

目 录

1 SSH	1-1
1.1 SSH服务器端配置命令	1-1
1.1.1 display ssh server	1-1
1.1.2 display ssh user-information	1-2
1.1.3 sftp server enable	1-4
1.1.4 sftp server idle-timeout	1-4
1.1.5 ssh server authentication-retries	1-5
1.1.6 ssh server authentication-timeout	1-6
1.1.7 ssh server compatible-ssh1x enable	1-6
1.1.8 ssh server enable	1-7
1.1.9 ssh server rekey-interval	1-7
1.1.10 ssh user	1-8
1.2 SSH客户端配置命令	1-10
1.2.1 bye	1-10
1.2.2 cd	1-10
1.2.3 cdup	1-11
1.2.4 delete	1-11
1.2.5 dir	1-12
1.2.6 display sftp client source	1-13
1.2.7 display ssh client source	1-13
1.2.8 display ssh server-info	1-14
1.2.9 exit	1-15
1.2.10 get	1-15
1.2.11 help	1-16
1.2.12 ls	1-16
1.2.13 mkdir	1-17
1.2.14 put	1-18
1.2.15 pwd	1-18
1.2.16 quit	1-19
1.2.17 remove	1-19
1.2.18 rename	1-20
1.2.19 rmdir	1-20
1.2.20 scp	1-21

1.2.21 sftp	1-22
1.2.22 sftp client ipv6 source.....	1-24
1.2.23 sftp client source	1-25
1.2.24 sftp ipv6.....	1-26
1.2.25 ssh client authentication server.....	1-28
1.2.26 ssh client first-time enable.....	1-28
1.2.27 ssh client ipv6 source.....	1-29
1.2.28 ssh client source	1-30
1.2.29 ssh2.....	1-30
1.2.30 ssh2 ipv6	1-32

1 SSH

1.1 SSH服务器端配置命令

1.1.1 display ssh server

【命令】

display ssh server { **session** | **status** } [| { **begin** | **exclude** | **include** } *regular-expression*]

【视图】

任意视图

【缺省级别】

1: 监控级

【参数】

session: 显示 SSH 服务器的会话信息。

status: 显示 SSH 服务器的状态信息。

|: 使用正则表达式对显示信息进行过滤。有关正则表达式的详细介绍，请参见“基础配置指导”中的“CLI”。

begin: 从包含指定正则表达式的行开始显示。

exclude: 只显示不包含指定正则表达式的行。

include: 只显示包含指定正则表达式的行。

regular-expression: 表示正则表达式，为 1~256 个字符的字符串，区分大小写。

【描述】

display ssh server 命令用来在 SSH 服务器端显示该服务器的状态信息或会话信息。

相关配置可参考命令 **ssh server authentication-retries**、**ssh server rekey-interval**、**ssh server authentication-timeout**、**ssh server enable** 和 **ssh server compatible-ssh1x enable**。

【举例】

在 SSH 服务器端显示该服务器的状态信息。

```
<Sysname> display ssh server status
SSH server: Disable
SSH version : 1.99
SSH authentication-timeout : 60 second(s)
SSH server key generating interval : 0 hour(s)
SSH authentication retries : 3 time(s)
SFTP server: Disable
SFTP server Idle-Timeout: 10 minute(s)
```

表1-1 display ssh server status 命令显示信息描述表

字段	描述
SSH server	SSH服务器功能的状态

字段	描述
SSH version	SSH协议版本 SSH服务器兼容SSH1时，协议版本为1.99；SSH服务器不兼容SSH1时，协议版本为2.0
SSH authentication-timeout	认证超时时间
SSH server key generating interval	服务器密钥对更新时间
SSH authentication retries	认证尝试的最大次数
SFTP server	SFTP服务器功能的状态
SFTP server Idle-Timeout	SFTP用户连接的空闲超时时间

在 SSH 服务器端显示该服务器的会话信息。

```
<Sysname> display ssh server session
```

```
Conn  Ver  Encry  State          Retry  SerType  Username
VTY 0  2.0  DES    Established    0      SFTP     client001
```

表1-2 display ssh server session 显示信息描述表

字段	描述
Conn	用户登录使用的VTY界面的编号
Ver	SSH服务器的协议版本
Encry	SSH使用的加密算法
State	会话状态，包括： <ul style="list-style-type: none"> • Init: 初始化状态 • Ver-exchange: 版本协商 • Keys-exchange: 密钥交换 • Auth-request: 用户认证 • Serv-request: 服务请求 • Established: 连接已经建立 • Disconnected: 断开连接
Retry	认证失败的次数
SerType	服务类型，包括SCP、SFTP和Stelnet三种类型
Username	客户端登录服务器时采用的用户名

