo ftp** [**ipv6**] **server**命令，及时关闭FTP服务器功能，从而保证设备的安全。

- **配置FTP本地用户**

当用户通过FTP进行文件操作时，需要在作为FTP服务器的设备上配置本地用户名及口令、指定用户的服务类型以及可以访问的目录，否则用户将无法通过FTP访问设备。

表 8-9 配置 FTP 本地用户

操作步骤	命令	说明
进入系统视图	**system-view**	-
进入AAA视图	**aaa**	-
配置本地用户名和密码	**local-user** *user-name* **password irreversible-cipher** *password*	-
配置本地用户级别	**local-user** *user-name* **privilege level** *level*	**说明** 必须将用户级别配置在3级或3级以上，否则FTP连接将无法成功。

操作步骤	命令	说明
配置本地用户的服务类型为FTP	**local-user** *user-name* **service-type ftp**	缺省情况下，本地用户可以使用所有的接入类型。
配置FTP用户的授权目录	**local-user** *user-name* **ftp-directory** *directory*	缺省情况下，本地用户的FTP目录为空。 当有多个FTP用户且有相同的授权目录时，可以执行**set default ftp-directory** *directory*命令，为FTP用户配置缺省工作目录。此时，不需要通过**local-user** *user-name* **ftp-directory** *directory*命令为每个用户配置授权目录。
配置本地用户的FTP权限	**local-user** *user-name* **ftp-privilege** [*directoryfilename*] { **read** | **write** | **execute** }*	缺省情况下，本地用户的FTP权限为读、写和执行权限。

- **（可选）配置FTP访问控制**

  ACL是一系列有顺序的规则组的集合，这些规则根据数据包的源地址、目的地址、端口号等来描述。ACL通过规则对数据包进行分类，这些规则应用到路由设备，路由设备根据这些规则判断哪些数据包可以接收，哪些数据包需要拒绝。

  用户可以配置FTP访问控制列表，实现只允许指定的客户端登录到设备，以提高安全性。

  ACL规则：

  - 当ACL的rule配置为**permit**时，则允许匹配该rule规则的其他设备与本设备建立FTP连接。
  - 当ACL的rule配置为**deny**时，则拒绝匹配该rule规则的其他设备与本设备建立FTP连接。
  - 当ACL配置了rule，但来自其他设备的报文没有匹配该rule规则时，则拒绝其他设备与本设备建立FTP连接。
  - 当ACL未配置rule时，则允许任何其他设备与本设备建立FTP连接。

  表 8-10 （可选）配置 FTP 访问控制

操作步骤	命令	说明
进入系统视图	**system-view**	-
进入ACL视图	**acl** [**number**] *acl-number*	-

操作步骤	命令	说明
配置ACL规则	**rule** [*rule-id*] { **deny** | **permit** } [**source** { *source-address source-wildcard* | **any** } | **fragment** | **logging** | **time-range** *time-name* | { **vpn-instance** *vpn-instance-name* | **public** }] *	-
退回到系统视图	**quit**	-
配置FTP基本访问控制列表	**ftp** [**ipv6**] **acl** *acl-number*	-

- **用户通过FTP访问设备**

  从终端通过FTP访问设备，可以选择使用Windows命令行提示符或第三方软件。此处以Windows命令行提示符为例进行配置。

  – 执行Windows命令**ftp** *ip-address*，通过FTP方式访问设备。

    此处输入的IP地址为设备上配置的IP地址，且与用户终端IP地址路由可达。

  – 根据提示输入用户名和口令，按Enter键，当出现FTP客户端视图的命令行提示符，如ftp>，此时用户进入了FTP服务器的工作目录。（以下显示信息仅为示意）

```
C:\Documents and Settings\Administrator> ftp 192.168.150.208
连接到 192.168.150.208。
220 FTP service ready.
用户(192.168.150.208:(none)):huawei
331 Password required for huawei.
密码:
230 User logged in.
ftp>
```

- **通过FTP命令进行文件操作**

  用户访问FTP服务器后，可以通过FTP命令进行文件操作，包括目录操作、文件操作、配置文件传输方式、查看FTP命令在线帮助等。

  说明

  用户的操作权限受限于服务器上对该用户的权限设置。

  由于文件系统对根目录下的文件个数有限制，当根目录中文件个数大于50个时，继续在根目录中创建文件可能会失败。

  以下各操作没有严格顺序，可根据需求选择一种或多种操作项目。

表 8-11 通过 FTP 命令进行文件操作

操作项目	命令	说明
改变服务器上的工作路径	**cd** *remote-directory*	-

操作项目	命令	说明
改变服务器的工作路径到上一级目录	**cdup**	-
显示服务器工作路径	**pwd**	-
显示或者改变客户端的工作路径	**lcd** [*local-directory*]	与**pwd**不同的是，**lcd**命令执行后显示的是客户端的本地工作路径，而**pwd**显示的则是远端服务器的工作路径。
在服务器上创建目录	**mkdir** *remote-directory*	创建的目录可以为字母和数字等的组合，但不可以为<、>、？ 、\、： 等特殊字符。
在服务器上删除目录	**rmdir** *remote-directory*	-
显示服务器上指定目录或文件的信息	**dir/ls** [*remote-filename* [*local-filename*]]	• **ls**命令只能显示出目录/文件的名称，而**dir**命令可以查看目录/文件的详细信息，如大小，创建日期等。 • 如果指定远程文件时没有指定路径名称，那么系统将在用户的授权目录下搜索指定的文件。
删除服务器上指定文件	**delete** *remote-filename*	-
上传单个或多个文件	**put** *local-filename* [*remote-filename*] 或 **mput** *local-filenames*	• **put**命令是上传单个文件。 • **mput**命令是上传多个文件。
下载单个或多个文件	**get** *remote-filename* [*local-filename*] 或 **mget** *remote-filenames*	• **get**命令是下载单个文件。 • **mget**命令是下载多个文件。
配置传输文件的数据类型为ASCII模式或二进制模式	**ascii** 或 **binary**	二选一 • 缺省情况下，文件传输方式为ASCII模式。 • 传输文本文件使用ASCII方式，传输程序、系统软件、数据库文件等使用二进制模式。

操作项目	命令	说明
配置文件传输方式为被动方式或主动方式	**passive** 或 **undo passive**	二选一 缺省情况下，数据传输方式是主动方式。
查看FTP命令的在线帮助	**remotehelp** [*command*]	-
使能系统的提示功能	**prompt**	缺省情况下，不使能信息提示。
打开verbose开关	**verbose**	如果打开verbose开关，将显示所有FTP响应，包括FTP协议信息，以及FTP服务器返回的详细信息。

- **（可选）更改登录用户**

  设备可以在不退出FTP客户端视图的情况下，以其他的用户名登录到FTP服务器。所建立的FTP连接，与执行**ftp**命令建立的FTP连接完全相同。

操作步骤	命令	说明
FTP客户端视图下，更改当前的登录用户	**user** *user-name* [*password*]	更改当前的登录用户后，原用户与服务器的连接将断开。

- **断开与FTP服务器的连接**

  用户可以在FTP客户端视图中选择不同的命令断开与FTP服务器的连接。

操作步骤	命令	说明
终止与服务器的连接，并退回到用户视图	**bye** 或 **quit**	二选一。
终止与服务器的连接，并退回到FTP客户端视图	**close** 或 **disconnect**	

----结束

检查配置结果

- 使用**display** [**ipv6**] **ftp-server**命令，查看FTP服务器的配置和状态信息。
- 使用**display ftp-users**命令，查看登录的FTP用户信息。

8.3.3 通过 SFTP 进行文件操作

前置任务

在配置通过SFTP进行文件操作之前，需完成以下任务：

- 终端与设备之间有可达路由。
- 终端上已安装SSH客户端软件。

配置流程

说明

使用SFTP V1协议存在安全风险，建议使用SFTP V2或FTPS方式进行文件操作。

从V200R020C00版本开始，当需要授权客户可以登录服务器时，必须执行命令指定服务器端的源接口或源地址。

通过SFTP进行文件操作的配置流程如表8-12所示。

表 8-12 通过 SFTP 进行文件操作的配置流程

序号	配置任务名称	配置任务说明	配置流程说明
1	配置SFTP服务器功能及参数	包括服务器本地密钥对生成、SFTP服务器功能的使能及服务器参数的配置：端口号、源地址、密钥对更新时间、SSH认证超时时间、SSH验证重试次数等。	序号1、2、3之间没有严格的配置顺序。
2	配置SSH用户登录的用户界面	包括VTY用户界面的用户验证方式、VTY用户界面支持SSH协议及其它基本属性。	
3	配置SSH用户	包括SSH用户的创建、认证方式、服务方式、SFTP服务授权目录等。	
4	用户通过SFTP协议访问设备	从终端通过SSH客户端软件访问设备。	-

缺省配置

表 8-13 缺省配置

参数	缺省值
SFTP服务器功能	关闭
端口号	22

参数	缺省值
服务器密钥对更新时间	0，表示永不更新
SSH认证超时时间	60秒
SSH验证重试次数	3
SSH用户	没有创建
SSH用户的服务方式	空，即不支持任何服务方式
SSH用户的SFTP服务授权目录	flash:

操作步骤

- **配置SFTP服务器功能及参数**

  表 8-14 配置 SFTP 服务器功能及参数

操作步骤	命令	说明
进入系统视图	**system-view**	-
生成本地密钥对	**rsa local-key-pair create**、**dsa local-key-pair create**或**ecc local-key-pair create**	根据生成的密钥类型，三选一。 密钥对生成后，可以执行**display rsa local-key-pair public**、**display dsa local-key-pair public**或**display ecc local-key-pair public**命令查看本地密钥对中的公钥信息。 **说明** 密钥对长度越大，密钥对安全性就越好，建议使用最大的密钥对长度。
指定SSH服务器端的源地址	• **ssh server-source -i** *interface-type interface-number* • **ssh ipv6 server-source -a** *ipv6_address* [**-vpn-instance** *vpn_name*]	缺省情况下，未指定SSH服务器端的源地址。
使能SFTP服务器功能	**sftp [ipv4 | ipv6] server enable**	缺省情况下，SFTP服务为关闭状态。

操作步骤	命令	说明
（可选）配置SSH服务器端的密钥交换算法列表	**ssh server key-exchange** { **dh_group14_sha256** | **dh_group15_sha512** | **dh_group16_sha512** | **dh_group_exchange_sha256** | **ecdh_sha2_nistp256**| **ecdh_sha2_nistp384**| **ecdh_sha2_nistp521**}*	缺省情况下，SSH服务器支持所有的密钥交换算法。 系统软件中不包含**dh_group_exchange_sha1**、**dh_group14_sha1和dh_group1_sha1**参数，如需使用，需要安装WEAKEA插件，但是该算法安全性低。为了保证更好的安全性，建议使用其它算法。WEAKEA插件安装方法请参见WEAKEA插件使用指南。
（可选）配置SSH服务器端的加密算法列表	**ssh server cipher** { **aes128_ctr** | **aes256_ctr** } *	缺省情况下，不安装WEAKEA插件，SSH服务器只支持**aes128_ctr**和**aes256_ctr**算法，不可以使用**undo ssh server cipher**命令，安装WEAKEA插件后，增加支持**aes256_cbc**、**aes128_cbc**、**3des_cbc**和**des_cbc**算法，并且可以使用**undo ssh server cipher**命令。 系统软件中不包含**aes256_cbc**、**aes128_cbc**、**3des_cbc**和**des_cbc**参数，如需使用，需要安装WEAKEA插件，但是该算法安全性低。为了保证更好的安全性，建议配置**aes256_ctr**或**aes128_ctr**参数。WEAKEA插件安装方法请参见WEAKEA插件使用指南。

操作步骤	命令	说明
（可选）配置SSH服务器上的校验算法列表	**ssh server hmac** {**sha2_256** }	缺省情况下，不安装WEAKEA插件，SSH服务器只支持**sha2_256**校验算法，不可以使用**undo ssh server hmac**命令，安装WEAKEA插件后，增加支持**sha2_256_96**、**sha1**、**sha1_96**、**md5**和**md5_96**校验算法，并且可以使用**undo ssh server hmac**命令。 系统软件中不包含**sha2_256_96**、**sha1**、**sha1_96**、**md5**和**md5_96**参数，如需使用，需要安装WEAKEA插件，但是该算法安全性低。为了保证更好的安全性，建议配置**sha2_256**参数。WEAKEA插件安装方法请参见WEAKEA插件使用指南。
（可选）配置与SSH客户端进行Diffie-hellman-group-exchange密钥交换时，支持的最小密钥长度	**ssh server dh-exchange min-len** *min-len*	缺省情况下，SSH服务器与客户端进行Diffie-hellman-group-exchange密钥交换时，支持的最小密钥长度为1024字节。
（可选）端口号	**ssh [ipv4 | ipv6] server port** *port-number*	缺省情况下，SSH服务器的端口号是22。 如果配置了新的端口号，SSH服务器端先断开当前已经建立的所有SSH连接，然后使用新的端口号开始尝试连接。这样可以有效防止攻击者对SSH服务标准端口的访问，确保安全性。

操作步骤	命令	说明
（可选）服务器密钥对更新时间	**ssh server rekey-interval** *hours*	缺省情况下，SSH服务器密钥对的更新时间间隔为0，表示永不更新。 配置服务器密钥对更新时间，使得当SSH服务器的更新周期到达时，自动更新服务器密钥对，从而可以保证安全性。 该命令只在SSH1.X版本生效。SSH1.X的安全性较低，不推荐使用。
（可选）配置SSH服务器重协商密钥时的参数	**ssh server rekey** { **time** *rekey-time* | **data-limit** *data-limit* | **max-packet** *max-packet* } *	缺省情况下，SSH服务器触发密钥重协商的时间间隔为60分钟，重协商密钥时收发数据大小上限为1000MB，重协商密钥时收发数据包个数上限为268435456（2^28）个。
（可选）指定SSH服务器的公钥算法	**ssh server publickey** { **dsa** | **ecc** | **rsa** | **rsa_sha2_256** | **rsa_sha2_512** } *	缺省情况下，DSA、ECC、RSA、RSA_SHA2_256、RSA_SHA2_512公钥算法都是开启的。
（可选）SSH认证超时时间	**ssh server timeout** *seconds*	缺省情况下，SSH连接认证超时时间为60秒。
（可选）SSH验证重试次数	**ssh server authentication-retries** *times*	缺省情况下，SSH连接的验证重试次数为3。
（可选）配置访问控制列表	**ssh** [**ipv6**] **server acl** *acl-number*	缺省情况下，没有配置访问控制列表。 配置了访问控制列表，可控制哪些客户端能以SSH方式访问本设备。

- 生成本地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，二者分别包括一个公钥和一个私钥。服务器密钥对和主机密钥对的长度均为2048位。
- 生成本地DSA密钥对时，只生成一个主机密钥对，长度可为1024、2048。缺省情况下，密钥对的长度为2048位。
- 生成本地ECC密钥对时，只生成一个主机密钥对，长度可为256、384、521。缺省情况下，密钥对的长度为521位。

- **配置SSH用户登录的用户界面**

  使用SFTP协议，用户将通过VTY用户界面登录设备，所以需要配置VTY用户界面的相关属性

表 8-15 配置 SSH 用户登录的用户界面

操作步骤	命令	说明
进入系统视图	**system-view**	-
进入VTY用户界面视图	**user-interface vty** *first-ui-number* [*last-ui-number*]	-
配置VTY用户界面的验证方式为AAA	**authentication-mode aaa**	缺省情况下，VTY用户界面没有验证方式。 必须配置VTY用户界面验证方式为AAA验证，否则**protocol inbound ssh**不能配置成功，用户也将无法登录设备。
配置VTY用户界面支持SSH协议	**protocol inbound ssh**	缺省情况下，用户界面支持的协议是SSH。 如果不配置某个或某几个VTY用户界面支持SSH协议，则SSH用户不能登录设备。
配置VTY用户界面的用户优先级	**user privilege level** *level*	必须将用户级别配置为3级及3级以上，否则连接不成功。 如果是password认证用户，还可以执行**local-user** *user-name* **privilege level** *level*命令配置本地用户的用户级别为3级及3级以上。
（可选）VTY用户界面其他属性	-	除配置VTY用户界面的验证方式和用户优先级外，VTY用户界面的其他属性包括： ● VTY用户界面的最大个数 ● VTY用户界面的呼入呼出限制 ● VTY用户界面的终端属性 请参见**6.6 配置通过STelnet登录设备**–其他功能命令。

- **配置SSH用户**

配置SSH用户包括配置SSH用户的验证方式，设备支持的认证方式包括RSA、password、password-rsa、DSA、password-dsa、ECC、password-ecc和all。其中：

- password-rsa认证需要同时满足password认证和RSA认证。
- password-dsa认证需要同时满足password认证和DSA认证。
- password-ecc认证需要同时满足password认证和ECC认证。
- all认证是指password认证、RSA、DSA或ECC认证方式满足其中一种即可。

表 8-16 配置 SSH 用户

操作步骤	命令	说明
进入系统视图	**system-view**	-
创建SSH用户	**ssh user** *user-name*	-
配置SSH用户的认证方式	**ssh user** *user-name* **authentication-type** { **password** | **rsa** | **password-rsa** | **dsa** | **password-dsa** | **ecc** | **password-ecc** | **all** }	如果没有使用**ssh user**命令配置相应的SSH用户，则可以直接执行**ssh authentication-type default password**命令为用户配置SSH认证缺省采用密码认证，在用户数量比较多时，对用户使用缺省密码认证方式可以简化配置，此时只需再配置AAA用户即可。 **说明** 当认证方式为all认证时，用户的优先级需根据接入用户选择的认证方式来决定： • 如果接入用户选择的认证方式为password认证，则用户优先级为AAA中设置的用户优先级。 • 如果接入用户选择的认证方式为RSA、DSA或ECC认证，则用户的优先级由用户接入时所采用的VTY界面的优先级决定。 如果SSH用户认证方式为all认证，且存在一个同名AAA用户，那通过这两种方式接入时用户优先级可能不同，请根据需要进行部署。
配置SSH用户的服务方式为SFTP或all	**ssh user** *username* **service-type** { **sftp** | **stelnet** | **all** }	缺省情况下，SSH用户的服务方式是空，即不支持任何服务方式。
配置SSH用户的SFTP服务授权目录	**ssh user** *username* **sftp-directory** *directoryname*	缺省情况下，SSH用户的SFTP服务授权目录是flash:。

- password认证依靠AAA实现，当用户使用password、password-rsa、password-dsa或password-ecc认证方式登录设备时，需要在AAA视图下创建同名的本地用户。
- 如果SSH用户使用password认证，则只需要在SSH服务器端生成本地RSA、DSA或ECC密钥。如果SSH用户使用RSA、DSA或ECC认证，则在服务器端和客户端都需要生成本地RSA、DSA或ECC密钥对，并且服务器端和客户端都需要将对方的公钥配置到本地。

根据上面配置的认证方式，进行选择配置：

- 若对SSH用户进行password认证，请根据**表8-17**进行配置。
- 若对SSH用户进行RSA、DSA或ECC认证，请根据**表8-18**进行配置。
- 若对SSH用户进行password-rsa、password-dsa或password-ecc认证，则AAA用户和RSA、DSA或ECC公共密钥都需要进行配置，即同时配置**表8-17**和**表8-18**。

表 8-17 配置对 SSH 用户进行 password、password-rsa、password-dsa 或 password-ecc 认证

操作步骤	命令	说明
进入系统视图	**system-view**	-
进入AAA视图	**aaa**	-
配置本地用户名和密码	**local-user** *user-name* **password irreversible-cipher** *password*	-
配置本地用户的服务方式	**local-user** *user-name* **service-type ssh**	-
配置本地用户的级别	**local-user** *user-name* **privilege level** *level*	-
退回到系统视图	**quit**	-

表 8-18 配置对 SSH 用户进行 dsa、rsa、ecc、password-dsa、password-rsa 或 password-ecc 认证

操作步骤	命令	说明
进入系统视图	**system-view**	-

操作步骤	命令	说明
进入RSA、DSA或ECC公共密钥视图	**rsa peer-public-key** *key-name* [**encoding-type** { **der** | **openssh** | **pem** }] 、 **dsa peer-public-key** *key-name* **encoding-type** { **der** | **openssh** | **pem** } 或 **ecc peer-public-key** *key-name* **encoding-type** { **der** | **openssh** | **pem** }	-
进入公共密钥编辑视图	**public-key-code begin**	-
编辑公共密钥	*hex-data*	• 键入的公共密钥必须是按公钥格式编码的十六进制字符串，由支持SSH的客户端软件生成。具体操作参见相应的SSH客户端软件的帮助文档。 • 请将RSA、DSA或ECC公钥输入到作为SSH服务器的设备上。
退出公共密钥编辑视图	**public-key-code end**	• 如果未输入合法的密钥编码hex-data，执行本步骤后，将无法生成密钥。 • 如果指定的密钥*key-name*已经在别的窗口下被删除，再执行本步骤时，系统会提示：密钥已经不存在，此时直接退到系统视图。
退出公共密钥视图，回到系统视图	**peer-public-key end**	-
为SSH用户分配RSA、DSA或ECC公钥	**ssh user** *user-name* **assign** { **rsa-key** | **dsa-key** | **ecc-key** } *key-name*	-

- **用户通过SFTP协议访问设备**

从终端通过SFTP访问设备，需要在终端上安装SSH客户端软件。此处以使用第三方软件OpenSSH和Windows命令行提示符为例进行配置。

- OpenSSH软件的安装请参考该软件的安装说明。
- 使用OpenSSH软件从终端访问设备时，需要使用OpenSSH的命令，命令的使用可以参见该软件的帮助文档。
- 只有安装了OpenSSH软件后，Windows命令行提示符才能识别OpenSSH相关命令。