1.1.2 display ssh user-information

【命令】

```
display ssh user-information [ username ] [ | { begin | exclude | include }
regular-expression ]
```

【视图】

任意视图

【缺省级别】

1: 监控级

【参数】

username: 显示指定 SSH 用户的信息。**username** 表示 SSH 用户名, 为 1~80 个字符的字符串。

|: 使用正则表达式对显示信息进行过滤。有关正则表达式的详细介绍, 请参见“基础配置指导”中的“CLI”。

begin: 从包含指定正则表达式的行开始显示。

exclude: 只显示不包含指定正则表达式的行。

include: 只显示包含指定正则表达式的行。

regular-expression: 表示正则表达式, 为 1~256 个字符的字符串, 区分大小写。

【描述】

display ssh user-information 命令用来在 SSH 服务器端显示 SSH 用户的信息。

需要注意的是:

- 本命令仅用来显示 SSH 服务器端通过 **ssh user** 命令配置的 SSH 用户信息。
- 如果没有指定参数 **username**, 则显示所有 SSH 用户的信息。

相关配置可参考命令 **ssh user**。

【举例】

显示所有 SSH 用户的信息。

```
<Sysname> display ssh user-information
Total ssh users : 2
Username      Authentication-type  User-public-key-name  Service-type
yemx         password            null                  stelnet
test         publickey           pubkey                 sftp
```

表1-3 display ssh user-information 显示信息描述表

字段	描述
Total ssh users	SSH用户的总数
Username	用户名
Authentication-type	认证类型, 如果认证类型为password, 则用户公钥名称显示为null
User-public-key-name	用户公钥名称或认证客户端证书的PKI域名
Service-type	服务类型, 包括stelnet、sftp、scp以及all, 其中all表示支持所有认证类型

1.1.3 sftp server enable

【命令】

sftp server enable
undo sftp server enable

【视图】

系统视图

【缺省级别】

3: 管理级

【参数】

无

【描述】

sftp server enable 命令用来启动 SFTP 服务器。**undo sftp server enable** 命令用来关闭 SFTP 服务器。

缺省情况下，SFTP 服务器处于关闭状态。

可以使用 **display ssh server** 命令来查看 SFTP 服务器端的相关状态信息或会话信息。

相关配置可参考命令 **display ssh server**。

【举例】

```
# 启动 SFTP 服务器。  
<Sysname> system-view  
[Sysname] sftp server enable
```

1.1.4 sftp server idle-timeout

【命令】

sftp server idle-timeout *time-out-value*
undo sftp server idle-timeout

【视图】

系统视图

【缺省级别】

3: 管理级

【参数】

time-out-value: 超时时间，取值范围为 1~35791，单位为分钟。

【描述】

sftp server idle-timeout 命令用来在 SFTP 服务器端设置 SFTP 用户连接的空闲超时时间。**undo sftp server idle-timeout** 命令用来恢复缺省情况。

缺省情况下，SFTP 用户连接的空闲超时时间为 10 分钟。

当 SFTP 用户连接的空闲时间超过设定的阈值后，系统会自动断开此用户的连接，从而有效避免用户长期占用连接而不进行任何操作。若同一时间内并发的 SFTP 连接数较多，可适当减小该值，及时释放系统资源给新用户接入。

相关配置可参考命令 **display ssh server**。

【举例】

```
# 设置 SFTP 用户连接的空闲超时时间为 500 分钟。
```

```
<Sysname> system-view  
[Sysname] sftp server idle-timeout 500
```

1.1.5 ssh server authentication-retries

【命令】

```
ssh server authentication-retries times  
undo ssh server authentication-retries
```

【视图】

系统视图

【缺省级别】

3: 管理级

【参数】

times: 指定认证尝试的最大次数，取值范围为 1~5。

【描述】

ssh server authentication-retries 命令用来设置 SSH 连接认证尝试的最大次数。**undo ssh server authentication-retries** 命令用来恢复缺省情况。

缺省情况下，SSH 连接认证尝试的最大次数为 3 次。

通过本命令可以限制用户登录的重试次数，防止非法用户对用户名和密码进行恶意地猜测和破解。

需要注意的是：

- 本配置对新登录的用户生效。
- SSH 客户端通过 **publickey** 和 **password** 两种方式进行认证尝试的次数总和，不能超过 **ssh server authentication-retries** 命令配置的 SSH 连接认证尝试的最大次数。
- 对于 **password-publickey** 认证方式，设备首先对 SSH 用户进行 **publickey** 认证，然后进行 **password** 认证，这个过程称为一次认证尝试，而不是两次认证尝试。

相关配置可参考命令 **display ssh server**。

【举例】

```
# 指定登录认证尝试的最大次数为 4 次。
```

```
<Sysname> system-view  
[Sysname] ssh server authentication-retries 4
```

1.1.6 ssh server authentication-timeout

【命令】

```
ssh server authentication-timeout time-out-value  
undo ssh server authentication-timeout
```

【视图】

系统视图

【缺省级别】

3: 管理级

【参数】

time-out-value: 认证超时时间，取值范围为 1~120，单位为秒。

【描述】

ssh server authentication-timeout 命令用来在 SSH 服务器端设置 SSH 用户的认证超时时间，如果用户在规定的时间内没有完成认证就拒绝该连接。**undo ssh server authentication-timeout** 命令用来恢复缺省情况。

缺省情况下，SSH 用户的认证超时时间为 60 秒。

为了防止不法用户建立起 TCP 连接后，不进行接下来的认证，而是空占着进程，妨碍其它合法用户的正常登录，可以适当调小 SSH 用户认证超时时间。

相关配置可参考命令 **display ssh server**。

【举例】

设置 SSH 用户认证超时时间为 10 秒。

```
<Sysname> system-view  
[Sysname] ssh server authentication-timeout 10
```

1.1.7 ssh server compatible-ssh1x enable

【命令】

```
ssh server compatible-ssh1x enable  
undo ssh server compatible-ssh1x
```

【视图】

系统视图

【缺省级别】

3: 管理级

【参数】

无

【描述】

ssh server compatible-ssh1x enable 命令用来设置 SSH 服务器兼容 SSH1 版本的客户端。

undo ssh server compatible-ssh1x 命令用来设置 SSH 服务器不兼容 SSH1 版本的客户端。

缺省情况下，SSH 服务器兼容 SSH1 版本的客户端。

该配置对新登录的用户生效。

相关配置可参考命令 **display ssh server**。

【举例】

配置服务器兼容 SSH1 版本的客户端。

```
<Sysname> system-view  
[Sysname] ssh server compatible-sshlx enable
```

1.1.8 ssh server enable

【命令】

```
ssh server enable  
undo ssh server enable
```

【视图】

系统视图

【缺省级别】

3: 管理级

【参数】

无

【描述】

ssh server enable 命令用来使能 SSH 服务器功能,使客户端能用 SSH 协议与服务器进行通信。

undo ssh server enable 命令用来关闭 SSH 服务器功能。

缺省情况下, SSH 服务器功能处于关闭状态。

相关配置可参考命令 **display ssh server**。

【举例】

使能 SSH 服务器功能。

```
<Sysname> system-view  
[Sysname] ssh server enable
```

1.1.9 ssh server rekey-interval

【命令】

```
ssh server rekey-interval hours  
undo ssh server rekey-interval
```

【视图】

系统视图

【缺省级别】

3: 管理级

【参数】

hours: 服务器密钥的更新周期,取值范围为 1~24,单位为小时。

【描述】

ssh server rekey-interval 命令用来设置 RSA 服务器密钥的更新时间。**undo ssh server rekey-interval** 命令用来恢复缺省情况。

缺省情况下，RSA 服务器密钥的更新时间为 0，表示系统不更新 RSA 服务器密钥。

SSH 的核心是密钥的协商和传输，因此密钥的管理是非常重要的。通过定时更新服务器密钥，可以防止对密钥的恶意猜测和破解，从而提高了 SSH 连接的安全性。

相关配置可参考命令 **display ssh server**。



注意

- 此命令仅对 SSH 客户端版本为 SSH1 的用户有效。
 - 系统不会定期更新 DSA 密钥对。
-

【举例】

设置每 3 小时更新一次 RSA 服务器密钥。

```
<Sysname> system-view
[Sysname] ssh server rekey-interval 3
```

1.1.10 ssh user

【命令】

```
ssh user username service-type stelnet authentication-type { password | { any | password-publickey | publickey } assign { pki-domain pkiname | publickey keyname } }
ssh user username service-type { all | scp | sftp } authentication-type { password | { any | password-publickey | publickey } assign { pki-domain pkiname | publickey keyname }
work-directory directory-name }
undo ssh user username
```