进入Windows的命令行提示符，执行OpenSSH命令，通过SFTP方式访问设备。

当出现SFTP客户端视图的命令行提示符，如sftp>，此时用户进入了SFTP服务器的工作目录。（以下显示信息仅为示意）

```
C:\Documents and Settings\Administrator> sftp sftpuser@10.136.23.5
Connecting to 10.136.23.5...
The authenticity of host '10.136.23.5 (10.136.23.5)' can't be established.
DSA key fingerprint is 46:b2:8a:52:88:42:41:d4:af:8f:4a:41:d9:b8:4f:ee.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.136.23.5' (DSA) to the list of known hosts.

User Authentication
Password:
sftp>
```

- **通过SFTP命令进行文件操作**

  当SFTP客户端登录到SSH服务器之后，用户可以在SFTP客户端进行如表8-19所示的操作。

  以下各操作没有严格顺序，可根据需求选择一种或多种操作项目。

  说明

  在SFTP客户端视图下，文件操作命令不支持联想功能，必须手动输入完整的命令，否则会提示是不支持的命令。

  由于文件系统对根目录下的文件个数有限制，当根目录中文件个数大于50个时，继续在根目录中创建文件可能会失败。

表 8-19 通过 SFTP 文件操作命令进行文件操作

操作项目	命令	说明
改变用户的当前工作目录	**cd** [*remote-directory*]	-
改变用户的工作目录为当前工作目录的上一级目录	**cdup**	-
显示用户的当前工作目录	**pwd**	-
显示指定目录下的文件列表	**dir/ls** [**-l** | **-a**] [*remote-directory*]	**dir**与**ls**执行的效果是一样的。

操作项目	命令	说明
删除服务器上目录	**rmdir** *remote-directory* &<1-10>	一次最多可以删除十个目录。 使用该命令删除目录时，目录中不能有文件，否则会删除失败。
在服务器上创建新目录	**mkdir** *remote-directory*	-
改变服务器上指定的文件的名字	**rename** *old-name new-name*	-
下载远程服务器上的文件	**get** *remote-filename* [*local-filename*]	-
上传本地文件到远程服务器	**put** *local-filename* [*remote-filename*]	-
删除服务器上文件	**remove** *remote-filename* &<1-10>	一次最多可以删除十个文件。
SFTP客户端命令帮助	**help** [**all** | *command-name*]	-

用户也可以在系统视图下执行如下命令下载服务器上的文件或者上传本地文件到远程服务器中:

- IPv4地址：**sftp client-transfile** { **get** | **put** } [**-a** *source-address* | **-i** *interface-type interface-number*] **host-ip** *host-ipv4* [*port*] [[**public-net** | **-vpn-instance** *vpn-instance-name*] | **prefer_kex** *prefer_key-exchange* | **identity-key** { **rsa** | **dsa** | **ecc** } | **prefer_ctos_cipher** *prefer_ctos_cipher* | **prefer_stoc_cipher** *prefer_stoc_cipher* | **prefer_ctos_hmac** *prefer_ctos_hmac* | **prefer_stoc_hmac** *prefer_stoc_hmac* | **-ki** *aliveinterval* | **-kc** *alivecountmax*] * **username** *user-name* **password** *password* **sourcefile** *source-file* [**destination** *destination*]
- IPv6地址：**sftp client-transfile** { **get** | **put** } **ipv6** [**-a** *source-address*] **host-ip** *host-ipv6* [**-oi** *interface-type interface-number*] [*port*] [**-vpn-instance** *vpn-instance-name* | **prefer_kex** *prefer_key-exchange* | **identity-key** { **rsa** | **dsa** | **ecc** } | **prefer_ctos_cipher** *prefer_ctos_cipher* | **prefer_stoc_cipher** *prefer_stoc_cipher* | **prefer_ctos_hmac** *prefer_ctos_hmac* | **prefer_stoc_hmac** *prefer_stoc_hmac* | **-ki** *aliveinterval* | **-kc** *alivecountmax*] * **username** *user-name* **password** *password* **sourcefile** *source-file* [**destination** *destination*]

- **断开与SFTP服务器的连接**

操作步骤	命令	说明
断开与SFTP服务器的连接	**quit**	-

----结束

检查配置结果

- 使用**display ssh user-information** [*username*]命令，在SSH服务器端查看SSH用户信息。
- 使用**display ssh server status**命令，查看SSH服务器的全局配置信息。
- 使用**display ssh server session**命令，在SSH服务器端查看SSH客户端连接会话信息。

8.3.4 通过 SCP 进行文件操作

前置任务

配置通过SCP进行文件操作之前，需完成以下任务：

- 终端与设备之间路由可达。
- 终端上已安装支持SCP的SSH客户端软件。

配置流程

通过SCP进行文件操作的配置流程如表8-20所示。

说明

从V200R020C00版本开始，当需要授权客户可以登录服务器时，必须执行命令指定服务器端的源接口或源地址。

表 8-20 通过 SCP 进行文件操作的配置流程

序号	配置任务名称	配置任务说明	配置流程说明
1	配置SCP服务器功能及参数	包括服务器本地密钥对生成、SCP服务器功能的使能及服务器参数的配置：端口号、源地址、密钥对更新时间、SSH认证超时时间、SSH验证重试次数等。	序号1、2、3之间没有严格的配置顺序。
2	配置SSH用户登录的用户界面	包括VTY用户界面的用户验证方式、VTY用户界面支持SSH协议及其它基本属性。	
3	配置SSH用户	包括SSH用户的创建、认证方式、服务方式等。	
4	用户通过SCP进行文件操作	从终端通过SCP客户端软件实现上传或下载文件的操作。	—

缺省配置

表 8-21 缺省配置

参数	缺省值
SCP服务器功能	关闭
端口号	22
服务器密钥对更新时间	0，表示永不更新
SSH认证超时时间	60秒
SSH验证重试次数	3
SSH用户	没有创建
SSH用户的服务方式	空，即不支持任何服务方式

操作步骤

- **配置SCP服务器功能及参数**

表 8-22 配置 SCP 服务器功能及参数

操作步骤	命令	说明
进入系统视图	**system-view**	-
生成本地密钥对	**rsa local-key-pair create**、**dsa local-key-pair create**或**ecc local-key-pair create**	根据生成的密钥类型，三选一。 密钥对生成后，可以执行**display rsa local-key-pair public**、**display dsa local-key-pair public**或**display ecc local-key-pair public**命令查看本地密钥对中的公钥信息。 **说明** 密钥对长度越大，密钥对安全性就越好，建议使用最大的密钥对长度。
指定SSH服务器端的源地址	• **ssh server-source -i** *interface-type interface-number* • **ssh ipv6 server-source -a** *ipv6_address* [**-vpn-instance** *vpn_name*]	缺省情况下，未指定SSH服务器端的源地址。
使能SCP服务器功能	**scp [ipv4 | ipv6] server enable**	缺省情况下，SCP服务为关闭状态。

操作步骤	命令	说明
（可选）配置SSH服务器端的密钥交换算法列表	**ssh server key-exchange** { **dh_group14_sha256** | **dh_group15_sha512** | **dh_group16_sha512** | **dh_group_exchange_sha256** | **ecdh_sha2_nistp256**| **ecdh_sha2_nistp384**| **ecdh_sha2_nistp521** }*	缺省情况下，SSH服务器支持所有的密钥交换算法。 系统软件中不包含**dh_group_exchange_sha1**、**dh_group14_sha1**和**dh_group1_sha1**参数，如需使用，需要安装WEAKEA插件，但是该算法安全性低。为了保证更好的安全性，建议使用其它算法。WEAKEA插件安装方法请参见WEAKEA插件使用指南。
（可选）配置SSH服务器端的加密算法列表	**ssh server cipher** { **aes128_ctr** | **aes256_ctr** } *	缺省情况下，不安装WEAKEA插件，SSH服务器只支持**aes128_ctr**和**aes256_ctr**算法，不可以使用**undo ssh server cipher**命令，安装WEAKEA插件后，增加支持**aes256_cbc**、**aes128_cbc**、**3des_cbc**和**des_cbc**算法，并且可以使用**undo ssh server cipher**命令。 系统软件中不包含**aes256_cbc**、**aes128_cbc**、**3des_cbc**和**des_cbc**参数，如需使用，需要安装WEAKEA插件，但是该算法安全性低。为了保证更好的安全性，建议配置**aes256_ctr**或**aes128_ctr**参数。WEAKEA插件安装方法请参见WEAKEA插件使用指南。
（可选）配置SSH服务器上的校验算法列表	**ssh server hmac sha2_256**	缺省情况下，不安装WEAKEA插件，SSH服务器只支持**sha2_256**校验算法，不可以使用**undo ssh server hmac**命令，安装WEAKEA插件后，增加支持**sha2_256_96**、**sha1**、**sha1_96**、**md5**和**md5_96**校验算法，并且可以使用**undo ssh server hmac**命令。 系统软件中不包含**sha2_256_96**、**sha1**、**sha1_96**、**md5**和**md5_96**参数，如需使用，需要安装WEAKEA插件，但是该算法安全性低。为了保证更好的安全性，建议配置**sha2_256**参数。WEAKEA插件安装方法请参见WEAKEA插件使用指南。

操作步骤	命令	说明
（可选）配置与SSH客户端进行Diffie-hellman-group-exchange密钥交换时，支持的最小密钥长度	**ssh server dh-exchange min-len** *min-len*	缺省情况下，SSH服务器与客户端进行Diffie-hellman-group-exchange密钥交换时，支持的最小密钥长度为1024字节。
（可选）端口号	**ssh [ipv4 | ipv6] server port** *port-number*	缺省情况下，SSH服务器的端口号是22。 如果配置了新的端口号，SSH服务器端先断开当前已经建立的所有SSH连接，然后使用新的端口号开始尝试连接。这样可以有效防止攻击者对SSH服务标准端口的访问，确保安全性。
（可选）服务器密钥对更新时间	**ssh server rekey-interval** *hours*	缺省情况下，SSH服务器密钥对的更新时间间隔为0，表示永不更新。 配置服务器密钥对更新时间，使得当SSH服务器的更新周期到达时，自动更新服务器密钥对，从而可以保证安全性。 该命令只在SSH1.X版本生效。SSH1.X的安全性较低，不推荐使用。
（可选）配置SSH服务器重协商密钥时的参数	**ssh server rekey** { **time** *rekey-time* | **data-limit** *data-limit* | **max-packet** *max-packet* } *	缺省情况下，SSH服务器触发密钥重协商的时间间隔为60分钟，重协商密钥时收发数据大小上限为1000MB，重协商密钥时收发数据包个数上限为268435456（2^28）个。
（可选）指定SSH服务器的公钥算法	**ssh server publickey** { **dsa** | **ecc** | **rsa** | **rsa_sha2_256** | **rsa_sha2_512** } *	缺省情况下，DSA、ECC、RSA、RSA_SHA2_256、RSA_SHA2_512公钥算法都是开启的。
（可选）SSH认证超时时间	**ssh server timeout** *seconds*	缺省情况下，SSH连接认证超时时间为60秒。
（可选）SSH验证重试次数	**ssh server authentication-retries** *times*	缺省情况下，SSH连接的验证重试次数为3。
（可选）配置访问控制列表	**ssh** [**ipv6**] **server acl** *acl-number*	缺省情况下，没有配置访问控制列表。 配置了访问控制列表，可控制哪些客户端能以SSH方式访问本设备。

- 生成本地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，二者分别包括一个公钥和一个私钥。服务器密钥对和主机密钥对的长度均为2048位。
- 生成本地DSA密钥对时，只生成一个主机密钥对，长度可为1024、2048。缺省情况下，密钥对的长度为2048位。
- 生成本地ECC密钥对时，只生成一个主机密钥对，长度可为256、384、521。缺省情况下，密钥对的长度为521位。

- **配置SSH用户登录的用户界面**

  使用SCP协议，用户将通过VTY用户界面登录设备，所以需要配置VTY用户界面的相关属性。

  表 8-23 配置 SSH 用户登录的用户界面

操作步骤	命令	说明
进入系统视图	**system-view**	-
进入VTY用户界面视图	**user-interface vty** *first-ui-number* [*last-ui-number*]	-
配置VTY用户界面的验证方式为AAA	**authentication-mode aaa**	缺省情况下，VTY用户界面没有验证方式。 必须配置VTY用户界面验证方式为AAA验证，否则**protocol inbound ssh**不能配置成功，用户也将无法登录设备。
配置VTY用户界面支持SSH协议	**protocol inbound ssh**	缺省情况下，用户界面支持的协议是SSH。 如果不配置某个或某几个VTY用户界面支持SSH协议，则SSH用户不能登录设备。
配置VTY用户界面的用户优先级	**user privilege level** *level*	必须将用户级别配置为3级及3级以上，否则连接不成功。 如果是password认证用户，还可以执行**local-user** *user-name* **privilege level** *level*命令配置本地用户的用户级别为3级及3级以上。

操作步骤	命令	说明
（可选）VTY用户界面其他属性	-	除配置VTY用户界面的验证方式和用户优先级外，VTY用户界面的其他属性包括： ● VTY用户界面的最大个数 ● VTY用户界面的呼入呼出限制 ● VTY用户界面的终端属性 请参见**6.6 配置通过STelnet登录设备**–其他功能命令。

- **配置SSH用户**

  配置SSH用户包括配置SSH用户的验证方式，设备支持的认证方式包括RSA、password、password-rsa、DSA、password-dsa、ECC、password-ecc和all。其中：

  – password-rsa认证需要同时满足password认证和RSA认证。
  – password-dsa认证需要同时满足password认证和DSA认证。
  – password-ecc认证需要同时满足password认证和ECC认证。
  – all认证是指password认证、RSA、DSA或ECC认证方式满足其中一种即可。

  表 8-24 配置 SSH 用户

操作步骤	命令	说明
进入系统视图	**system-view**	-
创建SSH用户	**ssh user** *user-name*	-

操作步骤	命令	说明
配置SSH用户的认证方式	**ssh user** *user-name* **authentication-type** { **password** | **rsa** | **password-rsa** | **dsa** | **password-dsa** | **ecc** | **password-ecc** | **all** }	如果没有使用**ssh user**命令配置相应的SSH用户，则可以直接执行**ssh authentication-type default password**命令为用户配置SSH认证缺省采用密码认证，在用户数量比较多时，对用户使用缺省密码认证方式可以简化配置，此时只需再配置AAA用户即可。 **说明** 当认证方式为all认证时，用户的优先级需根据接入用户选择的认证方式来决定： • 如果接入用户选择的认证方式为password认证，则用户优先级为AAA中设置的用户优先级。 • 如果接入用户选择的认证方式为RSA、DSA或ECC认证，则用户的优先级由用户接入时所采用的VTY界面的优先级决定。 如果SSH用户认证方式为all认证，且存在一个同名AAA用户，那通过这两种方式接入时用户优先级可能不同，请根据需要进行部署。
配置SSH用户的服务方式为all	**ssh user** *username* **service-type all**	缺省情况下，SSH用户的服务方式是空，即不支持任何服务方式。

- password认证依靠AAA实现，当用户使用password、password-rsa、password-dsa或password-ecc认证方式登录设备时，需要在AAA视图下创建同名的本地用户。
- 如果SSH用户使用password认证，则只需要在SSH服务器端生成本地RSA、DSA或ECC密钥。如果SSH用户使用RSA、DSA或ECC认证，则在服务器端和客户端都需要生成本地RSA、DSA或ECC密钥对，并且服务器端和客户端都需要将对方的公钥配置到本地。

根据上面配置的认证方式，进行选择配置：

- 若对SSH用户进行password认证，请根据**表8-25**进行配置。
- 若对SSH用户进行RSA、DSA或ECC认证，请根据**表8-26**进行配置。
- 若对SSH用户进行password-rsa、password-dsa或password-ecc认证，则AAA用户和RSA、DSA或ECC公共密钥都需要进行配置。即同时配置**表8-25**和**表8-26**。

表 8-25 配置对 SSH 用户进行 password、password-rsa、password-dsa 或 password-ecc 认证

操作步骤	命令	说明
进入系统视图	**system-view**	-
进入AAA视图	**aaa**	-
配置本地用户名和密码	**local-user** *user-name* **password irreversible-cipher** *password*	-
配置本地用户的服务方式	**local-user** *user-name* **service-type ssh**	-
配置本地用户的级别	**local-user** *user-name* **privilege level** *level*	-
退回到系统视图	**quit**	-

表 8-26 配置对 SSH 用户进行 dsa、rsa、ecc、password-dsa、password-rsa 或 password-ecc 认证

操作步骤	命令	说明
进入系统视图	**system-view**	-
进入RSA、DSA或ECC公共密钥视图	**rsa peer-public-key** *key-name* [**encoding-type** { **der** | **openssh** | **pem** }] 、 **dsa peer-public-key** *key-name* **encoding-type** { **der** | **openssh** | **pem** } 或 **ecc peer-public-key** *key-name* **encoding-type** { **der** | **openssh** | **pem** }	-
进入公共密钥编辑视图	**public-key-code begin**	-

操作步骤	命令	说明
编辑公共密钥	*hex-data*	• 键入的公共密钥必须是按公钥格式编码的十六进制字符串，由支持SSH的客户端软件生成。具体操作参见相应的SSH客户端软件的帮助文档。 • 请将RSA、DSA或ECC公钥输入到作为SSH服务器的设备上。
退出公共密钥编辑视图	**public-key-code end**	• 如果未输入合法的密钥编码hex-data，执行本步骤后，将无法生成密钥。 • 如果指定的密钥*key-name*已经在别的窗口下被删除，再执行本步骤时，系统会提示：密钥已经不存在，此时直接退到系统视图。
退出公共密钥视图，回到系统视图	**peer-public-key end**	-
为SSH用户分配RSA、DSA或ECC公钥	**ssh user** *user-name* **assign** { **rsa-key** | **dsa-key** | **ecc-key** } *key-name*	-

- **用户通过SCP进行文件操作**

  从终端通过SCP方式上传或下载文件，需要在终端上安装支持SCP的SSH客户端软件。此处以使用第三方软件OpenSSH和Windows命令行提示符为例进行配置。

  – OpenSSH软件的安装请参考该软件的安装说明。
  – 使用OpenSSH软件从终端访问设备时，需要使用OpenSSH的命令，命令的使用可以参见该软件的帮助文档。
  – 只有安装了OpenSSH软件后，Windows命令行提示符才能识别OpenSSH相关命令。

  进入Windows的命令行提示符，执行OpenSSH命令，通过SCP方式进行文件操作。(以下显示信息仅为示意)

```
C:\Documents and Settings\Administrator> scp scpuser@10.136.23.5:flash:/vrpcfg.zip vrpcfg-backup.zip
The authenticity of host '10.136.23.5 (10.136.23.5)' can't be established.
DSA key fingerprint is 46:b2:8a:52:88:42:41:d4:af:8f:4a:41:d9:b8:4f:ee.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.136.23.5' (DSA) to the list of known hosts.

User Authentication
Password:
```

```
vrpcfg.zip                                100% 1257     1.2KByte(s)/sec   00:00
Received disconnect from 10.136.23.5: 2: The connection is closed by SSH server


C:\Documents and Settings\Administrator>
```

可以看到，用户终端通过SCP方式，在与远端设备建立连接的同时完成了文件上传或下载的操作，最后又回到了用户本地路径。

说明

由于文件系统对根目录下的文件个数有限制，当根目录中文件个数大于50个时，继续在根目录中创建文件可能会失败。

----结束

检查配置结果

- 使用**display ssh user-information** [*username*]命令，在SSH服务器端查看SSH用户信息。
- 使用**display ssh server status**命令，查看SSH服务器的全局配置信息。
- 使用**display ssh server session**命令，在SSH服务器端查看SSH客户端连接会话信息。

8.3.5 通过 FTPS 进行文件操作

前置任务

在配置通过FTPS进行文件操作之前，需完成以下任务：

- 终端与设备之间路由可达。
- 终端上已经安装支持SSL的FTP客户端软件。

配置流程

通过FTPS进行文件操作的配置流程如表8-27所示。

说明

从V200R020C00版本开始，当需要授权客户可以登录服务器时，必须执行命令指定服务器端的源接口或源地址。

表 8-27 通过 FTPS 进行文件操作的配置流程

序号	配置任务名称	配置任务说明	配置流程说明
1	上传服务器数字证书文件及私钥文件	通过其他文件上传方式将数字证书文件和私钥文件上传至设备。	序号1、2、3、4配置任务中，加载数字证书（序号2）前必须先上传数字证书（序号1），其他无严格配置顺序。
2	配置SSL策略并加载数字证书	包括配置SSL策略及在服务器上加载数字证书。	

序号	配置任务名称	配置任务说明	配置流程说明
3	配置FTPS服务器功能及FTP服务参数	包括为FTPS服务器配置SSL策略、源地址、FTPS服务器的使能及FTP服务参数的配置：端口号、超时断连时间。	
4	配置FTP本地用户	包括配置本地用户的服务类型及FTP用户的授权目录。	
5	用户通过FTPS访问设备	从终端通过FTPS访问设备。	-

缺省配置

表 8-28 缺省配置

参数	缺省值
SSL策略	没有为FTPS服务创建SSL策略
FTPS服务器功能	关闭
端口号	21
FTP用户	没有创建本地用户

操作步骤

- **上传服务器数字证书文件及私钥文件**

  可使用SFTP或SCP方式将服务器数字证书文件和私钥文件上传至设备，且要保存至security中，如设备无此目录，可执行命令**mkdir** *directory*创建。

  服务器需要从证书颁发中心CA（Certificate Authority）获得数字证书文件（包括私钥文件），访问服务器的客户端也需要从CA得到CA证书，用来验证服务器数字证书的有效性。