【视图】

系统视图

【缺省级别】

3: 管理级

【参数】

username: SSH 用户名，为 1~80 个字符的字符串，区分大小写。

service-type: SSH 用户的服务类型。包括：

all: 包括 **scp**、**sftp** 和 **stelnet** 三种服务类型。

scp: 服务类型为 SCP（Secure Copy 的简称）。

sftp: 服务类型为 SFTP（Secure FTP 的简称）。

stelnet: 服务类型为 Stelnet（Secure Telnet 的简称）。

authentication-type: SSH 用户的认证方式。包括：

- **password:** 强制用户使用密码认证。该认证方式的加密机制简单，加密速度快，可结合 AAA（Authentication, Authorization, Accounting，认证、授权、计费）实现对用户认证、授权和计费，但容易受到攻击。
- **any:** 不指定用户的认证方式，用户既可以采用 password 认证，也可以采用 publickey 认证。
- **password-publickey:** 指定客户端版本为 SSH2 的用户认证方式为必须同时进行 password 和 publickey 两种认证，安全性更高；客户端版本为 SSH1 的用户认证方式为只要进行其中一种认证即可。
- **publickey:** 强制用户使用公钥认证。该认证方式的加密速度相对较慢，但认证强度高，不易受到“暴力猜测”等攻击方式的影响，而且具有较高的易用性。一次配置成功后，后续认证过程自动完成，不需要用户记忆和输入密码。

assign: 指定用于验证客户端的参数。

- **pki-domain pkiname:** 指定验证客户端证书的 PKI 域。*pkiname* 表示 PKI 域的名称，为 1~15 个字符的字符串，不区分大小写。服务器端使用保存在该 PKI 域中的 CA 证书对客户端证书进行合法性检查，无需提前保存客户端的公钥，能够灵活满足大数量客户端的认证需求。
- **publickey keyname:** 指定 SSH 用户的公钥。*keyname* 表示已经配置的客户端公钥名称，为 1~64 个字符的字符串，区分大小写。服务器端使用提前保存在本地的用户公钥对用户进行合法性检查，如果客户端密钥文件改变，服务器端需要及时更新本地配置。

work-directory directory-name: 为 SCP 或 SFTP 用户设置工作目录。*directory-name* 表示 SCP 或 SFTP 用户的工作目录，为 1~135 个字符的字符串。

【描述】

ssh user 命令用来创建 SSH 用户，并指定 SSH 用户的服务类型和认证方式。**undo ssh user** 命令用来删除 SSH 用户。

需要注意的是：

- 如果服务器采用 publickey 方式认证客户端，则必须通过本配置在设备上创建相应的 SSH 用户；如果服务器采用 password 方式认证客户端，则必须将 SSH 用户的账号信息配置在设备（适用于本地认证）或者远程认证服务器（如 RADIUS 服务器，适用于远程认证）上，而并不要求通过本配置创建相应的 SSH 用户。
- 使用该命令指定公钥或 PKI 域时，则以最后一次指定的参数为准。
- 对于已经登录的 SSH 用户的参数修改，仅在该用户重新登录后生效。
- 如果为 SCP 或 SFTP 用户指定了公钥或 PKI 域，则必须同时为该用户设置工作目录。
- SCP 或 SFTP 用户登录时使用的工作目录与用户使用的认证方式有关。采用 publickey 或 password-publickey 认证方式的用户，使用的工作目录为通过 **ssh user** 命令为该用户设置的工作目录；只采用 password 认证方式的用户，使用的工作目录为通过 AAA 授权的工作目录。

相关配置可参考命令 **display ssh user-information** 和“安全命令参考/PKI”中的 **pki domain**。

【举例】

创建 SSH 用户 user1，配置 user1 的服务类型为 SFTP，认证方式为 publickey，并指定客户端公钥为 key1，SFTP 服务器工作目录为 flash:。

```
<Sysname> system-view
```

```
[Sysname] ssh user user1 service-type sftp authentication-type publickey assign publickey  
key1 work-directory flash:
```

1.2 SSH客户端配置命令

1.2.1 bye

【命令】

bye

【视图】

SFTP 客户端视图

【缺省级别】

3: 管理级

【参数】

无

【描述】

bye 命令用来终止与远程 SFTP 服务器的连接，并退回到用户视图。
该命令功能与 **exit**、**quit** 相同。

【举例】

```
# 终止与远程 SFTP 服务器的连接。  
sftp-client> bye  
Bye  
Connection closed.  
<Sysname>
```

1.2.2 cd

【命令】

cd [*remote-path*]

【视图】

SFTP 客户端视图

【缺省级别】

3: 管理级

【参数】

remote-path: 服务器上的路径名。

【描述】

cd 命令用来改变远程 SFTP 服务器上的工作路径。
如果没有指定 *remote-path*，则显示当前工作路径。



说明

- 命令“cd ..”用来返回到上一级目录。
 - 命令“cd /”用来返回到系统的根目录。
-

【举例】

```
# 改变工作路径到 new1。
sftp-client> cd new1
Current Directory is:
/new1
```

1.2.3 cdup

【命令】

cdup

【视图】

SFTP 客户端视图

【缺省级别】

3: 管理级

【参数】

无

【描述】

cdup 命令用来返回到上一级目录。

【举例】

```
# 从当前工作目录/new1 返回到上一级目录。
sftp-client> cdup
Current Directory is:
/
```

1.2.4 delete

【命令】

delete remote-file<1-10>

【视图】

SFTP 客户端视图

【缺省级别】

3: 管理级

【参数】

remote-file&<1-10>: 服务器上的文件名。&<1-10>表示最多可以输入 10 个文件名，每个文件名之间用空格分隔。

【描述】

delete 命令用来删除 SFTP 服务器上指定的文件。

该命令和 **remove** 功能相同。

【举例】

```
# 删除服务器上的文件 temp.c。
sftp-client> delete temp.c
The following files will be deleted:
/temp.c
Are you sure to delete it? [Y/N]:y
This operation may take a long time.Please wait...

File successfully Removed
```

1.2.5 dir

【命令】

dir [**-a** | **-l**] [*remote-path*]

【视图】

SFTP 客户端视图

【缺省级别】

3: 管理级

【参数】

-a: 显示指定目录下文件及文件夹的名称。

-l: 以列表的形式显示指定目录下文件及文件夹的详细信息。

remote-path: 查询的目录名。

【描述】

dir 命令用来显示指定目录下文件及文件夹的信息。

如果没有指定 **-a** 和 **-l** 参数，则以列表的形式显示指定目录下文件及文件夹的详细信息。

如果没有指定 *remote-path*，则显示当前工作目录下文件及文件夹的信息。

该命令功能与 **ls** 相同。

【举例】

```
# 以列表的形式显示当前工作目录下文件及文件夹的详细信息。
sftp-client> dir
-rwxrwxrwx  1 noone    nogroup      1759 Aug 23 06:52 config.cfg
-rwxrwxrwx  1 noone    nogroup        225 Aug 24 08:01 pubkey2
-rwxrwxrwx  1 noone    nogroup        283 Aug 24 07:39 pubkey1
-rwxrwxrwx  1 noone    nogroup        225 Sep 28 08:28 publ
```

```
drwxrwxrwx  1 noone  nogroup      0 Sep 28 08:24 new1
drwxrwxrwx  1 noone  nogroup      0 Sep 28 08:18 new2
-rwxrwxrwx  1 noone  nogroup    225 Sep 28 08:30 pub2
```

1.2.6 display sftp client source

【命令】

display sftp client source [| { **begin** | **exclude** | **include** } *regular-expression*]

【视图】

任意视图

【缺省级别】

1: 监控级

【参数】

|: 使用正则表达式对显示信息进行过滤。有关正则表达式的详细介绍，请参见“基础配置指导”中的“CLI”。

begin: 从包含指定正则表达式的行开始显示。

exclude: 只显示不包含指定正则表达式的行。

include: 只显示包含指定正则表达式的行。

regular-expression: 表示正则表达式，为 1~256 个字符的字符串，区分大小写。

【描述】

display sftp client source 命令用来显示当前为 SFTP 客户端设置的源 IP 地址或者源接口。

如果没有为 SFTP 客户端指定源地址和源接口，则提示尚未指定。

相关配置可参考命令 **sftp client source**。

【举例】

显示 SFTP 客户端的源 IP 地址。

```
<Sysname> display sftp client source
The source IP address you specified is 192.168.0.1
```

1.2.7 display ssh client source

【命令】

display ssh client source [| { **begin** | **exclude** | **include** } *regular-expression*]