  说明

  CA是负责发放和管理数字证书的权威机构，当前FTPS服务器上加载的数字证书必须向CA申请。

  证书格式分为PEM格式、ASN1格式和PFX格式。虽然证书的格式不相同，但是证书的内容一样。

  - PEM格式的证书是最常用的一种数字证书格式，文件的扩展名是.pem，适用于系统之间的文本模式传输。
  - ASN1是通用的数字证书格式之一，文件的扩展名是.der，是大多数浏览器的默认格式。

- PFX是通用的数字证书格式之一，文件的扩展名是.pfx，是可移植的二进制格式。

具体的操作步骤请参考手册中其他文件上传方式的介绍。

- **配置SSL策略并加载数字证书文件**

  加载数字证书文件的同时指定私钥文件。

  表 8-29 配置 SSL 策略并加载数字证书

操作步骤	命令	说明
进入系统视图	**system-view**	-
（可选）定制SSL算法套	**ssl cipher-suite-list** *customization-policy-name*	创建SSL算法套定制策略并进入定制策略视图。 缺省情况下，没有配置SSL算法套定制策略。

操作步骤	命令	说明
	set cipher-suite { **tls12_ck_dss_aes_128_gcm_sha256** | **tls12_ck_dss_aes_256_gcm_sha384** | **tls12_ck_rsa_aes_128_gcm_sha256** | **tls12_ck_rsa_aes_256_gcm_sha384** | }	配置SSL算法套定制策略中支持的算法套。 缺省情况下，SSL算法套定制策略中没有配置算法套。 配置算法套定制策略中支持的算法套后，SSL协商时将使用定制策略中配置的策略进行协商。 如果算法套定制策略已经被SSL策略引用，可以对算法套进行增加、修改和部分删除，但不能将算法套定制策略中的算法套全部删除。 系统软件中不包含**tls12_ck_rsa_aes_256_cbc_sha256**、**tls1_ck_dhe_dss_with_aes_128_sha**、**tls1_ck_dhe_dss_with_aes_256_sha**、**tls1_ck_dhe_rsa_with_aes_128_sha**、**tls1_ck_dhe_rsa_with_aes_256_sha**、**tls1_ck_rsa_with_aes_128_sha**和**tls1_ck_rsa_with_aes_256_sha**参数，如需使用，需要安装WEAKEA插件，但是该算法安全性低。为了保证更好的安全性，建议使用其它算法。WEAKEA插件安装方法请参见WEAKEA插件使用指南。
	quit	返回系统视图。
配置SSL策略并进入SSL策略视图	**ssl policy** *policy-name*	-
（可选）设置SSL策略所采用的最低SSL版本	**ssl minimum version** { **tls1.1** | **tls1.2** | **tls1.3** }	缺省情况下，SSL策略所采用的最低SSL版本为TLS1.2。 系统软件中不包含**tls1.0**参数，如需使用，需要安装WEAKEA插件，但是该算法安全性低。为了保证更好的安全性，建议配置**tls1.2**参数。WEAKEA插件安装方法请参见WEAKEA插件使用指南。

操作步骤	命令	说明
（可选）在SSL策略中绑定指定的SSL算法套定制策略	**binding cipher-suite-customization** *customization-policy-name*	缺省情况下，SSL策略未绑定算法套定制策略，使用默认的算法套。SSL策略默认支持如下算法套： ● tls1_ck_rsa_with_aes_256_sha ● tls1_ck_rsa_with_aes_128_sha ● tls1_ck_dhe_rsa_with_aes_256_sha ● tls1_ck_dhe_dss_with_aes_256_sha ● tls1_ck_dhe_rsa_with_aes_128_sha ● tls1_ck_dhe_dss_with_aes_128_sha ● tls12_ck_rsa_aes_256_cbc_sha256 绑定的SSL算法套定制策略中如果仅有一种类型的算法（RSA或DSS），SSL策略需要加载对应类型的证书，确保SSL协商时能成功。
加载PEM格式的证书	**certificate load pem-cert** *cert-filename* **key-pair** { **dsa** | **rsa** } **key-file** *key-filename* **auth-code cipher** *auth-code*	根据证书类型，选其一。 **说明** ● 一个SSL策略只能加载一个证书或者证书链。如果已经加载了证书或者证书链，加载新证书或者证书链之前必须先卸载旧证书或者证书链。 ● 配置SSL策略加载证书或证书链时，证书或证书链中密钥对长度最大为2048位。如果该长度超过2048位，证书文件或证书链文件将无法上传到设备中使用。 ● 从V200R008C00及之后版本降级至以前版本时，需要先备份当前配置中加载的SSL私钥文件。
加载ASN1格式的证书	**certificate load asn1-cert** *cert-filename* **key-pair** { **dsa** | **rsa** } **key-file** *key-filename*	
加载PFX格式的证书	**certificate load pfx-cert** *cert-filename* **key-pair** { **dsa** | **rsa** } { **mac cipher** *mac-code* | **key-file** *key-filename* } **auth-code cipher** *auth-code*	
加载PEM格式的证书链	**certificate load pem-chain** *cert-filename* **key-pair** { **dsa** | **rsa** } **key-file** *key-filename* **auth-code cipher** *auth-code*	

- **配置FTPS服务器功能及FTP服务参数**

  基于FTP协议的FTPS，除了配置FTPS服务器功能外，还可以对FTP服务参数进行配置。

  表 8-30 配置 FTPS 服务器功能及 FTP 服务参数

操作步骤	命令	说明
进入系统视图	**system-view**	-
（可选）指定FTP服务器端口号	**ftp** [**ipv6**] **server port** *port-number*	缺省情况下，FTP服务器端口号是21。 如果配置了新的端口号，FTP服务器端先断开当前已经建立的所有FTP连接，然后使用新的端口号开始尝试连接。这样可以有效防止攻击者对FTP服务标准端口的访问。
为FTPS服务器配置SSL策略	**ftp secure-server ssl-policy** *policy-name*	此处配置的SSL策略即为上个操作步骤中创建的SSL策略。
指定FTP服务器的源地址	• **ftp server-source** { **-a** *source-ip-address* | **-i** *interface-type interface-number* } • **ftp ipv6 server-source -a** *ipv6_address* [**vpn-instance** *vpn_name*]	缺省情况下，未指定FTP服务器的源地址。 配置了服务器的源地址后，登录服务器时，所输入的服务器地址必须与该命令中配置的一致，否则无法成功登录。
使能FTPS服务器功能	**ftp** [**ipv6**] **secure-server enable**	缺省情况下，未使能FTPS服务器。 **说明** 使能FTPS服务功能前，必须去使能FTP服务器功能。
（可选）配置FTP连接空闲时间	**ftp** [**ipv6**] **timeout** *minutes*	缺省情况下，连接空闲时间为10分钟。 在设定的时间内，如果FTP连接始终处于空闲状态时，系统将自动断开FTP连接。
（可选）设置FTP服务器支持的最大会话数	**ftp** [**ipv6**] **server max-sessions** *max-sessions-number*	缺省情况下，FTP服务器支持的最大会话数是5。

说明

- 如果变更端口号前FTPS服务已经启动，则不能变更成功。需执行**undo ftp** [**ipv6**] **secure-server**命令关闭FTPS服务，再进行端口号变更。
- 当客户端与设备之间的文件操作结束后，请执行**undo ftp** [**ipv6**] **secure-server**命令，及时关闭FTPS服务器功能，从而保证设备的安全。

- **配置FTP本地用户**

  当用户通过FTPS进行文件操作时，需要在作为FTPS服务器的设备上配置本地用户名及口令，指定用户的服务类型以及可以访问的目录。否则用户将无法访问设备。

  表 8-31 配置 FTP 本地用户

操作步骤	命令	说明
进入系统视图	**system-view**	-
进入AAA视图	**aaa**	-
配置本地用户名和密码	**local-user** *user-name* **password irreversible-cipher** *password*	-
配置本地用户级别	**local-user** *user-name* **privilege level** *level*	**说明** 必须将用户级别配置在3级或3级以上，否则FTP连接将无法成功。
配置本地用户的服务类型为FTP	**local-user** *user-name* **service-type ftp**	缺省情况下，本地用户可以使用所有的接入类型。
配置FTP用户的授权目录	**local-user** *user-name* **ftp-directory** *directory*	缺省情况下，本地用户的FTP目录为空。 当有多个FTP用户且有相同的授权目录时，可以执行**set default ftp-directory** *directory*命令，为FTP用户配置缺省工作目录。此时，不需要通过**local-user** *user-name* **ftp-directory** *directory*命令为每个用户配置授权目录。
配置本地用户的FTP权限	**local-user** *user-name* **ftp-privilege** [*directoryfilename*] { **read** | **write** | **execute** }*	缺省情况下，本地用户的FTP权限为读、写和执行权限。

- **用户通过FTPS访问设备**

  需要在用户终端安装支持SSL的FTP客户端软件，通过第三方软件从用户终端登录FTPS服务器，实现对FTPS服务器进行文件的安全管理。

说明

由于文件系统对根目录下的文件个数有限制，当根目录中文件个数大于50个时，继续在根目录中创建文件可能会失败。

----结束

检查配置结果

- 使用**display ssl policy**命令，查看配置的SSL策略及加载的数字证书。
- 使用**display [ipv6] ftp-server**命令，查看FTPS服务器的状态。
- 使用**display ftp-users**命令，查看登录的FTP用户信息。

8.4 访问其他设备的文件

8.4.1 配置设备作为 TFTP 客户端访问其他设备的文件

前置任务

在配置通过TFTP访问其他设备的文件之前，需完成以下任务：

- 当前设备和TFTP服务器路由可达。
- 已获取TFTP服务器的主机名或IP地址以及下载或上传文件所在的目录。

配置流程

说明

使用TFTP协议存在安全风险，建议使用SFTP V2、SCP或FTPS方式进行文件操作。

通过TFTP访问其他设备文件的配置流程如**表8-32**所示。

表 8-32 配置设备作为 TFTP 客户端访问其他设备文件的配置流程

序号	配置任务名称	配置任务说明	配置流程说明
1	（可选）配置TFTP客户端源地址	客户端源地址可以配置为源接口或源IP，达到安全校验的目的。	在执行任务3前，任务1、2之间没有严格的配置顺序。
2	（可选）配置TFTP访问限制	包括配置ACL（Access Control List）规则及TFTP基本访问控制列表，提高TFTP访问的安全性。	
3	使用TFTP命令向其他设备上传或下载文件	包括文件的上传和下载操作。	

操作步骤

- **（可选）配置TFTP客户端源地址**

  配置源地址需要选择设备上状态稳定的接口，如LoopBack接口。该配置简化了ACL规则和安全策略的配置，只要将ACL规则的源地址或目的地址指定为该地址，就可以屏蔽接口IP地址的差异以及接口状态的影响，实现对设备进出报文的过滤。

  表 8-33 （可选）配置 TFTP 客户端源地址

操作步骤	命令	说明
进入系统视图	**system-view**	-
配置TFTP客户端的源地址信息	**tftp client-source** { **-a** *source-ip-address* | **-i** *interface-type interface-number* }	源地址可以是源IP或源接口，如果是源接口，必须要为该接口配置IP地址，否则会导致TFTP连接建立失败。 缺省情况下，TFTP客户端发送报文的源地址为与TFTP服务器通信的出接口的IP地址，显示为0.0.0.0。

- **（可选）配置TFTP访问限制**

  ACL是一系列有顺序的规则组的集合，这些规则根据数据包的源地址、目的地址、端口号等来描述。ACL通过规则对数据包进行分类，这些规则应用到路由设备，路由设备根据这些规则判断哪些数据包可以接收，哪些数据包需要拒绝。

  每个ACL中可以定义多个规则，根据规则的功能分为基本ACL规则、高级ACL规则和二层ACL规则等。

  TFTP只支持基本访问控制列表（编号范围为2000～2999）。

  ACL规则：

  - 当ACL的rule配置为**permit**时，则允许本设备与匹配该rule规则的其他设备建立TFTP连接。
  - 当ACL的rule配置为**deny**时，则拒绝本设备与匹配该rule规则的其他设备建立TFTP连接。

  表 8-34 （可选）配置 TFTP 访问限制

操作步骤	命令	说明
进入系统视图	**system-view**	-
创建一个ACL访问控制列表，并进入ACL视图	**acl** [**number**] *acl-number*	缺省情况下，未创建ACL访问控制列表。

操作步骤	命令	说明
配置ACL规则	**rule** [*rule-id*] { **deny** | **permit** } [**source** { *source-address source-wildcard* | **any** } | **fragment** | **logging** | **time-range** *time-name* | { **vpn-instance** *vpn-instance-name* | **public** }] *	缺省情况下，ACL视图下没有配置规则。 **说明** 仅S5720I-SI、S5735-S、S5735S-S、S5735-S-I、S5735S-H、S5736-S、S5731-H-K、S5731-H、S5731-S、S5731S-H、S5731S-S、S5732-H、S5732-H-K、S6735-S、S6720-EI、S6720S-EI、S6720S-S、S6730-H-K、S6730-H、S6730S-H、S6730-S和S6730S-S应用为软件ACL时才支持**vpn-instance**和**public**参数。软件ACL的应用场景请参见《S300, S500, S2700, S5700, S6700 V200R022C00 配置指南-安全》ACL配置 - ACL的基本原理中的“**ACL的实现方式**”。
退回到系统视图	**quit**	-
配置TFTP访问限制	**tftp-server** [**ipv6**] **acl** *acl-number*	-

- **使用TFTP命令向其他设备上传文件或从其他设备下载文件**

操作步骤	命令	说明
IPv4地址	**tftp** [**-a** *source-ip-address* | **-i** *interface-type interface-number*] *tftp-server* [**public-net** | **vpn-instance** *vpn-instance-name*] { **get** | **put** } *source-filename* [*destination-filename*]	• **get**表示从其他设备下载文件操作。 • **put**表示向其他设备上传文件操作。
IPv6地址	**tftp ipv6** [**-a** *source-ip-address*] *tftp-server-ipv6* [**-oi** *interface-type interface-number*] { **get** | **put** } *source-filename* [*destination-filename*]	

说明

由于文件系统对根目录下的文件个数有限制，当根目录中文件个数大于50个时，继续在根目录中创建文件可能会失败。

此命令中指定的源地址或者接口优先级高于**tftp client-source**命令中指定的源地址或者接口。如果执行命令**tftp client-source**指定了源地址或者接口，又在**tftp**命令中指定了源地址或者接口，则采用**tftp**命令中指定的源地址或者接口进行通信。**tftp client-source**命令指定的源地址或者接口对所有的TFTP连接都有效，**tftp**命令指定的源地址或者接口只对当前的TFTP连接有效。

----结束

检查配置结果

- 执行**display tftp-client**命令，查看设备作为TFTP客户端时的源地址。
- 执行**display acl** { *acl-number* | **all** }命令，查看TFTP客户端配置的ACL规则。

8.4.2 配置设备作为 FTP 客户端访问其他设备的文件

前置任务

在配置通过FTP访问其他设备的文件之前，需完成以下任务：

- 当前设备和FTP服务器路由可达。
- 已获取FTP服务器的主机名或IP地址、FTP用户名及密码。
- 如果服务器不是使用标准的端口号，则还需获取服务器端设置的端口号。

配置流程

须知

使用FTP协议存在安全风险，建议使用SFTP V2、SCP或FTPS方式进行文件操作。

从V200R020C00版本开始，缺省情况下FTP服务器端不接收来自任何接口登录连接的IPv4和IPv6请求，当需要授权客户可以登录服务器时，必须执行命令指定服务器端的源接口或源地址。

通过FTP访问其他设备文件的配置流程如表8-35所示。

表 8-35 配置设备作为 FTP 客户端访问其他设备的文件配置流程

序号	配置任务名称	配置任务说明	配置流程说明
1	（可选）配置FTP客户端源地址	客户端源地址可以配置为源接口或源IP，达到安全校验的目的。	序号1、2有序操作，FTP连接建立后，序号3、4无操作顺序，序号5（断开连接操作）为最后一步。
2	使用FTP连接其他设备	-	

序号	配置任务名称	配置任务说明	配置流程说明
3	通过FTP文件操作命令进行文件操作	包括目录操作、文件操作、配置文件传输方式、查看FTP命令在线帮助等。	
4	（可选）更改登录用户	-	
5	断开与FTP服务器的连接	-	

操作步骤

- **（可选）配置FTP客户端源地址**

  配置源地址需要选择设备上状态稳定的接口，如LoopBack接口。该配置简化了ACL规则和安全策略的配置，只要将ACL规则的源地址或目的地址指定为该地址，就可以屏蔽接口IP地址的差异以及接口状态的影响，实现对设备进出报文的过滤。

  FTP客户端配置的源地址必须为LoopBack地址或LoopBack接口。

  表 8-36 配置 FTP 客户端源地址

操作步骤	命令	说明
进入系统视图	**system-view**	-
配置FTP客户端的源地址信息	**ftp client-source** { **-a** *source-ip-address* | **-i** *interface-type interface-number* }	建议使用Loopback接口的地址。 当配置为LoopBack接口时，一定要为此接口配置IP地址，否则会导致FTP连接建立失败。

- **使用FTP连接其他设备**

  在用户视图和FTP客户端视图下，用户均可以使用相应命令访问FTP服务器。

  根据服务器端IP地址类型不同，进行如下操作。

  表 8-37 使用 FTP 命令连接其他设备（服务器端 IPv4 地址类型）

操作步骤	命令	说明
用户视图下直接建立与IPv4 FTP服务器的连接	**ftp** [**-a** *source-ip-address* | **-i** *interface-type interface-number*] *host-ip* [*port-number*] [**public-net** | **vpn-instance** *vpn-instance-name*]	二选一 FTP客户端视图下建立与FTP服务器的连接时需要先使用**ftp**命令进入FTP客户端视图。

操作步骤	命令	说明
FTP客户端视图下建立与IPv4 FTP服务器的连接	**ftp**	
	open [**-a** *source-ip-address* | **-i** *interface-type interface-number*] *host-ip* [*port-number*] [**public-net** | **vpn-instance** *vpn-instance-name*]	

说明

- 在访问FTP服务器之前，可以执行命令**set net-manager vpn-instance**，设置默认的VPN实例。执行该命令后，进行FTP操作时所使用的VPN实例即用户配置的默认VPN实例。
- 基于IPV4网络中，**ftp**命令中指定的源地址优先级高于**ftp client-source**命令中指定源地址的优先级。如果执行命令**ftp client-source**指定了源地址后，又在**ftp**命令中指定了源地址，则采用**ftp**命令中指定的源地址进行通信。**ftp client-source**命令指定的源地址对所有的FTP连接都有效，**ftp**命令指定的源地址只对当前的FTP连接有效。

表 8-38 使用 FTP 命令连接其他设备（服务器端 IPv6 地址类型）

操作步骤	命令	说明
用户视图下直接建立与IPv6 FTP服务器的连接	**ftp ipv6** *host-ipv6* [*port-number*]	二选一 FTP客户端视图下建立与FTP服务器的连接时需要先使用**ftp**命令进入FTP客户端视图。
FTP客户端视图下建立与IPv6 FTP服务器的连接	**ftp**	
	open ipv6 *host-ipv6* [*port-number*]	

用户访问服务器时，需要经过验证，输入正确的用户名和密码后，方可访问服务器。

- **通过FTP命令进行文件操作**

  用户访问FTP服务器后，可以通过FTP命令进行文件操作，包括目录操作、文件操作、配置文件传输方式、查看FTP命令在线帮助等。

  说明

  用户的操作权限受限于服务器上对该用户的权限设置。

  由于文件系统对根目录下的文件个数有限制，当根目录中文件个数大于50个时，继续在根目录中创建文件可能会失败。

  以下各操作没有严格顺序，可根据需求选择一种或多种操作项目。

表 8-39 通过 FTP 命令进行文件操作

操作项目	命令	说明
改变服务器上的工作路径	**cd** *remote-directory*	-
改变服务器的工作路径到上一级目录	**cdup**	-
显示服务器工作路径	**pwd**	-
显示或者改变客户端的工作路径	**lcd** [*local-directory*]	与**pwd**不同的是，**lcd**命令执行后显示的是客户端的本地工作路径，而**pwd**显示的则是远端服务器的工作路径。
在服务器上创建目录	**mkdir** *remote-directory*	创建的目录可以为字母和数字等的组合，但不可以为<、>、？ 、\、： 等特殊字符。
在服务器上删除目录	**rmdir** *remote-directory*	-
显示服务器上指定目录或文件的信息	**dir/ls** [*remote-filename* [*local-filename*]]	• **ls**命令只能显示出目录/文件的名称，而**dir**命令可以查看目录/文件的详细信息，如大小，创建日期等。 • 如果指定远程文件时没有指定路径名称，那么系统将在用户的授权目录下搜索指定的文件。
删除服务器上指定文件	**delete** *remote-filename*	-
上传单个或多个文件	**put** *local-filename* [*remote-filename*] 或 **mput** *local-filenames*	• **put**命令是上传单个文件。 • **mput**命令是上传多个文件。
下载单个或多个文件	**get** *remote-filename* [*local-filename*] 或 **mget** *remote-filenames*	• **get**命令是下载单个文件。 • **mget**命令是下载多个文件。

操作项目	命令	说明
配置传输文件的数据类型为ASCII模式或二进制模式	**ascii** 或 **binary**	二选一 • 缺省情况下，文件传输方式为ASCII模式。 • 传输文本文件使用ASCII方式，传输程序、系统软件、数据库文件等使用二进制模式。
配置文件传输方式为被动方式或主动方式	**passive** 或 **undo passive**	二选一 缺省情况下，数据传输方式是主动方式。
查看FTP命令的在线帮助	**remotehelp** [*command*]	-
使能系统的提示功能	**prompt**	缺省情况下，不使能信息提示。
打开verbose开关	**verbose**	如果打开verbose开关，将显示所有FTP响应，包括FTP协议信息，以及FTP服务器返回的详细信息。