【视图】

任意视图

【缺省级别】

1: 监控级

【参数】

|: 使用正则表达式对显示信息进行过滤。有关正则表达式的详细介绍，请参见“基础配置指导”中的“CLI”。

begin: 从包含指定正则表达式的行开始显示。

exclude: 只显示不包含指定正则表达式的行。

include: 只显示包含指定正则表达式的行。

regular-expression: 表示正则表达式，为 1~256 个字符的字符串，区分大小写。

【描述】

display ssh client source 命令用来显示当前为 Stelnet 客户端设置的源 IP 地址或者源接口。

如果没有为 Stelnet 客户端指定源地址和源接口，则提示尚未指定。

相关配置可参考命令 **ssh client source**。

【举例】

显示 Stelnet 客户端的源 IP 地址或者源接口。

```
<Sysname> display ssh client source  
The source IP address you specified is 192.168.0.1
```

1.2.8 display ssh server-info

【命令】

display ssh server-info [| { **begin** | **exclude** | **include** } *regular-expression*]

【视图】

任意视图

【缺省级别】

1: 监控级

【参数】

|: 使用正则表达式对显示信息进行过滤。有关正则表达式的详细介绍，请参见“基础配置指导”中的“CLI”。

begin: 从包含指定正则表达式的行开始显示。

exclude: 只显示不包含指定正则表达式的行。

include: 只显示包含指定正则表达式的行。

regular-expression: 表示正则表达式，为 1~256 个字符的字符串，区分大小写。

【描述】

display ssh server-info 命令用来在 SSH 客户端显示客户端保存的服务器端的主机公钥和服务器的对应关系。

SSH 客户端需要认证服务器时，以本地保存的服务器端的主机公钥对连接的服务器进行认证。如果认证不成功，可以通过 **display ssh server-info** 命令查看服务器是否与正确的公钥对应。

相关配置可参考命令 **ssh client authentication server**。



说明

该命令也可在 SFTP 客户端使用。

【举例】

显示客户端保存的服务器端的主机公钥和服务器的对应关系。

```
<Sysname> display ssh server-info
Server Name(IP)                Server public key name
-----
192.168.0.1                    abc_key01
192.168.0.2                    abc_key02
```

表1-4 display ssh server-info 显示信息描述表

字段	描述
Server Name(IP)	服务器名称或者IP地址
Server public key name	服务器端的主机公钥名称

1.2.9 exit

【命令】

exit

【视图】

SFTP 客户端视图

【缺省级别】

3: 管理级

【参数】

无

【描述】

exit 命令用来终止与远程 SFTP 服务器的连接，并退回到用户视图。
该命令功能与 **bye**、**quit** 相同。

【举例】

终止与远程 SFTP 服务器的连接。

```
sftp-client> exit
Bye
Connection closed.
<Sysname>
```

1.2.10 get

【命令】

get remote-file [local-file]

【视图】

SFTP 客户端视图

【缺省级别】

3: 管理级

【参数】

remote-file: 远程 SFTP 服务器上的文件名。

local-file: 本地文件名。

【描述】

get 命令用来从远程服务器上下载文件并存储在本机。

如果没有指定本地文件名，则认为本地文件与远程 SFTP 服务器上的文件同名。

【举例】

下载远程服务器上的 **temp1.c** 文件，并以文件名 **temp.c** 在本机保存。

```
sftp-client> get temp1.c temp.c
Remote file:/temp1.c ---> Local file: temp.c
Downloading file successfully ended
```

1.2.11 help

【命令】

help [**all** | *command-name*]

【视图】

SFTP 客户端视图

【缺省级别】

3: 管理级

【参数】

all: 显示所有命令的名字。

command-name: 命令名。

【描述】

help 命令用来显示 SFTP 客户端命令的帮助信息。

如果没有指定参数，系统将显示所有命令的名字。

【举例】

查看命令 **get** 的帮助信息。

```
sftp-client> help get
get remote-path [local-path] Download file.Default local-path is the same
as remote-path
```

1.2.12 ls

【命令】

ls [**-a** | **-l**] [*remote-path*]