- **（可选）更改登录用户**

  设备可以在不退出FTP客户端视图的情况下，以其他的用户名登录到FTP服务器。所建立的FTP连接，与执行**ftp**命令建立的FTP连接完全相同。

操作步骤	命令	说明
FTP客户端视图下，更改当前的登录用户	**user** *user-name* [*password*]	更改当前的登录用户后，原用户与服务器的连接将断开。

- **断开与FTP服务器的连接**

  用户可以在FTP客户端视图中选择不同的命令断开与FTP服务器的连接。

操作步骤	命令	说明
终止与服务器的连接，并退回到用户视图	**bye** 或 **quit**	二选一。
终止与服务器的连接，并退回到FTP客户端视图	**close** 或 **disconnect**	

----结束

检查配置结果

- 使用**display ftp-client**命令，查看设备作为FTP客户端时的源参数。

8.4.3 配置设备作为 SFTP 客户端访问其他设备的文件

前置任务

在配置通过SFTP访问其他设备的文件之前，需完成以下任务：

- 当前设备和SSH服务器路由可达。
- 已获取SSH服务器的主机名或IP地址以及SSH用户信息。
- 如果服务器不是使用标准的端口号，则还需获取服务器端设置的端口号。

配置流程

须知

从V200R020C00版本开始，缺省情况下SFTP服务器端不接收来自任何接口登录连接的IPv4和IPv6请求，当需要授权客户可以登录服务器时，必须执行命令指定服务器端的源接口或源地址。

通过SFTP访问其他设备文件的配置流程如**表8-40**所示。

表 8-40 配置设备作为 SFTP 客户端访问其他设备文件的配置流程

序号	配置任务名称	配置任务说明	配置流程说明
1	（可选）配置SFTP客户端源地址	客户端源地址可以配置为源接口或源IP，达到安全校验的目的。	序号1、2、3无序操作，SFTP连接（序号4）建立后，可执行序号5的操作，最后断开连接（序号6）。
2	生成本地密钥对	生成本地密钥对，然后将公钥配置到SSH服务器上。 本步骤仅在设备以RSA、DSA或ECC方式登录SSH服务器的时候执行，password方式登录SSH服务器则无需执行。	
3	配置设备首次连接SSH服务器的方式	有两种配置方式：使能SSH客户端首次认证功能方式和SSH客户端为SSH服务器分配公钥方式，用户可选择其一进行配置。	

序号	配置任务名称	配置任务说明	配置流程说明
4	使用SFTP命令连接其他设备	-	
5	通过SFTP文件操作命令进行文件操作	用户可以通过SFTP客户端管理SSH服务器上的目录和文件，以及查看SFTP客户端命令帮助。	
6	断开与SFTP服务器的连接	-	

操作步骤

- **（可选）配置SFTP客户端源地址**

  配置源地址需要选择设备上状态稳定的接口，如LoopBack接口。该配置简化了ACL规则和安全策略的配置，只要将ACL规则的源地址或目的地址指定为该地址，就可以屏蔽接口IP地址的差异以及接口状态的影响，实现对设备进出报文的过滤。

  SFTP客户端配置的源地址必须为LoopBack地址或LoopBack接口。

  表 8-41 配置 SFTP 客户端源地址

操作步骤	命令	说明
进入系统视图	**system-view**	-
配置SFTP客户端的源地址信息	**sftp client-source** { **-a** *source-ip-address* | **-i** *interface-type interface-number* }	缺省情况下，源地址为0.0.0.0。 配置的源地址为设备的LoopBack地址或LoopBack接口。

- **生成本地密钥对**

  说明

  此步骤仅在设备以RSA、DSA或ECC方式登录SSH服务器的时候执行，设备以password方式登录SSH服务器，则无需执行。

  表 8-42 生成本地密钥对

操作步骤	命令	说明
进入系统视图	**system-view**	-

操作步骤	命令	说明
生成本地密钥对	**rsa local-key-pair create**、**dsa local-key-pair create**或**ecc local-key-pair create**	根据对端密钥的类型，三选一。 密钥对生成后，可以执行**display rsa local-key-pair public**、**display dsa local-key-pair public**或**display ecc local-key-pair public**命令查看RSA本地密钥对、DSA本地密钥对或ECC密钥对中的公钥部分信息，然后将公钥配置到SSH服务器上。

- **配置设备首次连接SSH服务器的方式**

  作为客户端的设备首次连接SSH服务器时，因为客户端还没有保存过SSH服务器的公钥，无法对SSH服务器有效性进行检查，这样会导致连接不成功。可以通过下面两种方式来解决：

  - 使能SSH客户端首次认证功能方式：不对SSH服务器的公钥进行有效性检查，确保首次连接成功。成功连接后，系统将自动分配并保存公钥，为下次连接时认证使用。具体配置见**表8-43**。此种方式配置简单。
  - SSH客户端配置服务器公钥方式：将服务器端产生的公钥直接保存至客户端，保证在首次连接时SSH服务器有效性检查能够通过。具体配置见**表8-44**。此种方式配置较复杂，但比上面那种方式安全性更高。

表 8-43 使能 SSH 客户端首次认证功能

操作步骤	命令	说明
进入系统视图	**system-view**	-
使能SSH客户端首次认证功能	**ssh client first-time enable**	缺省情况下，SSH客户端首次认证功能是关闭的。

表 8-44 SSH 客户端为 SSH 服务器分配 RSA、DSA 或 ECC 公钥方式

操作步骤	命令	说明
进入系统视图	**system-view**	-

操作步骤	命令	说明
进入RSA、DSA或ECC公共密钥视图	**rsa peer-public-key** *key-name* [**encoding-type** { **der** | **openssh** | **pem** }] 、 **dsa peer-public-key** *key-name* **encoding-type** { **der** | **openssh** | **pem** } 或 **ecc peer-public-key** *key-name* **encoding-type** { **der** | **openssh** | **pem** }	根据生成的密钥类型，三选一。
进入公共密钥编辑视图	**public-key-code begin**	-
编辑公共密钥	*hex-data*	● 键入的公共密钥必须是按公钥格式编码的十六进制字符串，由SSH服务器随机生成。 ● 进入公共密钥编辑视图后，即可将服务器上产生的RSA、DSA或ECC公钥输入到客户端。
退出公共密钥编辑视图	**public-key-code end**	● 如果输入的密钥编码hex-data不合法，执行本步骤后，将无法生成密钥。 ● 如果指定的密钥key-name已经被删除，再执行本步骤时，系统会提示：密钥已经不存在，此时直接退到系统视图。
退出公共密钥视图，回到系统视图	**peer-public-key end**	-
为SSH服务器绑定RSA、DSA或ECC公钥	**ssh client** *servername* **assign** { **rsa-key** | **dsa-key** | **ecc-key** } *keyname*	如果SSH客户端保存的SSH服务器公钥失效，执行命令**undo ssh client** *servername* **assign** { **rsa-key** | **dsa-key** | **ecc-key** }，取消SSH服务器与RSA、DSA或ECC公钥的绑定关系，再执行本命令，为SSH服务器重新分配RSA、DSA或ECC公钥。

- **使用SFTP命令连接其他设备**

SFTP客户端连接命令跟STelnet客户端连接命令很相似，支持访问SSH服务器时携带源地址，选择密钥交换算法、加密算法和HMAC算法，以及设置keepalive功能。

表 8-45 使用 SFTP 命令连接其他设备

操作步骤	命令	说明
进入系统视图	**system-view**	-
（可选）配置SSH客户端的密钥交换算法列表	**ssh client key-exchange** { **dh_group14_sha256** | **dh_group15_sha512** | **dh_group16_sha512** | **dh_group_exchange_sha256** | **ecdh_sha2_nistp256**| **ecdh_sha2_nistp384**| **ecdh_sha2_nistp521**}*	缺省情况下，SSH客户端支持所有的密钥交换算法。 系统软件中不包含**dh_group_exchange_sha1**、**dh_group14_sha1和dh_group1_sha1**参数，如需使用，需要安装WEAKEA插件，但是该算法安全性低。为了保证更好的安全性，建议使用其它算法。WEAKEA插件安装方法请参见WEAKEA插件使用指南。
（可选）配置SSH客户端的加密算法列表	**ssh client cipher** { **aes128_ctr** | **aes256_ctr** } *	缺省情况下，不安装WEAKEA插件，SSH客户端只支持**aes128_ctr**和**aes256_ctr**算法，不可以使用**undo ssh client cipher**命令，安装WEAKEA插件后，增加支持**aes256_cbc**、**aes128_cbc**、**3des_cbc**和**des_cbc**算法，并且可以使用**undo ssh client cipher**命令。 系统软件中不包含**aes256_cbc**、**aes128_cbc**、**3des_cbc**和**des_cbc**参数，如需使用，需要安装WEAKEA插件，但是该算法安全性低。为了保证更好的安全性，建议配置**aes256_ctr**或**aes128_ctr**参数。WEAKEA插件安装方法请参见WEAKEA插件使用指南。

操作步骤	命令	说明
（可选）配置SSH客户端上的校验算法列表	**ssh client hmac** { **sha2_256** }	缺省情况下，不安装WEAKEA插件，SSH客户端只支持**sha2_256**校验算法，不可以使用**undo ssh client hmac**命令，安装WEAKEA插件后，增加支持**sha2_256_96**、**sha1**、**sha1_96**、**md5**和**md5_96**校验算法，并且可以使用**undo ssh client hmac**命令。 系统软件中不包含**sha2_256_96**、**sha1**、**sha1_96**、**md5**和**md5_96**参数，如需使用，需要安装WEAKEA插件，但是该算法安全性低。为了保证更好的安全性，建议配置**sha2_256**参数。WEAKEA插件安装方法请参见WEAKEA插件使用指南。
（可选）配置SSH客户端重协商密钥时的参数	**ssh client rekey** { **time** *rekey-time* | **data-limit** *data-limit* | **max-packet** *max-packet* } *	缺省情况下，SSH客户端触发密钥重协商的时间间隔为60分钟，重协商密钥收发数据大小上限为1000MB，重协商密钥收发数据包个数上限为268435456（2^28）个。
IPv4地址	**sftp** [**-a** *source-address* | **-i** *interface-type interface-number*] *host-ip* [*port*] [[**public-net** | **-vpn-instance** *vpn-instance-name*] | **identity-key** { **dsa** | **rsa** | **ecc** | **rsa_sha2_256** | **rsa_sha2_512** } | **user-identity-key** { **rsa** | **dsa** | **ecc** } | **prefer_kex** *prefer_key-exchange* | **prefer_ctos_cipher** *prefer_ctos_cipher* | **prefer_stoc_cipher** *prefer_stoc_cipher* | **prefer_ctos_hmac** *prefer_ctos_hmac* | **prefer_stoc_hmac** *prefer_stoc_hmac*| **-ki** *aliveinterval*] | [**-kc** *alivecountmax*] *	根据地址类型选其一。 大多数情况下，该命令可以只指定IP地址，而不需要指定其他可选项。 **说明** 为了保证更好的安全性，建议您使用更安全的aes128或aes256算法作为客户端到服务器端的认证算法。

操作步骤	命令	说明
IPv6地址	**sftp ipv6** [**-a** *source-address*] *host-ipv6* [**-oi** *interface-type interface-number*] [*port*] [**identity-key** { **dsa** | **rsa** | **ecc** | **rsa_sha2_256** | **rsa_sha2_512** } | **user-identity-key** { **rsa** | **dsa** | **ecc** } | **-vpn-instance** *vpn-instance-name* | **prefer_kex** *prefer_key-exchange* | **prefer_ctos_cipher** *prefer_ctos_cipher* | **prefer_stoc_cipher** *prefer_stoc_cipher* | **prefer_ctos_hmac** *prefer_ctos_hmac* | **prefer_stoc_hmac** *prefer_stoc_hmac* | **-ki** *aliveinterval* | **-kc** *alivecountmax*] *	

例如：

```
[HUAWEI] sftp 10.137.217.201
```

连接成功后，屏幕会显示**sftp-client>**，此时已经进入了SFTP客户端视图。

- **通过SFTP命令进行文件操作**

  当SFTP客户端登录到SSH服务器之后，用户可以在SFTP客户端进行如表8-46所示的操作。

  以下各操作没有严格顺序，可根据需求选择一种或多种操作项目。

  说明

  在SFTP客户端视图下，文件操作命令不支持联想功能，必须手动输入完整的命令，否则会提示是不支持的命令。

  由于文件系统对根目录下的文件个数有限制，当根目录中文件个数大于50个时，继续在根目录中创建文件可能会失败。

表 8-46 通过 SFTP 文件操作命令进行文件操作

操作项目	命令	说明
改变用户的当前工作目录	**cd** [*remote-directory*]	-
改变用户的工作目录为当前工作目录的上一级目录	**cdup**	-
显示用户的当前工作目录	**pwd**	-

操作项目	命令	说明
显示指定目录下的文件列表	**dir/ls** [**-l** | **-a**] [*remote-directory*]	**dir**与**ls**执行的效果是一样的。
删除服务器上目录	**rmdir** *remote-directory* &<1-10>	一次最多可以删除十个目录。 使用该命令删除目录时，目录中不能有文件，否则会删除失败。
在服务器上创建新目录	**mkdir** *remote-directory*	-
改变服务器上指定的文件的名字	**rename** *old-name new-name*	-
下载远程服务器上的文件	**get** *remote-filename* [*local-filename*]	-
上传本地文件到远程服务器	**put** *local-filename* [*remote-filename*]	-
删除服务器上文件	**remove** *remote-filename* &<1-10>	一次最多可以删除十个文件。
SFTP客户端命令帮助	**help** [**all** | *command-name*]	-

用户也可以在系统视图下执行如下命令下载服务器上的文件或者上传本地文件到远程服务器中:

- IPv4地址：**sftp client-transfile** { **get** | **put** } [**-a** *source-address* | **-i** *interface-type interface-number*] **host-ip** *host-ipv4* [*port*] [[**public-net** | **-vpn-instance** *vpn-instance-name*] | **prefer_kex** *prefer_key-exchange* | **identity-key** { **rsa** | **dsa** | **ecc** } | **prefer_ctos_cipher** *prefer_ctos_cipher* | **prefer_stoc_cipher** *prefer_stoc_cipher* | **prefer_ctos_hmac** *prefer_ctos_hmac* | **prefer_stoc_hmac** *prefer_stoc_hmac* | **-ki** *aliveinterval* | **-kc** *alivecountmax*] * **username** *user-name* **password** *password* **sourcefile** *source-file* [**destination** *destination*]
- IPv6地址：**sftp client-transfile** { **get** | **put** } **ipv6** [**-a** *source-address*] **host-ip** *host-ipv6* [**-oi** *interface-type interface-number*] [*port*] [**-vpn-instance** *vpn-instance-name* | **prefer_kex** *prefer_key-exchange* | **identity-key** { **rsa** | **dsa** | **ecc** } | **prefer_ctos_cipher** *prefer_ctos_cipher* | **prefer_stoc_cipher** *prefer_stoc_cipher* | **prefer_ctos_hmac** *prefer_ctos_hmac* | **prefer_stoc_hmac** *prefer_stoc_hmac* | **-ki** *aliveinterval* | **-kc** *alivecountmax*] * **username** *user-name* **password** *password* **sourcefile** *source-file* [**destination** *destination*]

- **断开与SFTP服务器的连接**

操作步骤	命令	说明
断开与SFTP服务器的连接	**quit**	-

----结束

检查配置结果

- 使用**display sftp-client**命令，查看设备作为SFTP客户端时的源参数地址。
- 使用**display ssh server-info**命令，查看客户端所有的SSH服务器与公钥之间的对应关系。

8.4.4 配置设备作为 SCP 客户端访问其他设备的文件

前置任务

在配置通过SCP访问其他设备的文件之前，需完成以下任务：

- 当前设备和SSH服务器路由可达。
- 已获取SSH服务器的主机名或IP地址以及SSH用户信息。
- 如果服务器不是使用标准的端口号，则还需获取服务器端设置的端口号。

配置流程

须知

从V200R020C00版本开始，缺省情况下SCP服务器端不接收来自任何接口登录连接的IPv4和IPv6请求，当需要授权客户可以登录服务器时，必须执行命令指定服务器端的源接口或源地址。

通过SCP访问其他设备文件的配置流程如表8-47所示。

表 8-47 配置设备作为 SCP 客户端访问其他设备文件的配置流程

序号	配置任务名称	配置任务说明	配置流程说明
1	（可选）配置SCP客户端源地址	客户端源地址可以配置为源接口或源IP，达到安全校验的目的。	序号1、2、3之间没有严格的配置顺序。

序号	配置任务名称	配置任务说明	配置流程说明
2	生成本地密钥对	生成本地密钥对，然后将公钥配置到SSH服务器上。 本步骤仅在设备以RSA、DSA或ECC方式登录SSH服务器的时候执行，password方式登录SSH服务器则无需执行。	
3	配置设备首次连接SSH服务器的方式	有两种配置方式：使能SSH客户端首次认证功能方式和SSH客户端为SSH服务器分配公钥方式，用户可选择其一进行配置。	
4	使用SCP命令连接其他设备	-	

操作步骤

- **（可选）配置SCP客户端源地址**

表 8-48 （可选）配置 SCP 客户端源地址

操作步骤	命令	说明
进入系统视图	**system-view**	-
配置SCP客户端的源地址信息	**scp client-source** { **-a** *source-ip-address* | **-i** *interface-type interface-number* }	缺省情况下，没有配置源地址。

- **生成本地密钥对**

说明

此步骤仅在设备以RSA、DSA或ECC方式登录SSH服务器的时候执行，设备以password方式登录SSH服务器，则无需执行。

表 8-49 生成本地密钥对

操作步骤	命令	说明
进入系统视图	**system-view**	-

操作步骤	命令	说明
生成本地密钥对	**rsa local-key-pair create**、**dsa local-key-pair create**或**ecc local-key-pair create**	根据对端密钥的类型，三选一。 密钥对生成后，可以执行**display rsa local-key-pair public**、**display dsa local-key-pair public**或**display ecc local-key-pair public**命令查看RSA本地密钥对、DSA本地密钥对或ECC密钥对中的公钥部分信息，然后将公钥配置到SSH服务器上。

- **配置设备首次连接SSH服务器的方式**

  作为客户端的设备首次连接SSH服务器时，因为客户端还没有保存过SSH服务器的公钥，无法对SSH服务器有效性进行检查，这样会导致连接不成功。可以通过下面两种方式来解决：

  - 使能SSH客户端首次认证功能方式：不对SSH服务器的公钥进行有效性检查，确保首次连接成功。成功连接后，系统将自动分配并保存公钥，为下次连接时认证使用。具体配置见表8-43。此种方式配置简单。
  - SSH客户端配置服务器公钥方式：将服务器端产生的公钥直接保存至客户端，保证在首次连接时SSH服务器有效性检查能够通过。具体配置见表8-44。此种方式配置较复杂，但比上面那种方式安全性更高。

表 8-50 使能 SSH 客户端首次认证功能

操作步骤	命令	说明
进入系统视图	**system-view**	-
使能SSH客户端首次认证功能	**ssh client first-time enable**	缺省情况下，SSH客户端首次认证功能是关闭的。

表 8-51 SSH 客户端为 SSH 服务器分配 RSA、DSA 或 ECC 公钥方式

操作步骤	命令	说明
进入系统视图	**system-view**	-

操作步骤	命令	说明
进入RSA、DSA或ECC公共密钥视图	**rsa peer-public-key** *key-name* [**encoding-type** { **der** | **openssh** | **pem** }] 、 **dsa peer-public-key** *key-name* **encoding-type** { **der** | **openssh** | **pem** } 或 **ecc peer-public-key** *key-name* **encoding-type** { **der** | **openssh** | **pem** }	根据生成的密钥类型，三选一。
进入公共密钥编辑视图	**public-key-code begin**	-
编辑公共密钥	*hex-data*	● 键入的公共密钥必须是按公钥格式编码的十六进制字符串，由SSH服务器随机生成。 ● 进入公共密钥编辑视图后，即可将服务器上产生的RSA、DSA或ECC公钥输入到客户端。
退出公共密钥编辑视图	**public-key-code end**	● 如果输入的密钥编码hex-data不合法，执行本步骤后，将无法生成密钥。 ● 如果指定的密钥key-name已经被删除，再执行本步骤时，系统会提示：密钥已经不存在，此时直接退到系统视图。
退出公共密钥视图，回到系统视图	**peer-public-key end**	-
为SSH服务器绑定RSA、DSA或ECC公钥	**ssh client** *servername* **assign** { **rsa-key** | **dsa-key** | **ecc-key** } *keyname*	如果SSH客户端保存的SSH服务器公钥失效，执行命令**undo ssh client** *servername* **assign** { **rsa-key** | **dsa-key** | **ecc-key** }，取消SSH服务器与RSA、DSA或ECC公钥的绑定关系，再执行本命令，为SSH服务器重新分配RSA、DSA或ECC公钥。

- **使用SCP命令连接其他设备**

SCP与SFTP方式不同，当SCP命令执行后，与服务器建立安全连接，客户端可以直接上传文件至服务器或从服务器下载文件至本地。

表 8-52 使用 SCP 命令连接其他设备

操作步骤	命令	说明
进入系统视图	**system-view**	-
（可选）配置SSH客户端的密钥交换算法列表	**ssh client key-exchange** { **dh_group14_sha256** | **dh_group15_sha512** | **dh_group16_sha512** | **dh_group_exchange_sha256** | **ecdh_sha2_nistp256**| **ecdh_sha2_nistp384**| **ecdh_sha2_nistp521** }*	缺省情况下，SSH客户端支持所有的密钥交换算法。 系统软件中不包含**dh_group_exchange_sha1**、**dh_group14_sha1和dh_group1_sha1**参数，如需使用，需要安装WEAKEA插件，但是该算法安全性低。为了保证更好的安全性，建议使用其它算法。WEAKEA插件安装方法请参见WEAKEA插件使用指南。
（可选）配置SSH客户端的加密算法列表	**ssh client cipher** { **aes128_ctr** | **aes256_ctr** } *	缺省情况下，不安装WEAKEA插件，SSH客户端只支持**aes128_ctr**和**aes256_ctr**算法，不可以使用**undo ssh client cipher**命令，安装WEAKEA插件后，增加支持**aes256_cbc**、**aes128_cbc**、**3des_cbc**和**des_cbc**算法，并且可以使用**undo ssh client cipher**命令。 系统软件中不包含**aes256_cbc**、**aes128_cbc**、**3des_cbc**和**des_cbc**参数，如需使用，需要安装WEAKEA插件，但是该算法安全性低。为了保证更好的安全性，建议配置**aes256_ctr**或**aes128_ctr**参数。WEAKEA插件安装方法请参见WEAKEA插件使用指南。