【视图】

SFTP 客户端视图

【缺省级别】

3: 管理级

【参数】

-a: 显示指定目录下文件及文件夹的名称。

-l: 以列表的形式显示指定目录下文件及文件夹的详细信息。

remote-path: 查询的目录名。

【描述】

ls 命令用来显示指定目录下文件及文件夹的信息。

如果没有指定 **-a** 和 **-l** 参数，则以列表的形式显示指定目录下文件及文件夹的详细信息。

如果没有指定 *remote-path*，则显示当前工作目录下文件及文件夹的信息。

该命令功能与 **dir** 相同。

【举例】

以列表的形式显示当前工作目录下文件及文件夹的详细信息。

```
sftp-client> ls
-rwxrwxrwx  1 noone   nogroup    1759 Aug 23 06:52 config.cfg
-rwxrwxrwx  1 noone   nogroup     225 Aug 24 08:01 pubkey2
-rwxrwxrwx  1 noone   nogroup     283 Aug 24 07:39 pubkey1
-rwxrwxrwx  1 noone   nogroup     225 Sep 28 08:28 pub1
drwxrwxrwx  1 noone   nogroup      0 Sep 28 08:24 new1
drwxrwxrwx  1 noone   nogroup      0 Sep 28 08:18 new2
-rwxrwxrwx  1 noone   nogroup     225 Sep 28 08:30 pub2
```

1.2.13 mkdir

【命令】

mkdir *remote-path*

【视图】

SFTP 客户端视图

【缺省级别】

3: 管理级

【参数】

remote-path: 远程 SFTP 服务器上的目录名。

【描述】

mkdir 命令用来在远程 SFTP 服务器上创建新的目录。

【举例】

在远程 SFTP 服务器上建立目录 **test**。

```
sftp-client> mkdir test
```

New directory created

1.2.14 put

【命令】

put *local-file* [*remote-file*]

【视图】

SFTP 客户端视图

【缺省级别】

3: 管理级

【参数】

local-file: 本地的文件名。

remote-file: 远程 SFTP 服务器上的文件名。

【描述】

put 命令用来将本地的文件上传到远程 SFTP 服务器。

如果没有指定远程服务器上的文件名，则认为服务器上的文件与本地文件同名。

【举例】

将本地 **temp.c** 文件上传到远程 SFTP 服务器，并以 **temp1.c** 文件名保存。

```
sftp-client> put temp.c temp1.c
Local file:temp.c ---> Remote file: /temp1.c
Uploading file successfully ended
```

1.2.15 pwd

【命令】

pwd

【视图】

SFTP 客户端视图

【缺省级别】

3: 管理级

【参数】

无

【描述】

pwd 命令用来显示远程 SFTP 服务器上的当前工作目录。

【举例】

显示远程 SFTP 服务器上的当前工作目录。

```
sftp-client> pwd
/
```

1.2.16 quit

【命令】

quit

【视图】

SFTP 客户端视图

【缺省级别】

3: 管理级

【参数】

无

【描述】

quit 命令用来终止与远程 SFTP 服务器的连接，并退回到用户视图。
该命令功能与 **bye**、**exit** 相同。

【举例】

终止与远程 SFTP 服务器的连接。

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

1.2.17 remove

【命令】

remove *remote-file*&<1-10>

【视图】

SFTP 客户端视图

【缺省级别】

3: 管理级

【参数】

remote-file&<1-10>: 服务器上的文件名。&<1-10>表示最多可以输入 10 个文件名，每个文件名之间用空格分隔。

【描述】

remove 命令用来删除 SFTP 服务器上指定的文件。
该命令和 **delete** 功能相同。

【举例】

删除服务器上的文件 temp.c。

```
sftp-client> remove temp.c
The following files will be deleted:
/temp.c
```

```
Are you sure to delete it? [Y/N]:y
This operation may take a long time.Please wait...

File successfully Removed
```

1.2.18 rename

【命令】

```
rename oldname newname
```

【视图】

SFTP 客户端视图

【缺省级别】

3: 管理级

【参数】

oldname: 原文件名或者目录名。

newname: 新文件名或者目录名。

【描述】

rename 命令用来改变 SFTP 服务器上指定的文件或者目录的名字。

【举例】

将 SFTP 服务器上的文件 **temp1.c** 改名为 **temp2.c**。

```
sftp-client> rename temp1.c temp2.c
File successfully renamed
```

1.2.19 rmdir

【命令】

```
rmdir remote-path&<1-10>
```

【视图】

SFTP 客户端视图

【缺省级别】

3: 管理级

【参数】

remote-path&<1-10>: 远程 SFTP 服务器上的目录名。**&<1-10>**表示最多可以输入 10 个目录名，每个文件名之间用空格分隔。

【描述】

rmdir 命令用来删除 SFTP 服务器上指定的目录。

【举例】

删除 SFTP 服务器上当前工作目录下的 **temp1** 目录。

```
sftp-client> rmdir temp1
Directory successfully removed
```