操作步骤	命令	说明
（可选）配置SSH客户端上的校验算法列表	**ssh client hmac sha2_256**	缺省情况下，不安装WEAKEA插件，SSH服务器只支持**sha2_256**校验算法，不可以使用**undo ssh server hmac**命令，安装WEAKEA插件后，增加支持**sha2_256_96**、**sha1**、**sha1_96**、**md5**和**md5_96**校验算法，并且可以使用**undo ssh server hmac**命令。 系统软件中不包含**sha2_256_96**、**sha1**、**sha1_96**、**md5**和**md5_96**参数，如需使用，需要安装WEAKEA插件，但是该算法安全性低。为了保证更好的安全性，建议配置**sha2_256**参数。 WEAKEA插件安装方法请参见WEAKEA插件使用指南。
（可选）配置SSH客户端重协商密钥时的参数	**ssh client rekey** { **time** *rekey-time* | **data-limit** *data-limit* | **max-packet** *max-packet* } *	缺省情况下，SSH客户端触发密钥重协商的时间间隔为60分钟，重协商密钥收发数据大小上限为1000MB，重协商密钥收发数据包个数上限为268435456（2^28）个。
IPv4地址	**scp** [**-port** *port-number* | { **public-net** | **vpn-instance** *vpn-instance-name* } | **identity-key** { **dsa** | **rsa** | **ecc** | **rsa_sha2_256** | **rsa_sha2_512** } | **user-identity-key** { **rsa** | **dsa** | **ecc** } | { **-a** *source-address* | **-i** *interface-type interface-number* } | **-r** | **-cipher** *cipher* | **-c**] * *sourcefile destinationfile*	根据地址类型选其一。 **说明** 在使用中需要注意，为了安全性考虑，用户选择加密算法时，建议采用aes128或aes256算法。

操作步骤	命令	说明
IPv6地址	**scp ipv6** [**-port** *port-number* | { **public-net** | **vpn-instance** *vpn-instance-name* } | **identity-key** { **dsa** | **rsa** | **ecc** | **rsa_sha2_256** | **rsa_sha2_512** } | **user-identity-key** { **rsa** | **dsa** | **ecc** } | **-a** *source-address* | **-r** | **-cipher** *-cipher* | **-c**] * *sourcefile destinationfile* [**-oi** *interface-type interface-number*]	

说明

由于文件系统对根目录下的文件个数有限制，当根目录中文件个数大于50个时，继续在根目录中创建文件可能会失败。

----结束

检查配置结果

- 使用**display scp-client**命令，在SCP客户端查看源配置信息。
- 使用**display ssh server-info**命令，查看客户端所有的SSH服务器与公钥之间的对应关系。

8.4.5 配置设备作为 FTPS 客户端访问其他设备的文件

前置任务

在配置通过FTPS访问其他设备的文件之前，需完成以下任务：

- 设备和安全FTP（FTPS）服务器路由可达。
- FTPS服务器端已加载数字证书，能正常访问。
- 已获取FTPS服务器的主机名或IP地址、FTP用户名及密码。

配置流程

须知

从V200R020C00版本开始，缺省情况下FTPS服务器端不接收来自任何接口登录连接的IPv4和IPv6请求，当需要授权客户可以登录服务器时，必须执行命令指定服务器端的源接口或源地址。

通过FTPS访问其他设备文件的配置流程如表8-53所示。

表 8-53 配置设备作为 FTPS 客户端访问其他设备的文件配置流程

序号	配置任务名称	配置任务说明	配置流程说明
1	上传CA证书和证书撤销列表（CRL）	通过其他文件上传方式将所需文件上传至设备。	序号1、2、3有序操作，FTPS连接建立后，序号4、5无操作顺序，序号6（断开连接操作）为最后一步。
2	配置SSL策略并加载CA证书和CRL	-	
3	使用FTPS连接其他设备	-	
4	通过FTP文件操作命令进行文件操作	包括目录操作、文件操作、配置文件传输方式、查看FTP命令在线帮助等。	
5	（可选）更改登录用户	-	
6	断开与FTP服务器的连接	-	

操作步骤

- **上传CA证书和证书撤销列表（CRL）**

  可使用FTP、SFTP或SCP方式将CA证书和CRL文件上传至设备，且要保存至security中，如设备无此目录，可执行命令**mkdir** *security*创建。

  说明

  - 访问FTPS服务器的客户端需要从CA得到CA证书，用来验证服务器数字证书的有效性。
  - CRL也由CA发布，包含了被吊销证书的序列号，若服务器端的数字证书被列入了CRL，则客户端认证服务器不成功，FTPS无法连接。

  证书格式分为PEM格式、ASN1格式和PFX格式。虽然证书的格式不相同，但是证书的内容一样。

  - PEM格式的证书是最常用的一种数字证书格式，文件的扩展名是.pem，适用于系统之间的文本模式传输。
  - ASN1是通用的数字证书格式之一，文件的扩展名是.der，是大多数浏览器的默认格式。
  - PFX是通用的数字证书格式之一，文件的扩展名是.pfx，是可移植的二进制格式。

  CRL文件支持ASN1和PEM两种类型，虽然格式不一样，但是文件的内容一样。

  具体的操作步骤请参考手册中其他文件上传方式的介绍。

- **配置SSL策略并加载CA证书和CRL**

  表 8-54 配置 SSL 策略并加载 CA 证书和 CRL

操作步骤	命令	说明
进入系统视图	**system-view**	-

操作步骤	命令	说明
（可选）定制SSL算法套	**ssl cipher-suite-list** *customization-policy-name*	创建SSL算法套定制策略并进入定制策略视图。 缺省情况下，没有配置SSL算法套定制策略。
	set cipher-suite { **tls12_ck_dss_aes_128_gcm_sha256** | **tls12_ck_dss_aes_256_gcm_sha384** | **tls12_ck_rsa_aes_128_gcm_sha256** | **tls12_ck_rsa_aes_256_gcm_sha384** }	配置SSL算法套定制策略中支持的算法套。 缺省情况下，SSL算法套定制策略中没有配置算法套。 配置算法套定制策略中支持的算法套后，SSL协商时将使用定制策略中配置的策略进行协商。 如果算法套定制策略已经被SSL策略引用，可以对算法套进行增加、修改和部分删除，但不能将算法套定制策略中的算法套全部删除。 系统软件中不包含**tls12_ck_rsa_aes_256_cbc_sha256**、**tls1_ck_dhe_dss_with_aes_128_sha**、**tls1_ck_dhe_dss_with_aes_256_sha**、**tls1_ck_dhe_rsa_with_aes_128_sha**、**tls1_ck_dhe_rsa_with_aes_256_sha**、**tls1_ck_rsa_with_aes_128_sha**和**tls1_ck_rsa_with_aes_256_sha**参数，如需使用，需要安装WEAKEA插件，但是该算法安全性低。为了保证更好的安全性，建议使用其它算法。WEAKEA插件安装方法请参见WEAKEA插件使用指南。
	quit	返回系统视图。
配置SSL策略并进入SSL策略视图	**ssl policy** *policy-name*	-

操作步骤	命令	说明
（可选）设置SSL策略所采用的最低SSL版本	**ssl minimum version** { **tls1.1** | **tls1.2** | **tls1.3** }	缺省情况下，SSL策略所采用的最低SSL版本为TLS1.2。 系统软件中不包含**tls1.0**参数，如需使用，需要安装WEAKEA插件，但是该算法安全性低。为了保证更好的安全性，建议配置**tls1.2**参数。WEAKEA插件安装方法请参见WEAKEA插件使用指南。
（可选）在SSL策略中绑定指定的SSL算法套定制策略	**binding cipher-suite-customization** *customization-policy-name*	缺省情况下，SSL策略未绑定算法套定制策略，使用默认的算法套。SSL策略默认支持如下算法套： • tls1_ck_rsa_with_aes_256_sha • tls1_ck_rsa_with_aes_128_sha • tls1_ck_dhe_rsa_with_aes_256_sha • tls1_ck_dhe_dss_with_aes_256_sha • tls1_ck_dhe_rsa_with_aes_128_sha • tls1_ck_dhe_dss_with_aes_128_sha • tls12_ck_rsa_aes_256_cbc_sha256 绑定的SSL算法套定制策略中如果仅有一种类型的算法（RSA或DSS），SSL策略需要加载对应类型的证书，确保SSL协商时能成功。
加载PEM格式的证书	**trusted-ca load pem-ca** *ca-filename*	根据证书类型，选其一。 一个SSL策略最多可以同时加载4个CA证书。如果多次加载不同的CA证书，CA证书会被增加到现有的CA证书列表中。 **说明** 从V200R008C00版本及之后版本降级至以前版本时，需要先备份当前配置中加载的SSL私钥文件。
加载ASN1格式的证书	**trusted-ca load asn1-ca** *ca-filename*	
加载PFX格式的证书	**trusted-ca load pfx-ca** *ca-filename* **auth-code cipher** *auth-code*	
加载CRL	**crl load** { **pem-crl** | **asn1-crl** } *crl-filename*	一个SSL策略最多可以同时加载2个CRL文件。如果多次加载不同的CRL文件，CRL文件会被增加到现有的CRL文件列表中。

说明

- 如果FTPS服务器端配置的证书文件包含的是单个证书，则需要在客户端配置此证书以上的各级CA证书，直接到根证书为止。
- 如果FTPS服务器端配置的是证书链，则只需在客户端配置根证书即可。
- 若没有加载CRL，其实是不影响FTPS的正常连接的，但此时客户端无法保证服务器端数字证书的有效性，建议在客户端加载CRL，并定期更新。

- **使用FTPS连接其他设备**

表 8-55 使用 FTPS 连接其他设备

操作步骤	命令	说明
IPv4网络	**ftp ssl-policy** *policy-name* [**-a** *source-ip-address* | **-i** *interface-type interface-number*] *host* [*port-number*] [**public-net** | **vpn-instance** *vpn-instance-name*]	根据地址类型，二选一。
IPv6网络	**ftp ssl-policy** *policy-name* **ipv6** *host-ipv6-address* [*port-number*]	

使用FTPS连接其他设备，也可以先执行**ftp**命令进入FTP客户端视图，然后再执行**open**命令完成FTP连接操作。

用户访问服务器时，需要经过验证，输入正确的用户名和密码后，则可以进入FTP客户端视图，对服务器上的文件进行管理和操作。

- **通过FTP命令进行文件操作**

用户访问FTPS服务器后，可对FTPS服务器中的文件进行操作（与普通FTP方式一样）。

说明

用户的操作权限受限于服务器上对该用户的权限设置。

由于文件系统对根目录下的文件个数有限制，当根目录中文件个数大于50个时，继续在根目录中创建文件可能会失败。

以下各操作没有严格顺序，可根据需求选择一种或多种操作项目。

表 8-56 通过 FTP 命令进行文件操作

操作项目	命令	说明
改变服务器上的工作路径	**cd** *remote-directory*	-

操作项目	命令	说明
改变服务器的工作路径到上一级目录	**cdup**	-
显示服务器工作路径	**pwd**	-
显示或者改变客户端的工作路径	**lcd** [*local-directory*]	与**pwd**不同的是，**lcd**命令执行后显示的是客户端的本地工作路径，而**pwd**显示的则是远端服务器的工作路径。
在服务器上创建目录	**mkdir** *remote-directory*	创建的目录可以为字母和数字等的组合，但不可以为<、>、？ 、\、： 等特殊字符。
在服务器上删除目录	**rmdir** *remote-directory*	-
显示服务器上指定目录或文件的信息	**dir/ls** [*remote-filename* [*local-filename*]]	• **ls**命令只能显示出目录/文件的名称，而**dir**命令可以查看目录/文件的详细信息，如大小，创建日期等。 • 如果指定远程文件时没有指定路径名称，那么系统将在用户的授权目录下搜索指定的文件。
删除服务器上指定文件	**delete** *remote-filename*	-
上传单个或多个文件	**put** *local-filename* [*remote-filename*] 或 **mput** *local-filenames*	• **put**命令是上传单个文件。 • **mput**命令是上传多个文件。
下载单个或多个文件	**get** *remote-filename* [*local-filename*] 或 **mget** *remote-filenames*	• **get**命令是下载单个文件。 • **mget**命令是下载多个文件。
配置传输文件的数据类型为ASCII模式或二进制模式	**ascii** 或 **binary**	二选一 • 缺省情况下，文件传输方式为ASCII模式。 • 传输文本文件使用ASCII方式，传输程序、系统软件、数据库文件等使用二进制模式。

操作项目	命令	说明
配置文件传输方式为被动方式或主动方式	**passive** 或 **undo passive**	二选一 缺省情况下，数据传输方式是主动方式。
查看FTP命令的在线帮助	**remotehelp** [*command*]	-
使能系统的提示功能	**prompt**	缺省情况下，不使能信息提示。
打开verbose开关	**verbose**	如果打开verbose开关，将显示所有FTP响应，包括FTP协议信息，以及FTP服务器返回的详细信息。

- **（可选）更改登录用户**

  设备可以在不退出FTP客户端视图的情况下，以其他的用户名登录到FTPS服务器。所建立的FTP连接，与执行**ftp ssl-policy**命令建立的FTP连接完全相同。

操作步骤	命令	说明
FTP客户端视图下，更改当前的登录用户	**user** *user-name* [*password*]	更改当前的登录用户后，原用户与服务器的连接将断开。

- **断开与FTPS服务器的连接**

  用户可以在FTP客户端视图中选择不同的命令断开与FTPS服务器的连接。

操作步骤	命令	说明
终止与服务器的连接，并退回到用户视图	**bye** 或 **quit**	二选一。
终止与服务器的连接，并退回到FTP客户端视图	**close** 或 **disconnect**	

----结束

检查配置结果

- 使用**display ssl policy**命令，查看FTPS客户端配置的SSL策略、加载的CA证书和CRL。

8.5 文件管理的配置举例

8.5.1 通过登录系统进行文件操作示例

组网需求

用户通过Console口、Telnet或STelnet方式登录设备，需要对设备上的文件进行以下操作：

- 查看当前目录下的文件及子目录。
- 创建目录**test**，将文件**vrpcfg.zip**复制至**test**目录下，并命名为**backup.zip**。
- 查看**test**目录下的文件。

图 8-2 登录设备进行文件操作组网图

操作步骤

步骤1 查看当前目录下的文件及子目录。

```
<HUAWEI> system-view
[HUAWEI] sysname Switch
[Switch] quit
<Switch> dir
Directory of flash:/

  Idx  Attr     Size(Byte)  Date        Time       FileName
    0  -rw-           889  Mar 01 2012 14:41:56   private-data.txt
    1  -rw-         6,311  Feb 17 2012 14:05:04   backup.cfg
    2  -rw-         2,393  Mar 06 2012 17:20:10   vrpcfg.zip
    3  -rw-           812  Dec 12 2011 15:43:10   hostkey
    4  drw-             -  Mar 01 2012 14:41:46   compatible
    5  -rw-           540  Dec 12 2011 15:43:12   serverkey
...
65,233 KB total (7,289 KB free)
```

步骤2 创建目录**test**，将文件**vrpcfg.zip**复制至**test**目录下，并命名为**backup.zip**。

创建目录**test**。

```
<Switch> mkdir test
```

复制**vrpcfg.zip**至**test**目录下，并命名为**backup.zip**。

```
<Switch> copy vrpcfg.zip flash:/test/backup.zip
```

说明

如果不指定目标文件名，则目标文件名默认为源文件名，即目标文件和源文件同名。

步骤3 查看**test**目录下的文件。

进入**test**目录。

```
<Switch> cd test
```

查看当前的工作路径。

```
<Switch> pwd
flash:/test
```

查看**test**目录下的文件。

```
<Switch> dir
Directory of flash:/test/

 Idx  Attr     Size(Byte)  Date        Time       FileName
   0  -rw-         2,399  Mar 12 2012 11:16:44   backup.zip

65,233 KB total (7,285 KB free)
```

----结束

配置文件

Switch的配置文件

```
#
sysname Switch
#
return
```

8.5.2 FTP 服务器配置示例

组网需求

如图8-3所示，PC与设备之间路由可达，10.136.23.5是设备的管理网口IP地址，设备需要进行升级操作，要求将设备作为FTP服务器，从终端PC将系统软件上传至设备，且保存当前设备的配置文件到终端进行备份。

图 8-3 通过 FTP 进行文件操作组网图

配置思路

采用如下的思路配置通过FTP进行文件操作：

1. 配置设备的FTP功能及FTP用户信息（包括用户名及密码、用户级别、服务类型、授权目录）。
2. 保存设备当前配置文件。
3. 从终端PC通过FTP连接设备。
4. 将系统软件上传至设备以及配置文件备份至PC。

说明

当所处环境不足够安全时，建议选择较安全的SFTP接入方式登录设备，具体配置案例请参见**SFTP服务器配置示例**。

操作步骤

步骤1 配置设备的FTP功能及FTP用户信息。

```
<HUAWEI> system-view
[HUAWEI] sysname FTP_Server
[FTP_Server] ftp server-source -i MEth 0/0/1
//如果设备无管理网口，则可配置为管理IP地址对应的接口。如果此处服务器端源地址配置为了非管理IP地址及其对应的接口，则客户端必须使用配置的源地址才能连接服务器。
[FTP_Server] ftp server enable
[FTP_Server] aaa
[FTP_Server-aaa] local-user admin1234 password irreversible-cipher YsHsjx_202206
[FTP_Server-aaa] local-user admin1234 privilege level 15
[FTP_Server-aaa] local-user admin1234 service-type ftp
[FTP_Server-aaa] local-user admin1234 ftp-directory flash:/
[FTP_Server-aaa] quit
[FTP_Server] quit
```

步骤2 保存设备当前配置文件。

```
<FTP_Server> save
```

步骤3 从终端PC通过FTP连接设备，输入用户名**admin1234**和密码**YsHsjx_202206**，并采用binary模式进行文件传输。

终端以Window XP操作系统为例说明。

```
C:\Documents and Settings\Administrator> ftp 10.136.23.5
连接到 10.136.23.5。
220 FTP service ready.
用户 (10.136.23.5:(none)): admin1234
331 Password required for admin1234.
密码:
230 User logged in.
ftp> binary
200 Type set to I.
ftp>
```

步骤4 将系统软件上传至设备以及配置文件备份至终端。

上传系统软件至设备。

```
ftp> put devicesoft.cc
200 Port command okay.
150 Opening BINARY mode data connection for devicesoft.cc
226 Transfer complete.
ftp: 发送 23876556 字节，用时 25.35Seconds 560.79Kbytes/sec.
```

备份配置文件。

```
ftp> get vrpcfg.zip
200 Port command okay.
150 Opening BINARY mode data connection for vrpcfg.zip.
226 Transfer complete.
ftp: 收到 1257 字节，用时 0.03Seconds 40.55Kbytes/sec.
```

说明

用户在进行上传和下载操作时，需要明确客户端FTP的工作路径，例如Windows XP操作系统默认的FTP路径是登录用户的用户文件夹（如：C:\Documents and Settings\Administrator）。待上传的系统软件需要预先保存至此路径下，以及备份的配置文件也将保存在此路径下。

步骤5 检查配置结果。

在设备中执行**dir**命令，查看系统软件配置文件是否上传至设备。

```
<FTP_Server> dir
Directory of flash:/
```

```
 Idx  Attr     Size(Byte)  Date       Time       FileName
   0  -rw-             14  Mar 13 2012 14:13:38   back_time_a
   1  drw-              -  Mar 11 2012 00:58:54   logfile
   2  -rw-              4  Nov 17 2011 09:33:58   snmpnotilog.txt
   3  -rw-         11,238  Mar 12 2012 21:15:56   private-data.txt
   4  -rw-          1,257  Mar 12 2012 21:15:54   vrpcfg.zip
   5  -rw-             14  Mar 13 2012 14:13:38   back_time_b
   6  -rw-     23,876,556  Mar 13 2012 14:24:24   devicesoft.cc
   7  drw-              -  Oct 31 2011 10:20:28   sysdrv
   8  drw-              -  Feb 21 2012 17:16:36   compatible
   9  drw-              -  Feb 09 2012 14:20:10   selftest
  10  -rw-         19,174  Feb 20 2012 18:55:32   backup.cfg
  11  -rw-         23,496  Dec 15 2011 20:59:36   20111215.zip
  12  -rw-            588  Nov 04 2011 13:54:04   servercert.der
  13  -rw-            320  Nov 04 2011 13:54:26   serverkey.der
  14  drw-              -  Nov 04 2011 13:58:36   security
...
65,233 KB total (7,289 KB free)
```

在终端FTP用户的工作路径下，可以看到**vrpcfg.zip**文件已保存至此路径。

----结束

配置文件

FTP_Server的配置文件

```
#
sysname FTP_Server
# FTP server enable
FTP server-source -i MEth 0/0/1
#
aaa
 local-user admin1234 password irreversible-cipher $1a$P2m&M5d"'JHR7b~SrcHF\Z\,2R"t&6V|zOLh9y$>M
\bjG$D>%@Ug/<3I$+=Y$
 local-user admin1234 privilege level 15
 local-user admin1234 ftp-directory flash:/
 local-user admin1234 service-type ftp
#
return
```

相关信息

视频

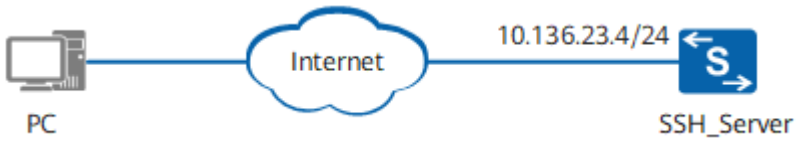
如何通过FTP拷贝文件

8.5.3 SFTP 服务器配置示例

组网需求

如图8-4所示，终端PC与设备路由可达，10.136.23.4是设备的管理网口IP地址。用户希望在终端与设备之间进行安全的文件传输操作，以防止普通FTP服务带来的“中间人”攻击和一些网络欺骗（DNS欺骗和IP欺骗）。将设备配置为SSH服务器，提供SFTP服务，服务器通过对客户端的认证和双向的数据加密，实现用户对安全文件传输操作的要求。

图 8-4 配置通过 SFTP 进行文件操作组网图



配置思路

采用如下的思路配置用户通过SFTP进行文件操作：

1. 在SSH服务器端生成本地密钥对及使能SFTP服务器功能，实现在服务器端和客户端进行安全地数据交互。
2. 配置SSH服务器端的VTY用户界面。
3. 配置SSH用户，包括认证方式、服务类型、授权目录以及用户名和密码等。
4. 从终端通过第三方软件OpenSSH实现访问SSH服务器。

操作步骤

步骤1 在服务器端生成本地密钥对，并使能SFTP服务器功能。

```
<HUAWEI> system-view
[HUAWEI] sysname SSH_Server
[SSH_Server] dsa local-key-pair create
Info: The key name will be: SSH_Server_Host_DSA.
Info: The key modulus can be any one of the following : 1024,
2048.
Info: If the key modulus is greater than 512, it may take a few
minutes.
Please input the modulus [default=2048]:
Info: Generating keys...
Info: Succeeded in creating the DSA host keys.
[SSH_Server] ssh server-source -i MEth 0/0/1
//如果设备无管理网口，则可配置为管理IP地址对应的接口。如果此处服务器端源地址配置为了非管理IP地址及其对应的接口，则客户端必须使用配置的源地址才能连接服务器。
[SSH_Server] sftp server enable
```

步骤2 在服务器端配置VTY用户界面。

```
[SSH_Server] user-interface vty 0 14
[SSH_Server-ui-vty0-14] authentication-mode aaa
[SSH_Server-ui-vty0-14] protocol inbound ssh
[SSH_Server-ui-vty0-14] quit
```

步骤3 配置SSH用户，包括认证方式、服务类型、授权目录以及用户名和密码等。

```
[SSH_Server] ssh user client001 authentication-type password
[SSH_Server] ssh user client001 service-type sftp
[SSH_Server] ssh user client001 sftp-directory flash:
[SSH_Server] aaa
[SSH_Server-aaa] local-user client001 password irreversible-cipher YsHsjx_202206
[SSH_Server-aaa] local-user client001 privilege level 15
[SSH_Server-aaa] local-user client001 service-type ssh
[SSH_Server-aaa] quit
```

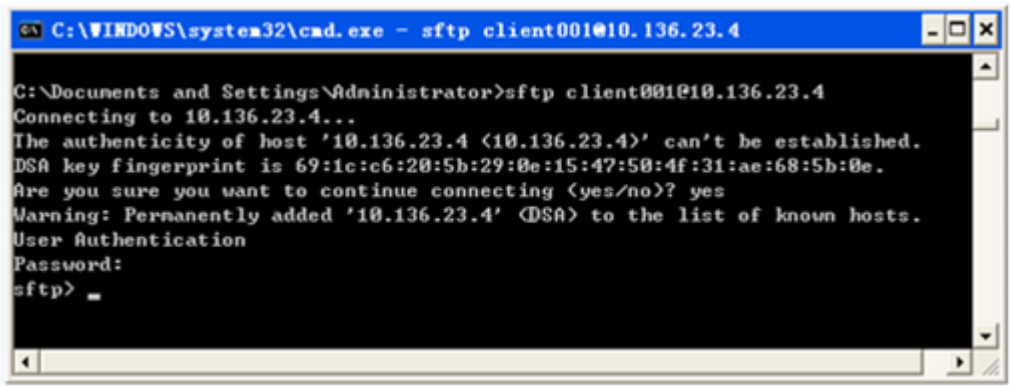
步骤4 从终端通过OpenSSH软件实现访问SFTP服务器。

只有在用户终端安装了OpenSSH软件后，Windows命令行提示符才能识别OpenSSH相关命令。

说明

请使用与当前终端操作系统相匹配的OpenSSH版本，否则可能会导致通过SFTP方式访问交换机失败。

图 8-5 访问界面



通过第三方软件连接设备后，进入SFTP视图，此时可以执行一系列文件操作。

----结束

配置文件

SSH_Server的配置文件

```
#
sysname SSH_Server
#
aaa
 local-user client001 password irreversible-cipher $1a$P2m&M5d"'JHR7b~SrcHF\Z\,2R"t&6V|zOLh9y$>M\bjG
$D>%@Ug/<3I$+=Y$
 local-user client001 privilege level 15
 local-user client001 service-type ssh
#
sftp server enable
ssh user client001
ssh user client001 authentication-type password
ssh user client001 service-type sftp
ssh user client001 sftp-directory flash:
ssh server-source -i MEth 0/0/1 #
user-interface vty 0 14
 authentication-mode aaa
#
return
```

8.5.4 FTPS 服务器配置示例

组网需求

如图8-6所示，终端与设备之间路由可达，10.137.217.201是设备的管理网口IP地址。

用户希望终端与设备之间进行安全的文件传输操作，因为传统的FTP不具备安全机制，采用明文的形式传输数据，会造成“中间人”攻击和网络欺骗。可在设备上部署SSL策略，利用数据加密、身份验证和消息完整性验证机制，为网络上数据的传输提供安全性保证。SSL是在传统FTP服务的基础上提供安全连接，从而很大程度上改善了传统FTP服务器安全性问题。

图 8-6 通过 FTPS 进行文件操作组网图

配置思路

采用如下的思路配置通过FTPS进行文件操作：

1. 先配置设备的普通FTP功能，将PC上存储的数字证书上传到设备上。
2. 将FTPS服务器根目录下的数字证书拷贝到security子目录中，再配置SSL策略并加载数字证书，以实现客户端对服务器的身份验证。
3. 使能安全FTP服务器功能及配置FTP本地用户。
4. 用户通过终端第三方软件连接FTPS服务器。

操作步骤

步骤1 先配置服务器的普通FTP功能，将PC上存储的数字证书上传到服务器上。

配置普通FTP功能：使能FTP功能和配置FTP用户信息。

```
<HUAWEI> system-view
[HUAWEI] sysname FTPS_Server
[FTPS_Server] ftp server-source -i MEth 0/0/1
//如果设备无管理网口，则可配置为管理IP地址对应的接口。如果此处服务器端源地址配置为了非管理IP地址及其对应的接口，则客户端必须使用配置的源地址才能连接服务器。
[FTPS_Server] ftp server enable
[FTPS_Server] aaa
[FTPS_Server-aaa] local-user admin password irreversible-cipher huawei@6789
[FTPS_Server-aaa] local-user admin service-type ftp
[FTPS_Server-aaa] local-user admin privilege level 3
[FTPS_Server-aaa] local-user admin ftp-directory flash:
[FTPS_Server-aaa] quit
[FTPS_Server] quit
```

在终端PC上进入windows命令行提示符输入，执行**ftp**命令指定FTP服务器的连接地址。然后输入正确的用户名和密码与FTP服务器建立FTP连接。在用户终端将数字证书及私钥文件上传到服务器上。

上述步骤成功执行后，在FTP服务器端执行命令**dir**，可看到成功上传的数字证书及私钥文件。

```
<FTPS_Server> dir
Directory of flash:/

Idx  Attr     Size(Byte)  Date       Time        FileName
   0  drw-              -  May 10 2011 05:05:40   src
   1  -rw-        524,575  May 10 2011 05:05:53   private-data.txt
   2  -rw-            446  May 10 2011 05:05:51   vrpcfg.zip
   3  -rw-          1,302  May 10 2011 05:32:05   4_servercert_der_dsa.der
   4  -rw-            951  May 10 2011 05:32:44   4_serverkey_der_dsa.der
...
65,233 KB total (7,289 KB free)
```

步骤2 配置SSL策略并加载数字证书。

创建security子目录，并将安全证书移动到security子目录。


```
<FTPS_Server> mkdir security/
<FTPS_Server> move 4_servercert_der_dsa.der security/
<FTPS_Server> move 4_serverkey_der_dsa.der security/
```

上述步骤成功执行后，在security子目录下执行命令**dir**，可看到拷贝成功的数字证书及私钥文件。

```
<FTPS_Server> cd security/
<FTPS_Server> dir
Directory of flash:/security/

 Idx  Attr     Size(Byte)  Date        Time       FileName
   0  -rw-          1,302  May 10 2011 05:44:34   4_servercert_der_dsa.der
   1  -rw-            951  May 10 2011 05:45:22   4_serverkey_der_dsa.der

65,233 KB total (7,289 KB free)
```

创建SSL策略，并加载ASN1格式的数字证书。

```
<FTPS_Server> system-view
[FTPS_Server] ssl policy ftp_server
[FTPS_Server-ssl-policy-ftp_server] certificate load asn1-cert 4_servercert_der_dsa.der key-pair dsa key-file 4_serverkey_der_dsa.der
[FTPS_Server-ssl-policy-ftp_server] quit
```

步骤3 使能安全FTP服务器功能及配置FTP本地用户。

使能安全FTP服务器功能。

说明

使能安全FTP服务功能，必须去使能普通FTP服务器功能。

```
[FTPS_Server] undo ftp server
[FTPS_Server] ftp secure-server ssl-policy ftp_server
[FTPS_Server] ftp secure-server enable
```

配置FTP本地用户。

使用上面配置过的**admin**用户即可。

步骤4 用户通过终端第三方软件连接FTPS服务器。

具体操作过程请参见第三方软件的帮助文档。

步骤5 检查配置结果。

在安全FTP服务器端执行命令**display ssl policy**，可以看到加载的证书详细信息。

```
[FTPS_Server] display ssl policy

      SSL Policy Name: ftp_server
    Policy Applicants:
       Key-pair Type: DSA
 Certificate File Type: ASN1
     Certificate Type: certificate
 Certificate Filename: 4_servercert_der_dsa.der
    Key-file Filename: 4_serverkey_der_dsa.der
           Auth-code:
                MAC:
          CRL File:
      Trusted-CA File:
         Issuer Name:
  Validity Not Before:
   Validity Not After:
```

在安全FTP服务器端执行命令**display ftp-server**，可以看到SSL策略名称、安全FTP服务器的状态是running。

```
[FTPS_Server] display ftp-server
  FTP server is stopped
```

```
Max user number              5
User count                   1
Timeout value(in minute)     30
Listening port               21
Acl number                   0
FTP server's source address  0.0.0.0
FTP SSL policy               ftp_server
FTP Secure-server is running
```

用户可以通过支持SSL的FTP客户端软件与安全FTP服务器建立连接，并实现文件的上传和下载。

----结束

配置文件

FTPS_Server的配置文件

```
#
sysname FTPS_Server
#
FTP secure-server enable
FTP server-source -i MEth 0/0/1
ftp secure-server ssl-policy ftp_server
#
aaa
 local-user admin password irreversible-cipher $1a$P2m&M5d"'JHR7b~SrcHF\Z\,2R"t&6V|zOLh9y$>M\bjG
$D>%@Ug/<3I$+=Y$
 local-user admin privilege level 3
 local-user admin ftp-directory flash:
 local-user admin service-type ftp
#
ssl policy ftp_server
 certificate load asn1-cert 4_servercert_der_dsa.der key-pair dsa key-file 4_serverkey_der_dsa.der
#
return
```

8.5.5 TFTP 客户端配置示例

组网需求

如图8-7所示，远端服务器提供TFTP Server功能，IP地址为10.1.1.1/24。设备作为TFTP客户端，IP地址为10.2.1.1/24，与服务器之间的路由可达。

设备需要进行升级操作，要求：从TFTP服务器上下载系统软件至设备，且备份当前设备的配置文件到TFTP服务器。

图 8-7 配置通过 TFTP 访问其他设备文件组网图

配置思路

采用如下的思路配置TFTP传输文件功能：

1. 在TFTP服务器端运行TFTP软件，并设置TFTP的工作路径。
2. 在设备上使用TFTP命令下载和上传文件。

操作步骤

步骤1 在TFTP服务器端运行TFTP软件，并设置TFTP的工作路径。（具体操作见第三方软件帮助文档）

步骤2 在设备上使用TFTP命令下载和上传文件。

```
<HUAWEI> tftp 10.1.1.1 get devicesoft.cc
Info: Transfer file in binary mode.
Downloading the file from the remote TFTP server. Please wait...\
TFTP: Downloading the file successfully.
23876556 bytes received in 199 seconds.
<HUAWEI> tftp 10.1.1.1 put vrpcfg.zip
Info: Transfer file in binary mode.
Uploading the file to the remote TFTP server. Please wait...|
TFTP: Uploading the file successfully.
7717 bytes send in 1 second.
```

步骤3 检查配置结果。

在设备中执行**dir**命令，查看系统软件是否下载至设备。

```
<HUAWEI> dir
Directory of flash:/

  Idx  Attr     Size(Byte)  Date        Time       FileName
    0  -rw-            14  Mar 13 2012 14:13:38   back_time_a
    1  drw-             -  Mar 11 2012 00:58:54   logfile
    2  -rw-             4  Nov 17 2011 09:33:58   snmpnotilog.txt
    3  -rw-        11,238  Mar 12 2012 21:15:56   private-data.txt
    4  -rw-         7,717  Mar 12 2012 21:15:54   vrpcfg.zip
    5  -rw-            14  Mar 13 2012 14:13:38   back_time_b
    6  -rw-    23,876,556  Mar 13 2012 14:24:24   devicesoft.cc
    7  drw-             -  Oct 31 2011 10:20:28   sysdrv
    8  drw-             -  Feb 21 2012 17:16:36   compatible
    9  drw-             -  Feb 09 2012 14:20:10   selftest
   10  -rw-        19,174  Feb 20 2012 18:55:32   backup.cfg
   11  -rw-        43,496  Dec 15 2011 20:59:36   20111215.zip
   12  -rw-           588  Nov 04 2011 13:54:04   servercert.der
   13  -rw-           320  Nov 04 2011 13:54:26   serverkey.der
   14  drw-             -  Nov 04 2011 13:58:36   security
...
65,233 KB total (7,289 KB free)
```

在TFTP服务器的工作路径下，可以看到**vrpcfg.zip**文件已保存至此路径。

----结束

配置文件

无

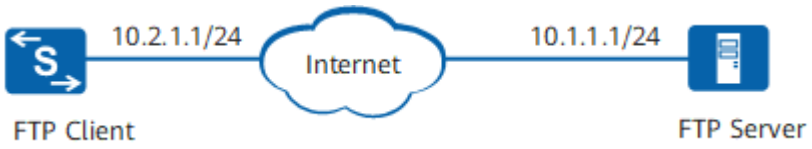
8.5.6 FTP 客户端配置示例

组网需求

如图8-8所示，远端服务器提供FTP Server功能，IP地址为10.1.1.1/24。设备作为FTP客户端，IP地址为10.2.1.1/24，与服务器之间的路由可达。

设备需要进行升级操作，要求：从FTP服务器上下载系统软件至设备，且备份当前设备的配置文件到FTP服务器。

图 8-8 配置通过 FTP 访问其他设备文件组网图



配置思路

采用如下的思路配置FTP访问其他设备文件功能：

1. 在FTP服务器端运行FTP软件，并设置FTP用户的相关信息。
2. 通过FTP与FTP服务器建立连接。
3. 在设备上使用FTP命令下载和上传文件。

操作步骤

步骤1 在FTP服务器端运行FTP软件，并设置FTP用户的相关信息。（具体操作见第三方软件帮助文档）

步骤2 通过FTP与FTP服务器建立连接。

```
<HUAWEI> ftp 10.1.1.1
Trying 10.1.1.1 ...
Press CTRL+K to abort
Connected to 10.1.1.1.
220 FTP service ready.
User(10.1.1.1:(none)):admin
331 Password required for admin.
Enter password:
230 User logged in.

[ftp]
```

步骤3 在设备上使用FTP命令下载和上传文件。

```
[ftp] binary
[ftp] get devicesoft.cc
[ftp] put vrpcfg.zip
[ftp] quit
```

步骤4 检查配置结果。

在设备中执行**dir**命令，查看系统软件是否下载至设备。

```
<HUAWEI> dir
Directory of flash:/

 Idx  Attr     Size(Byte)  Date        Time       FileName
   0  -rw-           14  Mar 13 2012 14:13:38   back_time_a
   1  drw-            -  Mar 11 2012 00:58:54   logfile
   2  -rw-            4  Nov 17 2011 09:33:58   snmpnotilog.txt
   3  -rw-       11,238  Mar 12 2012 21:15:56   private-data.txt
   4  -rw-        7,717  Mar 12 2012 21:15:54   vrpcfg.zip
   5  -rw-           14  Mar 13 2012 14:13:38   back_time_b
   6  -rw-   23,876,556  Mar 13 2012 14:24:24   devicesoft.cc
   7  drw-            -  Oct 31 2011 10:20:28   sysdrv
   8  drw-            -  Feb 21 2012 17:16:36   compatible
   9  drw-            -  Feb 09 2012 14:20:10   selftest
  10  -rw-       19,174  Feb 20 2012 18:55:32   backup.cfg
  11  -rw-       43,496  Dec 15 2011 20:59:36   20111215.zip
  12  -rw-          588  Nov 04 2011 13:54:04   servercert.der
```



```
  13  -rw-          320  Nov 04 2011 13:54:26   serverkey.der
  14  drw-            -  Nov 04 2011 13:58:36   security
...
65,233 KB total (7,289 KB free)
```

在FTP服务器的工作路径下，可以看到**vrpcfg.zip**文件已保存至此路径。

----结束

配置文件

无

8.5.7 SFTP 客户端配置示例

组网需求

SSH提供了在一个传统不安全的网络环境中，服务器通过对客户端的认证及双向的数据加密，为网络终端访问提供了安全的服务。通过SFTP方式，客户端可以安全地连接到SSH服务器，进行文件的安全传输。

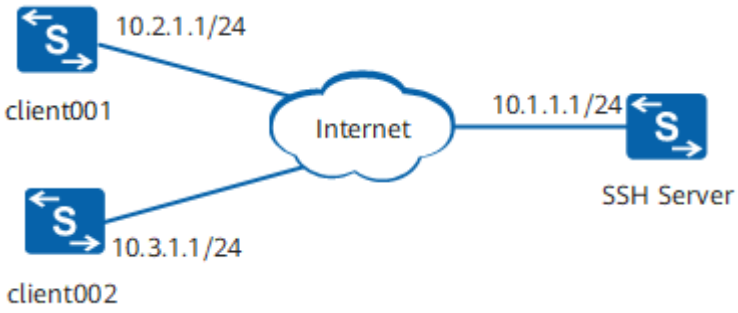
如图8-9所示，SSH服务器与客户端client001、client002路由可达，此例中用华为设备作为SSH服务器。

要求：两个客户端分别使用password方式和DSA方式与SSH服务器连接，实现安全访问服务器上的文件。

说明

Password认证为不安全的认证，实际应用中建议使用AAA认证。

图 8-9 通过 SFTP 访问其他设备文件组网图



配置思路

采用如下思路配置通过SFTP访问其他设备文件功能：

1. 在服务器端生成本地密钥对及使能SFTP服务器功能，实现在服务器端和客户端进行安全地数据交互。
2. 在SSH服务器上配置用户client001和client002，分别使用password和DSA的认证方式登录SSH服务器。
3. 在客户端client002生成本地密钥对，并将客户端生成的DSA公钥配置到SSH服务器上，实现客户端登录服务器端时，对客户端进行验证。

4. 用户client001和client002分别以SFTP方式登录SSH服务器，实现访问服务器上的文件。

操作步骤

步骤1 在服务器端生成本地密钥对及使能SFTP服务器功能。

```
<HUAWEI> system-view
[HUAWEI] sysname SSH Server
[SSH Server] dsa local-key-pair create
Info: The key name will be: SSH Server_Host_DSA.
Info: The key modulus can be any one of the following : 1024,
2048.
Info: If the key modulus is greater than 512, it may take a few
minutes.
Please input the modulus [default=2048]:
Info: Generating keys...
Info: Succeeded in creating the DSA host keys.
[SSH_Server] ssh server-source -i Vlanif 10   //假设服务器IP地址10.1.1.1对应的接口为Vlanif 10。
[SSH Server] sftp server enable
```

步骤2 在服务器端创建SSH用户。

配置VTY用户界面。

```
[SSH Server] user-interface vty 0 4
[SSH Server-ui-vty0-4] authentication-mode aaa
[SSH Server-ui-vty0-4] protocol inbound ssh
[SSH Server-ui-vty0-4] user privilege level 3
[SSH Server-ui-vty0-4] quit
```

新建用户名为client001的SSH用户，且认证方式为password。

```
[SSH Server] ssh user client001
[SSH Server] ssh user client001 authentication-type password
[SSH Server] ssh user client001 service-type sftp
[SSH Server] ssh user client001 sftp-directory flash:
[SSH Server] aaa
[SSH Server-aaa] local-user client001 password irreversible-cipher Helloworld@6789
[SSH Server-aaa] local-user client001 service-type ssh
[SSH Server-aaa] local-user client001 privilege level 3
[SSH Server-aaa] quit
```

新建用户名为client002的SSH用户，且认证方式为DSA。

```
[SSH Server] ssh user client002
[SSH Server] ssh user client002 authentication-type dsa
[SSH Server] ssh user client002 service-type sftp
[SSH Server] ssh user client002 sftp-directory flash:
```

步骤3 在客户端client002生成本地密钥对，并将客户端生成的DSA公钥配置到SSH服务器上。

客户端生成客户端的本地密钥对。

```
<HUAWEI> system-view
[HUAWEI] sysname client002
[client002] dsa local-key-pair create
Info: The key name will be: SSH Server_Host_DSA.
Info: The key modulus can be any one of the following : 1024,
2048.
Info: If the key modulus is greater than 512, it may take a few
minutes.
Please input the modulus [default=2048]:
Info: Generating keys...
Info: Succeeded in creating the DSA host keys.
```

查看客户端上生成DSA公钥。


```
[client002] display dsa local-key-pair public

=============================================
Time of Key pair created: 2014-03-03 19:11:04+00:00
Key name: client002_Host
Key type: DSA encryption Key
=============================================
Key code:
30820109
  02820100
    C7D92E27 E88745D4 933AB1F5 DA692AC4 1D544BDC
    8EA252B0 E90A5001 1F2567C6 3952DEFD 95EF93C2
    D77E8CDF B36E7F43 57C1D7BA 0978DD7A 2F7F7187
    04FD6A03 C4FFDB58 04B3A0C4 B6E50528 AAE56FF9
    5F66EE00 8E4702DB AA764006 322E6F72 CC9C1A39
    462DBCD0 EA934441 1678BA23 40473EC4 58DF84FA
    20C9CB60 98E5ACDA 2E98B55A 0299FBAB FE91EFA3
    E155E065 7C7FFCD4 4EAB71EC A7A73DD7 AC8474B7
    2DD37D1C 710C6E14 57DA200C 477E45BC 38AC7685
    BD8D6325 CCBE3F32 85435E5B EB6A08DF 752B7EBD
    CE21CFCB F3AC0C35 671E5ACC AFC36F0B 54E646F6
    D12B4BA3 6E9EF69F A5BED377 954709EB CE29A923
    04B347D7 29296E7D 3D5F69AB 4365AA2F
  0203
    010001

 Host public key for PEM format code:
---- BEGIN SSH2 PUBLIC KEY ----
AAAAB3NzaC1yc2EAAAADAQABAAABAQDH2S4n6IdF1JM6sfXaaSrEHVRL3I6iUrDp
ClABHyVnxjlS3v2V75PC136M37Nuf0NXwde6CXjdei9/cYcE/WoDxP/bWASzoMS2
5QUoquVv+V9m7gCORwLbqnZABjIub3LMnBo5Ri280OqTREEWeLojQEc+xFjfhPog
yctgmOWs2i6YtVoCmfur/pHvo+FV4GV8f/zUTqtx7KenPdeshHS3LdN9HHEMbhRX
2iAMR35FvDisdoW9jWMlzL4/MoVDXlvragjfdSt+vc4hz8vzrAw1Zx5azK/DbwtU
5kb20StLo26e9p+lvtN3lUcJ684pqSMEs0fXKSlufT1faatDZaov
---- END SSH2 PUBLIC KEY ----

Public key code for pasting into OpenSSH authorized_keys file :
ssh-dsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDH2S4n6IdF1JM6sfXaaSrEHVRL3I6iUrDpClABHyVnxjlS3v2V75PC13
6M37Nuf0NXwde6CXjdei9/cYcE/WoDxP/bWASz
oMS25QUoquVv+V9m7gCORwLbqnZABjIub3LMnBo5Ri280OqTREEWeLojQEc
+xFjfhPogyctgmOWs2i6YtVoCmfur/pHvo+FV4GV8f/zUTqtx7KenPdeshHS3LdN9HHEMbhRX
2iAMR35FvDisdoW9jWMlzL4/MoVDXlvragjfdSt+vc4hz8vzrAw1Zx5azK/DbwtU5kb20StLo26e9p
+lvtN3lUcJ684pqSMEs0fXKSlufT1faatDZaov= dsa-key
```

将客户端上产生的DSA公钥配置到服务器端(上面**display**命令显示信息中黑体部分即为客户端产生的DSA公钥，将其拷贝粘贴至服务器端)。

```
[SSH Server] dsa peer-public-key dsakey001 encoding-type der
[SSH Server-dsa-public-key] public-key-code begin
[SSH Server-dsa-key-code] 30820109
[SSH Server-dsa-key-code] 02820100
[SSH Server-dsa-key-code] C7D92E27 E88745D4 933AB1F5 DA692AC4 1D544BDC
[SSH Server-dsa-key-code] 8EA252B0 E90A5001 1F2567C6 3952DEFD 95EF93C2
[SSH Server-dsa-key-code] D77E8CDF B36E7F43 57C1D7BA 0978DD7A 2F7F7187
[SSH Server-dsa-key-code] 04FD6A03 C4FFDB58 04B3A0C4 B6E50528 AAE56FF9
[SSH Server-dsa-key-code] 5F66EE00 8E4702DB AA764006 322E6F72 CC9C1A39
[SSH Server-dsa-key-code] 462DBCD0 EA934441 1678BA23 40473EC4 58DF84FA
[SSH Server-dsa-key-code] 20C9CB60 98E5ACDA 2E98B55A 0299FBAB FE91EFA3
[SSH Server-dsa-key-code] E155E065 7C7FFCD4 4EAB71EC A7A73DD7 AC8474B7
[SSH Server-dsa-key-code] 2DD37D1C 710C6E14 57DA200C 477E45BC 38AC7685
[SSH Server-dsa-key-code] BD8D6325 CCBE3F32 85435E5B EB6A08DF 752B7EBD
[SSH Server-dsa-key-code] CE21CFCB F3AC0C35 671E5ACC AFC36F0B 54E646F6
[SSH Server-dsa-key-code] D12B4BA3 6E9EF69F A5BED377 954709EB CE29A923
[SSH Server-dsa-key-code] 04B347D7 29296E7D 3D5F69AB 4365AA2F
[SSH Server-dsa-key-code] 0203
[SSH Server-dsa-key-code] 010001
[SSH Server-dsa-key-code] public-key-code end
[SSH Server-dsa-public-key] peer-public-key end
```


为SSH用户client002绑定SSH客户端的DSA公钥。

```
[SSH Server] ssh user client002 assign dsa-key dsakey001
```

步骤4 SFTP客户端连接SSH服务器。

第一次登录，使能SSH客户端首次认证功能。

使能客户端client001首次认证功能。

```
<HUAWEI> system-view
[HUAWEI] sysname client001
[client001] ssh client first-time enable
```

使能客户端client002首次认证功能。

```
[client002] ssh client first-time enable
```

SFTP客户端client001用password认证方式连接SSH服务器。

```
[client002] sftp 10.1.1.1
Please input the username:client001
Trying 10.1.1.1 ...
Press CTRL+K to abort
Connected to 10.1.1.1 ...
password:SSH_SERVER_CODE

Please select public key type for user authentication [R for RSA; D for DSA; Enter for Skip publickey
authentication; Ctrl_C for Cancel], Please select [R, D, Enter or
Ctrl_C]:D

sftp-client>
```

SFTP客户端client002用DSA认证方式连接SSH服务器。

```
[client002] sftp 10.1.1.1
Please input the username:client002
Trying 10.1.1.1 ...
Press CTRL+K to abort
Connected to 10.1.1.1 ...
password:SSH_SERVER_CODE

Please select public key type for user authentication [R for RSA; D for DSA; Enter for Skip publickey
authentication; Ctrl_C for Cancel], Please select [R, D, Enter or
Ctrl_C]:D

sftp-client>
```

步骤5 检查配置结果。

配置完成后，在SSH服务器端执行**display ssh server status**命令可以查看到SFTP服务已经使能。执行**display ssh user-information**命令可以查看服务器端SSH用户信息。

查看SSH状态信息。

```
[SSH Server] display ssh server status
 SSH version                    :1.99
 SSH connection timeout             :60 seconds
 SSH server key generating interval  :0 hours
 SSH authentication retries         :3 times
 SFTP server                   :Enable
 Stelnet server                :Disable
 Scp server                    :Disable
 SSH server source                :0.0.0.0
 ACL4 number                      :0
 ACL6 number                      :0
```

查看SSH用户信息。


```
[SSH Server] display ssh user-information
 User 1:
     User Name           : client001
     Authentication-type  : password
     User-public-key-name : -
     User-public-key-type : -
     Sftp-directory       : flash:
     Service-type         : sftp
     Authorization-cmd    : No
 User 2:
     User Name           : client002
     Authentication-type  : dsa
     User-public-key-name : dsakey001
     User-public-key-type : dsa
     Sftp-directory       : flash:
     Service-type         : sftp
     Authorization-cmd    : No
```

----结束

配置文件

- SSH服务器上的配置文件

```
#
sysname SSH Server
#
dsa peer-public-key dsakey001 encoding-type der
 public-key-code begin
  30820109
    02820100
      C7D92E27 E88745D4 933AB1F5 DA692AC4 1D544BDC 8EA252B0 E90A5001 1F2567C6
      3952DEFD 95EF93C2 D77E8CDF B36E7F43 57C1D7BA 0978DD7A 2F7F7187 04FD6A03
      C4FFDB58 04B3A0C4 B6E50528 AAE56FF9 5F66EE00 8E4702DB AA764006 322E6F72
      CC9C1A39 462DBCD0 EA934441 1678BA23 40473EC4 58DF84FA 20C9CB60 98E5ACDA
      2E98B55A 0299FBAB FE91EFA3 E155E065 7C7FFCD4 4EAB71EC A7A73DD7 AC8474B7
      2DD37D1C 710C6E14 57DA200C 477E45BC 38AC7685 BD8D6325 CCBE3F32 85435E5B
      EB6A08DF 752B7EBD CE21CFCB F3AC0C35 671E5ACC AFC36F0B 54E646F6 D12B4BA3
      6E9EF69F A5BED377 954709EB CE29A923 04B347D7 29296E7D 3D5F69AB 4365AA2F
    0203
      010001
 public-key-code end
peer-public-key end
#
aaa
 local-user client001 password irreversible-cipher $1a$P2m&M5d"'JHR7b~SrcHF\Z\,2R"t&6V|zOLh9y
$>M\bjG$D>%@Ug/<3I$+=Y$
 local-user client001 privilege level 3
 local-user client001 service-type ssh
#
sftp server enable
ssh user client001
ssh user client001 authentication-type password
ssh user client001 service-type sftp
ssh user client001 sftp-directory flash:
ssh user client002
ssh user client002 authentication-type dsa
ssh user client002 assign dsa-key dsakey001
ssh user client002 service-type sftp
ssh user client002 sftp-directory flash:
ssh server-source -i Vlanif 10
#
user-interface vty 0 4
 authentication-mode aaa
 user privilege level 3
#
return
```

- SSH客户端client001的配置文件

```
#
sysname client001
#
ssh client first-time enable
#
return
```

- SSH客户端client002的配置文件

```
#
sysname client002
#
ssh client first-time enable
#
return
```

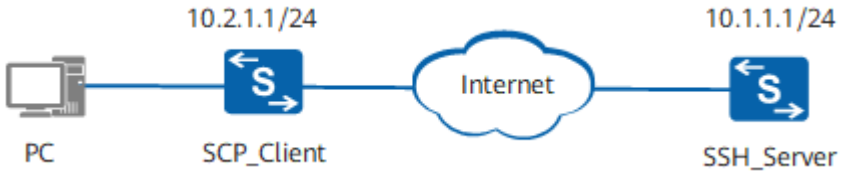
8.5.8 SCP 客户端配置示例

组网需求

与使用SFTP协议传输文件相比，SCP协议可以简化用户传输文件的操作，将用户身份认证、文件传输等步骤合并，提高配置效率。

如图8-10所示，作为SCP客户端的设备和服务器路由可达，并从SSH服务器中下载文件至客户端。

图 8-10 配置通过 SCP 访问其他设备文件配置示例组网图



配置思路

采用如下的思路配置通过SCP访问其他设备文件：

1. 在SSH服务器端生成本地密钥对。
2. 在SSH服务器端创建SSH用户。
3. 在SSH服务器端使能SCP功能。
4. 从SSH服务器下载文件至本地。

操作步骤

步骤1 在服务器端生成本地密钥对。

```
<HUAWEI> system-view
[HUAWEI] sysname SSH_Server
[SSH_Server] dsa local-key-pair create
Info: The key name will be: SSH_Server_Host_DSA.
Info: The key modulus can be any one of the following : 1024, 2048.
Info: If the key modulus is greater than 512, it may take a few minutes.
Please input the modulus [default=2048]:
Info: Generating keys...
Info: Succeeded in creating the DSA host keys.
```

步骤2 在服务器端创建SSH用户。

配置VTY用户界面。

```
[SSH_Server] user-interface vty 0 14
[SSH_Server-ui-vty0-14] authentication-mode aaa
[SSH_Server-ui-vty0-14] protocol inbound ssh
[SSH_Server-ui-vty0-14] quit
```

新建用户名为Client001的SSH用户，且认证方式为password，服务方式为all。

```
[SSH_Server] ssh user client001
[SSH_Server] ssh user client001 authentication-type password
[SSH_Server] ssh user client001 service-type all
```

为SSH用户Client001配置密码为Helloworld@6789。

```
[SSH_Server] aaa
[SSH_Server-aaa] local-user client001 password irreversible-cipher Helloworld@6789
[SSH_Server-aaa] local-user client001 service-type ssh
[SSH_Server-aaa] local-user client001 privilege level 3
[SSH_Server-aaa] quit
```

步骤3 在服务器端使能SCP服务。

```
[SSH_Server] ssh server-source -i Vlanif 10   //假设服务器IP地址10.1.1.1对应的接口为Vlanif 10。
[SSH_Server] scp server enable
```

步骤4 从SCP客户端下载服务器上的文件。

第一次登录，使能SSH客户端首次认证功能。

```
<HUAWEI> system-view
[HUAWEI] sysname SCP_Client
[SCP_Client] ssh client first-time enable
```

使用aes256加密算法将文件backup.cfg从IP地址为10.1.1.1的远端SSH服务器下载至本地用户目录下。

```
[SCP_Client] scp -cipher aes256 client001@10.1.1.1:backup.cfg backup.cfg
Trying 10.1.1.1 ...
Press CTRL+K to abort
Connected to 10.1.1.1 ...
The server has not been authenticated. Continue to access it? [Y/N]:y
Do you want to save the server's public key? [Y/N]:y
The server's public key will be saved with the name 10.1.1.1. Please wait.
..
Enter password:
backup.cfg                   100%       19174Bytes          7KByte(s)/sec
```

----结束

配置文件

- SSH_Server的配置文件

```
#
sysname SSH_Server
#
aaa
 local-user client001 password irreversible-cipher $1a$P2m&M5d"'JHR7b~SrcHF\Z\,2R"t&6V|zOLh9y
$>M\bjG$D>%@Ug/<3I$+=Y$
 local-user client001 privilege level 3
 local-user client001 service-type ssh
#
scp server enable
ssh user client001
ssh user client001 authentication-type password
ssh user client001 service-type all
```



```
ssh server-source -i Vlanif 10
#
user-interface vty 0 14
 authentication-mode aaa
#
return
```

- SCP_Client的配置文件

```
#
sysname SCP_Client
#
ssh client first-time enable
#
return
```

8.5.9 FTPS 客户端配置示例

组网需求

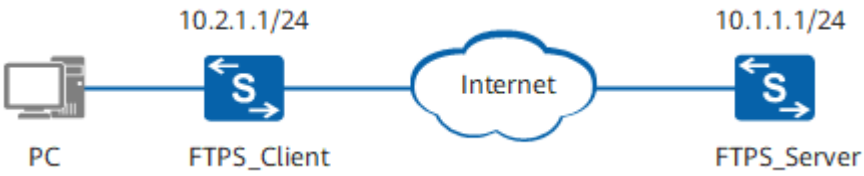
用户希望终端与设备之间进行安全的文件传输操作，因为传统的FTP不具备安全机制，采用明文的形式传输数据，会造成“中间人”攻击和网络欺骗。可在设备上部署SSL策略，利用数据加密、身份验证和消息完整性验证机制，为网络上数据的传输提供安全性保证。SSL是在传统FTP服务的基础上提供安全连接，从而很大程度上改善了传统FTP服务器安全性问题。

如图8-11所示，FTPS客户端和服务器之间路由可达，要求从客户端连接到安全FTP（FTPS）服务器上实现远程管理文件。

- 在作为FTPS客户端的设备上部署SSL策略，并加载CA证书文件，检查证书持有者身份的合法性，并签发证书，以防证书被伪造或篡改，以及对证书和密钥进行管理。
- 在作为FTPS服务器的设备上部署SSL策略，加载数字证书并使能安全FTP服务器功能，检查CA证书文件的合法性，保证合法客户端安全登录服务器。

服务器和客户端所要加载的证书文件需要预先从CA获取。此例中用华为设备作为FTPS服务器。

图 8-11 配置通过 FTPS 访问其他设备文件组网图



配置思路

采用如下的思路配置通过FTPS访问其他设备文件配置示例：

1. 上传证书。
   - 将数字证书及私钥文件上传至作为FTPS服务器的设备上。
   - 将CA证书文件上传至作为FTP客户端的设备上。
2. 加载证书，并配置SSL策略。

- 将服务器根目录下的数字证书文件拷贝到security子目录中，再配置SSL策略并加载数字证书。
- 将客户端根目录下的CA证书文件拷贝到security子目录中，再配置SSL策略并加载CA证书文件。

3. 在FTP服务器端使能安全FTP服务器功能及配置FTP本地用户。
4. 在客户端通过FTP命令连接安全FTP服务器，实现远程文件管理。

操作步骤

步骤1 上传证书。

- 在客户端和服务器分别配置普通FTP服务功能，将所需证书文件上传至客户端和服务器。具体操作可参考**8.3.2 通过FTP进行文件操作**。

  # 上传完成后，使用**dir**命令，在服务器端可看到成功上传的数字证书及私钥文件。

```
<HUAWEI> system-view
[HUAWEI] sysname FTPS_Server
[FTPS_Server] quit
<FTPS_Server> dir
Directory of flash:/

 Idx  Attr     Size(Byte)  Date       Time       FileName
   0  drw-              -  May 10 2011 05:05:40   src
   1  -rw-        524,575  May 10 2011 05:05:53   private-data.txt
   2  -rw-            446  May 10 2011 05:05:51   vrpcfg.zip
   3  -rw-          1,302  Mar 13 2012 18:23:28   4_servercert_der_dsa.der
   4  -rw-            951  Mar 13 2012 18:30:20   4_serverkey_der_dsa.der
...

65,233 KB total (7,289 KB free)
```

  # 在客户端使用**dir**命令，可看到成功上传的CA证书文件。

```
<HUAWEI> system-view
[HUAWEI] sysname FTPS_Client
[FTPS_Client] quit
<FTPS_Client> dir
Directory of flash:/

 Idx  Attr     Size(Byte)  Date       Time       FileName
   0  -rw-        524,558  May 10 2011 04:50:39   private-data.txt
   1  -rw-          1,237  Mar 14 2012 07:46:24   cacert.der
   2  -rw-          1,241  Mar 14 2012 07:46:20   rootcert.der
   3  drw-              -  Apr 09 2011 19:46:14   src
   4  -rw-            421  Apr 09 2011 19:46:14   vrpcfg.zip
   5  -rw-      1,308,478  Apr 14 2011 19:22:45   we1.zip
   6  drw-              -  Apr 10 2011 01:35:54   logfile
   7  -rw-              4  Apr 19 2011 04:24:28   snmpnotilog.txt
   8  drw-              -  Apr 13 2011 11:37:40   lam
...

65,233 KB total (17,489 KB free)
```

步骤2 配置SSL策略并加载证书。

- 在服务器上进行如下配置。

  # 创建security子目录，并将安全证书移动到security子目录。

```
<FTPS_Server> mkdir security/
<FTPS_Server> move 4_servercert_der_dsa.der security/
<FTPS_Server> move 4_serverkey_der_dsa.der security/
```

  # 上述步骤成功执行后，在security子目录下执行命令**dir**，可看到拷贝成功的数字证书及私钥文件。

```
<FTPS_Server> cd security/
<FTPS_Server> dir
```



```
Directory of flash:/security/

 Idx  Attr     Size(Byte)  Date       Time       FileName
   0  -rw-          1,302  Mar 13 2012 18:23:28   4_servercert_der_dsa.der
   1  -rw-            951  Mar 13 2012 18:30:20   4_serverkey_der_dsa.der

65,233 KB total (7,289 KB free)
```

创建SSL策略，并加载ASN1格式的数字证书。

```
<FTPS_Server> system-view
[FTPS_Server] ssl policy ftp_server
[FTPS_Server-ssl-policy-ftp_server] certificate load asn1-cert 4_servercert_der_dsa.der key-pair dsa key-file 4_serverkey_der_dsa.der
[FTPS_Server-ssl-policy-ftp_server] quit
```

上述步骤成功配置后，在服务器端执行命令**display ssl policy**，可以看到加载的证书详细信息。

```
[FTPS_Server] display ssl policy

      SSL Policy Name: ftp_server
    Policy Applicants:
       Key-pair Type: DSA
Certificate File Type: ASN1
    Certificate Type: certificate
Certificate Filename: 4_servercert_der_dsa.der
   Key-file Filename: 4_serverkey_der_dsa.der
         Auth-code:
               MAC:
          CRL File:
     Trusted-CA File:
        Issuer Name:
 Validity Not Before:
  Validity Not After:
```

- 在客户端进行如下配置。

  # 创建security子目录，并将CA证书文件移动到security子目录。

  ```
  <FTPS_Client> mkdir security/
  <FTPS_Client> move cacert.der security/
  <FTPS_Client> move rootcert.der security/
  ```

  # CA证书文件拷贝到security子目录后，在security子目录下执行命令**dir**，可看到拷贝成功的CA证书文件。

  ```
  <FTPS_Client> cd security/
  <FTPS_Client> dir
  Directory of flash:/security/

   Idx  Attr     Size(Byte)  Date       Time       FileName
     0  -rw-          1,237  Mar 14 2012 07:46:24   cacert.der
     1  -rw-          1,241  Mar 14 2012 07:46:20   rootcert.der

  65,233 KB total (17,489 KB free)
  ```

  # 创建SSL策略，并加载CA证书文件。

  ```
  <FTPS_Client> system-view
  [FTPS_Client] ssl policy ftp_client
  [FTPS_Client-ssl-policy-ftp_client] trusted-ca load asn1-ca cacert.der
  [FTPS_Client-ssl-policy-ftp_client] trusted-ca load asn1-ca rootcert.der
  [FTPS_Client-ssl-policy-ftp_client] quit
  ```

  # 上述步骤成功配置后，在FTP客户端执行命令**display ssl policy**，可以看到加载的CA证书文件详细信息。

  ```
  [FTPS_Client] display ssl policy

        SSL Policy Name: ftp_client
      Policy Applicants:
         Key-pair Type:
  Certificate File Type:
      Certificate Type:
  ```

```
Certificate Filename:
  Key-file Filename:
       Auth-code:
            MAC:
        CRL File:
    Trusted-CA File:
  Trusted-CA File 1: Format = ASN1, Filename = cacert.der
  Trusted-CA File 2: Format = ASN1, Filename = rootcert.der
```

步骤3 使能安全FTP服务器功能及配置FTP本地用户。

使能安全FTP服务器功能。

说明

使能安全FTP服务功能，必须去使能普通FTP服务器功能。

```
[FTPS_Server] undo ftp server
[FTPS_Server] ftp secure-server ssl-policy ftp_server
[FTPS_Server] ftp secure-server enable
[FTPS_Server] ftp server-source -i Vlanif 10    //假设服务器IP地址10.1.1.1对应的接口为Vlanif 10。
```

配置FTP本地用户。

```
[FTPS_Server] aaa
[FTPS_Server-aaa] local-user admin password irreversible-cipher Helloworld@6789
[FTPS_Server-aaa] local-user admin service-type ftp
[FTPS_Server-aaa] local-user admin privilege level 3
[FTPS_Server-aaa] local-user admin ftp-directory flash:
[FTPS_Server-aaa] quit
```

此用户可以使用上传证书时FTP用户，也可重新配置新的用户。

步骤4 在FTPS客户端通过FTP命令登录安全FTP服务器实现远程文件管理。

```
[FTPS_Client] ftp ssl-policy ftp_client 10.1.1.1
Trying 10.1.1.1 ...
Press CTRL+K to abort
Connected to 10.1.1.1.
220 FTP service ready.
234 AUTH command successfully, Security mechanism accepted.
200 PBSZ is ok.
200 Data channel security level is changed to private.
User(10.1.1.1:(none)):admin
331 Password required for admin.
Enter password:
230 User logged in.

[ftp]
```

在客户端需要正确输入用户名和密码，才能通过FTPS方式成功登录FTPS服务器。

步骤5 检查配置结果。

在安全FTP服务器端执行命令**display ftp-server**，可以看到SSL策略名称、安全FTP服务器的状态是running。

```
[FTPS_Server] display ftp-server
  FTP server is stopped
  Max user number              5
  User count                   1
  Timeout value(in minute)     30
  Listening port               21
  Acl number                   0
  FTP server's source address  0.0.0.0
  FTP SSL policy               ftp_server
  FTP Secure-server is running
```


在客户端，用户可远程管理服务器上的文件。

----结束

配置文件

- FTPS_Server的配置文件

```
#
sysname FTPS_Server
#
FTP secure-server enable
FTP server-source -i Vlanif10
ftp secure-server ssl-policy ftp_server
#
aaa
 local-user admin password irreversible-cipher $1a$P2m&M5d"'JHR7b~SrcHF\Z\,2R"t&6V|zOLh9y$>M
\bjG$D>%@Ug/<3I$+=Y$
 local-user admin privilege level 3
 local-user admin ftp-directory flash:
 local-user admin service-type ftp
#
ssl policy ftp_server
 certificate load asn1-cert 4_servercert_der_dsa.der key-pair dsa key-file 4_serverkey_der_dsa.der
#
return
```

- FTPS_Client的配置文件

```
#
sysname FTPS_Client
#
ssl policy ftp_client
 trusted-ca load asn1-ca cacert.der
 trusted-ca load asn1-ca rootcert.der
#
return
```

8.6 文件管理的常见配置错误

8.6.1 FTP 登录失败

故障原因

- 未配置FTP服务器端的源地址
- FTP服务器功能没有启动。
- FTP服务器指定端口号不是缺省端口号，且FTP客户端登录时没有指定端口号。
- 未配置FTP用户的验证信息、授权目录及用户级别。
- 登录FTP服务器的用户数达到上限。
- FTP服务器配置了ACL规则限制客户端登录。
- FTP服务器配置了多种认证模式。

操作步骤

步骤1 检查设备上是否配置了FTP服务器端的源地址。

- 对于FTP IPv4

在系统视图下执行命令**display this**，查看是否有**ftp server-source**的配置。如果没有，可以在系统视图下执行命令**ftp server-source**，配置FTP服务器端的源IPv4地址。

- 对于FTP IPv6

  在系统视图下执行命令**display this**，查看是否有**ftp ipv6 server-source**的配置。如果没有，可以在系统视图下执行命令**ftp ipv6 server-source**，配置FTP服务器端的IPv6源地址。

步骤2 检查FTP服务器功能是否启动。

在任意视图下执行命令**display ftp-server**查看FTP服务器的状态。

- 如果FTP服务器没有启动，显示信息如下：

```
<HUAWEI> display ftp-server
Info: The FTP server is already disabled.
```

在系统视图下执行命令**ftp server enable**，使能FTP服务器功能。

```
<HUAWEI> system-view
[HUAWEI] ftp server enable
Info: Succeeded in starting the FTP server.
```

- 如果FTP服务器功能启动，显示信息如下:

```
<HUAWEI> display ftp-server
  FTP server is running
  Max user number              5
  User count                   0
  Timeout value(in minute)     30
  Listening port               21
  Acl number                   0
  FTP server's source address  0.0.0.0
  FTP SSL policy
  FTP Secure-server is stopped
```

步骤3 检查FTP服务器的端口号是否是缺省端口号。

1. 在任意视图下执行命令**display tcp status**查看当前TCP端口尝试连接状态，是否有FTP的缺省端口号是21。

```
<HUAWEI> display tcp status
TCPCB     Tid/Soid Local Add:port       Foreign Add:port      VPNID  State
2a67f47c  6  /1    0.0.0.0:21           0.0.0.0:0             23553  Listening
2b72e6b8  115/4    0.0.0.0:22           0.0.0.0:0             23553  Listening
3265e270  115/1    0.0.0.0:23           0.0.0.0:0             23553  Listening
2a6886ec  115/23   10.137.129.27:23     10.138.77.43:4053     0      Establish
ed
2a680aac  115/14   10.137.129.27:23     10.138.80.193:1525    0      Establish
ed
2a68799c  115/20   10.137.129.27:23     10.138.80.202:3589    0      Establish
ed
```

2. 在任意视图下执行命令**display ftp-server**查看FTP服务器的端口号。

```
<HUAWEI> display ftp-server
  FTP server is running
  Max user number              5
  User count                   0
  Timeout value(in minute)     30
  Listening port               21
  Acl number                   0
  FTP server's source address  0.0.0.0
  FTP SSL policy
  FTP Secure-server is stopped
```

如果当前FTP服务器的端口号不是21，执行命令**ftp server port**，设置FTP服务器的端口号为21。

```
<HUAWEI> system-view
[HUAWEI] undo ftp server
```



```
Warning: The operation will stop the FTP server. Continue? [Y/N]:y
Info: Succeeded in closing the FTP server.
[HUAWEI] ftp server port 21
[HUAWEI] ftp server enable
Info: Succeeded in starting the FTP server.
```

或者在FTP连接时，在客户端指定服务端设置的端口号。

步骤4 检查是否配置FTP用户的验证信息、授权目录及用户级别。

FTP用户名、密码、授权目录和用户级别是必配置项。没有指定FTP授权目录及用户级别而登录失败是常见故障。

1. 执行命令**aaa**，进入AAA视图。
2. 执行命令**local-user** *user-name* **password irreversible-cipher** *password*，配置本地用户名和密码。
3. 执行命令**local-user** *user-name* **ftp-directory** *directory*，配置FTP用户的授权目录。
4. 执行命令**local-user** *user-name* **privilege level** *level*，必须将用户级别配置在3级及3级以上，否则FTP连接将无法成功。

接入类型是可选项。缺省情况下，系统支持所有接入类型。如果配置了其中一项或者几项服务，那么只为该用户提供配置的这几项服务。

执行命令**local-user** *user-name* **service-type ftp**，配置FTP服务类型。

步骤5 检查登录FTP服务器的用户数是否达到上限。

执行命令**display ftp-users**，查看FTP用户数是否达到5个。

步骤6 检查FTP服务器端是否配置了ACL。

执行命令**display** [**ipv6**] **ftp-server**，查看FTP服务器端是否配置了ACL。

如果配置了ACL规则，系统仅允许在ACL规则列表中指定的IP地址登录FTP服务器。

步骤7 检查FTP服务器端是否配置了多种认证模式。

1. 执行命令**aaa**，进入AAA视图。
2. 执行命令**display this**，查看是否配置了多种认证模式。详细信息请参考**AAA配置**。

----结束

8.6.2 上传文件失败

故障原因

- 源路径、目的路径中含有空格等设备不支持的字符。
- 服务器根目录存储空间不足。
- 服务器、客户端由于调整MTU发送的数据帧长度超过了对端所能够承受的最大值，或者是超过了发送路径上途经的某台设备所能够承受的最大值，导致数据帧被丢弃。

操作步骤

步骤1 源路径、目的路径中含有空格等设备不支持的字符。

设备中目录名使用的字符不可以是空格、“~”、“*”、“/”、“\”、“:”、“'”、“"”。

如果路径中含有以上设备不支持的字符，请修改路径。

步骤2 检查服务器根目录存储空间是否不足。

在服务器端执行命令**dir**，查看服务器根目录下的空闲空间。

如果存储空间已满，在用户视图下执行命令**delete /unreserved**删除不需要的文件。

步骤3 检查服务器、客户端接口上配置的MTU是否超过了设备所能承受的最大值。

分别在服务器、客户端的接口视图下执行命令**display this**查看接口当前的MTU值，如果没有显示，则MTU为缺省值1500字节。

如果配置的MTU大小超过了服务器或者客户端所能承受的最大帧长，在该接口视图下执行命令**mtu**减小MTU值。设备所能承受的最大帧长可以参见《FAQ》接口管理 中的“接口MTU和接口允许通过的最大帧长”章节。

----结束

8.7 文件管理 FAQ

8.7.1 如何查看已删除文件

设备提供回收站功能，使用**delete**命令删除的文件保留在回收站中，只有使用**delete / unreserved**命令才能真正删除文件。

使用**dir**命令不显示已经被删除并被放入回收站中的文件，只有使用**dir /all**命令才能显示回收站中的文件，这些文件的文件名被“[]”包含。

8.7.2 设备支持的 SSH 版本号

设备支持的SSH版本号是1.99，即支持SSH1（SSH1.x）协议和SSH2（SSH2.0）协议。

设备做SSH客户端时，只能做SSH服务器端版本为2.0的客户端，不能做SSH服务器端版本为1.x的客户端；设备做SSH服务器端时，允许版本号为1.x和2.0的SSH客户端登录该设备。

8.7.3 为什么 ssh 用户在配置远端认证时必须同时在设备本地配置用户才能通过认证

在设备本地配置用户不是必需操作，当在设备上配置**ssh authentication-type default password**后，无须再在本地配置用户。

8.7.4 当存储设备出现异常时，如何修复

- 如果用户在设备上执行**dir**命令查看设备中的指定文件或目录的信息，当显示信息中含有**unknown**信息时，如: 30,000 KB total (672 KB free, 25,560 KB used, **3,616 KB unknown**)，可以通过在用户视图下执行**fixdisk** *device-name*命令释放**unknown**空间。

  此命令是问题修复类命令，在系统未出现问题时，建议用户不要执行此命令。
- 如果用户在设备上执行**dir**命令查看不到文件，但是存储空间被占用。则可能存在以下情况：

被删除的文件放在回收站中。用户可以执行命令**dir /all**命令显示所有文件信息，包括已经删除的文件信息（用[ ]标识）。此类文件可使用**undelete**命令恢复。若要从回收站中删除该文件，使用**reset recycle-bin**命令。

须知

- 执行**fixdisk** *device-name*命令后，会清空指定存储器中的所有文件和目录，并且不可恢复，请谨慎使用。
- **fixdisk** *device-name*命令无法修复设备级的故障。

8.7.5 如何上传/下载文件

用户可以通过Console口（串口）、FTP、TFTP、SFTP、SCP、FTPS方式，在设备与设备之间或者设备与主机之间传送文件。设备、主机在文件传输的过程中，均可以充当服务器或者客户端的角色。各种文件传输方式的应用场景及优缺点如表8-57所示，用户可以根据需求选择其中一种方式。具体每种传输方式的配置方法请参见相应版本“配置指南-基础配置”中的“文件管理”部分。

表 8-57 文件传输方式

文件传输方式	应用场景	优点	缺点
Console口	通过设备的BootLoad菜单实现，适用于没有网络环境、设备的管理网口损坏或者无法正常登录的场景。	• 只需要使用一根串口线连接主机与设备。 • 传输过程不需要网络环境，可以避免网络带来的不安全因素。	传输速度较慢。
FTP（File Transfer Protocol）	适用于对网络安全性要求不是很高的文件传输场景，广泛用于版本升级等业务中。	• 配置较简单。 • 具有授权和认证功能。	明文传输数据，存在安全隐患。
TFTP（Trivial File Transfer Protocol）	在网络条件良好的实验室局域网中，可以使用TFTP进行版本的在线加载和升级。适用于客户端和服务器之间，不需要复杂交互的环境。	TFTP所占的内存要比FTP小。	TFTP没有授权和认证，且是明文传输数据，存在安全隐患，易于网络病毒传输以及被黑客攻击。
SFTP（Secure File Transfer Protocol）	适用于网络安全性要求高的场景，目前被广泛用于日志下载、配置文件备份等业务中。	数据进行了严格加密和完整性保护，安全性高。	配置较复杂。

文件传输方式	应用场景	优点	缺点
SCP（Secure Copy Protocol）	适用于网络安全性要求高，且文件上传下载效率高的场景。	• 数据进行了严格加密和完整性保护，安全性高。 • 客户端与服务器连接的同时完成文件的上传下载操作（即连接和拷贝操作使用一条命令完成），效率较高。	配置较复杂（与SFTP方式的配置非常类似）。
FTPS（FTP over SSL（Secure Sockets Layer））	适用于网络安全性要求高，且不提供普通FTP功能的场景。	利用数据加密、身份验证和消息完整性验证机制，为基于TCP可靠连接的应用层协议提供安全性保证。	配置较复杂，需要预先从CA处获得一套证书。

说明

- 串口采用的传输协议是XModem协议，用户在传输文件时，注意选择正确的传输协议。
- 对于TFTP方式，设备仅支持作为客户端；对于FTP、SFTP、SCP以及FTPS方式，设备可作为客户端，也可作为服务器。
- 在上传系统文件到设备中时，请保持设备正常供电。否则可能会引起文件损坏或文件系统损坏，从而造成设备存储介质损坏或设备不能正常启动等问题。
- Console口、FTP、TFTP、SFTP、SCP以及FTPS文件传输方式不支持定时从服务器中下载文件。

8.7.6 怎么限制 FTP 上传/下载速度

FTP协议本身没有限速的机制，只能通过在用于FTP客户端/服务器通信的接口上配置接口限速，设置FTP上传或者下载的最高限速。具体请参见相应版本“配置指南-QoS”中的“流量监管、流量整形和接口限速配置”部分。

8.7.7 如何检查文件上传是否完整

用户文件上传完之后，可以通过比较文件上传前后的大小来检查文件上传是否完整。上传文件之前查看并记录文件的大小，文件上传完之后执行**dir**命令查看存储器中文件的大小，比较这两个数值的大小：如果大小一致，说明上传的文件是完整的；如果大小不一致，说明上传的文件不完整，需要执行**delete**命令删除不完整文件，重新上传。

```
<HUAWEI> dir /all
Directory of flash:/

 Idx  Attr     Size(Byte)  Date        Time       FileName
   0  -rw-             14  Feb 27 2012 11:20:12   back_time_a
   1  -rw-             16  Dec 28 2011 13:10:56   abc.tbl
   2  drw-              -  Feb 25 2012 14:19:56   logfile
   3  drw-              -  Oct 31 2011 15:05:26   sysdrv
   4  drw-              -  Feb 25 2012 14:20:08   compatible
   5  drw-              -  Oct 31 2011 15:19:02   selftest
```



```
  6  -rw-           14  Feb 27 2012 11:20:12   back_time_b
  7  -rw-        9,637  Feb 25 2012 14:18:22   vrpcfg.cfg
  8  -rw-            4  Jan 18 2012 16:34:56   snmpnotilog.txt
  9  -rw-        1,968  Feb 25 2012 14:20:22   private-data.txt
 10  -rw-          637  Nov 04 2011 11:48:46   cacert.der
 11  -rw-        4,303  Feb 09 2012 21:16:06   vrpcfg1.cfg.bak
 12  -rw-          639  Nov 04 2011 11:49:04   rootcert.der
 13  drw-            -  Nov 04 2011 11:50:24   security
 14  -rw-           13  Nov 29 2011 20:33:40   tftp_test.txt
 15  -rw-   52,770,448  Dec 05 2011 17:00:06   basicsoft.cc
 16  -rw-   98,139,547  Jan 31 2012 16:11:52   devicesoft.cc
 17  -rw-      463,309  Jan 31 2012 15:55:40   rbsaveddata.txt

509,256 KB total (272,952 KB free)
```

回显信息中的**Size(Byte)**即为文件的大小。

8.7.8 各类型文件的后缀名是什么

各类型文件的后缀名如表8-58所示。

表 8-58 各类型文件的后缀名

文件类型	后缀名
web网页文件	.7z
license文件	.dat
配置文件	.cfg或者.zip
系统文件	.cc
补丁文件	.pat

8.7.9 日志文件存放在哪里

交换机将日志文件保存在主交换机flash的**syslogfile**或**logfile**文件夹下。

```
<HUAWEI>dir            //显示flash目录下的所有文件和文件夹
Directory of flash:/

  Idx  Attr     Size(Byte)  Date        Time       FileName
    0  -rw-         1,766  Dec 24 2040 03:37:54   private-data.txt
    3  drw-             -  Dec 24 2040 03:40:12   syslogfile
    4  drw-             -  Dec 24 2040 03:37:58   compatible
   16  -rw-        10,571  Jan 04 2041 03:51:18   elabel-slot0.fls
......
<HUAWEI>cd logfile          //进入logfile文件夹
<HUAWEI>dir
Directory of flash:/logfile/

  Idx  Attr     Size(Byte)  Date        Time       FileName
    0  -rw-         10,824  Jan 24 2042 09:15:04   logfile-2042-01-24-09-15-03.zip
    1  -rw-         15,334  Feb 03 2042 14:45:08   logfile-2042-02-03-14-45-08.zip
```

8.7.10 如何删除文件

执行**delete** [**/unreserved**] [**/quiet**] { *filename* | *devicename* } [**all**]命令可以删除存储器中的指定文件，包括系统文件、配置文件、paf、license、日志文件等。

- 删除存储器中的文件。

```
<HUAWEI> delete test.txt
Delete flash:/test.txt?[Y/N]:y
Info: Deleting file flash:/test.txt...succeeded.
```

  说明

  - 以上显示信息请以设备实际显示为准。
  - 参数**all**仅在设备堆叠情况下支持该参数。指定参数**all**可以批量删除所有成员设备上对应路径下的文件。
  - 不能在命令行界面删除设备当前正在使用的版本文件（包括系统软件、补丁文件、Web网页文件和配置文件等）。

- 日志文件保存在Flash的**logfile**或**syslogfile**目录下。用户可以切换到**logfile**或**syslogfile**目录下删除日志文件，也可以在Flash下使用绝对路径删除日志文件。

  # 切换到**logfile**目录下删除日志文件。

```
<HUAWEI> cd logfile/
<HUAWEI> delete logfile-2013-01-24-09-15-03.zip
Delete flash:/logfile/logfile-2013-01-24-09-15-03.zip?[Y/N]:y
Info: Deleting file flash:/logfile/logfile-2013-01-24-09-15-03.zip...succeeded.
```

  # 在Flash下使用绝对路径删除日志文件。

```
<HUAWEI> delete flash:/logfile/logfile-2013-01-24-09-15-03.zip
Delete flash:/logfile/logfile-2013-01-24-09-15-03.zip?[Y/N]:y
Info: Deleting file flash:/logfile/logfile-2013-01-24-09-15-03.zip...succeeded.
```

8.7.11 怎么在两台设备之间传送文件

如果需要在两台设备之间传送文件，例如补丁文件、配置文件等，可以将一台设备作为服务器，另一台设备作为客户端，使用FTP、TFTP、SFTP、SCP和FTPS方式在服务器设备和客户端设备之间上传或者下载文件，具体请参见相应版本“配置指南-基础配置”中的“文件管理”部分。