1.2.20 scp

【命令】

在非 FIPS 模式下：

```
scp [ ipv6 ] server [ port-number ] { get | put } source-file-path [ destination-file-path ]  
[ identity-key { dsa | rsa } | prefer-compress { zlib | zlib-openssh } | prefer-ctos-cipher  
{ 3des | aes128 | des } | prefer-ctos-hmac { md5 | md5-96 | sha1 | sha1-96 } | prefer-kex  
{ dh-group-exchange | dh-group1 | dh-group14 } | prefer-stoc-cipher { 3des | aes128 | des }  
| prefer-stoc-hmac { md5 | md5-96 | sha1 | sha1-96 } ] *
```

在 FIPS 模式下：

```
scp [ ipv6 ] server [ port-number ] { get | put } source-file-path [ destination-file-path ]  
[ identity-key rsa | prefer-compress { zlib | zlib-openssh } | prefer-ctos-cipher { aes128 |  
aes256 } | prefer-ctos-hmac { sha1 | sha1-96 } | prefer-kex dh-group14 | prefer-stoc-cipher  
{ aes128 | aes256 } | prefer-stoc-hmac { sha1 | sha1-96 } ] *
```

【视图】

用户视图

【缺省级别】

3: 管理级

【参数】

ipv6: 指定 IPv6 服务器。若不指定该参数，则表示指定 IPv4 服务器。

server: 服务器的 IP 地址或主机名称。指定为 IPv4 服务器时，**server** 为 1~255 个字符的字符串，不区分大小写。

port-number: 服务器端口号，取值范围为 0~65535，缺省值为 22。

get: 指定下载文件操作。

put: 指定上传文件操作。

source-file-path: 源文件路径。

destination-file-path: 目的文件路径。不指定该参数时，表示使用源文件路径作为目的文件名称。

identity-key: publickey 认证采用的公钥算法，在非 FIPS 模式下，可以选择 DSA 或 RSA 任何一种；在 FIPS 模式下只支持 RSA 算法。

- **dsa**: 公钥算法为 DSA。

- **rsa**: 公钥算法为 RSA。

prefer-compress: 首选压缩算法，缺省为无压缩。

- **zlib**: ZLIB 压缩算法。

- **zlib-openssh**: ZLIB@openssh.com 压缩算法。

prefer-ctos-cipher: 客户端到服务器端的首选加密算法，缺省算法为 **aes128**。

- **3des**: 3des-cbc 加密算法，FIPS 模式下不支持该参数。

- **aes128**: aes128-cbc 加密算法。

- **aes256**: aes256-cbc 加密算法，非 FIPS 模式下不支持该参数。

- **des**: des-cbc 加密算法，FIPS 模式下不支持该参数。

prefer-ctos-hmac: 客户端到服务器端的首选 HMAC 算法，缺省算法为 **sha1-96**。

- **md5:** HMAC 算法 hmac-md5, FIPS 模式下不支持该参数。
- **md5-96:** HMAC 算法 hmac-md5-96, FIPS 模式下不支持该参数。
- **sha1:** HMAC 算法 hmac-sha1。
- **sha1-96:** HMAC 算法 hmac-sha1-96。

prefer-kex: 密钥交换首选算法，缺省算法为 **dh-group-exchange**。

- **dh-group-exchange:** 密钥交换算法 diffie-hellman-group-exchange-sha1, FIPS 模式下不支持该参数。
- **dh-group1:** 密钥交换算法 diffie-hellman-group1-sha1, FIPS 模式下不支持该参数。
- **dh-group14:** 密钥交换算法 diffie-hellman-group14-sha1。

prefer-stoc-cipher: 服务器端到客户端的首选加密算法，缺省算法为 **aes128**。

prefer-stoc-hmac: 服务器端到客户端的首选 HMAC 算法，缺省算法为 **sha1-96**

【描述】

scp 命令用来与远程 SCP 服务器建立连接，并进行文件传输。

需要注意的是，当服务器端指定客户端的认证方式为 **publickey** 认证时，客户端需要读取本地的私钥进行验证。在非 FIPS 模式下，由于 **publickey** 认证可以采用 RSA 和 DSA 两种加密算法，所以需要 **identity-key** 关键字指定采用的加密算法，才能得到正确的本地私钥数据。

在非 FIPS 模式下，缺省的算法如下：

- 公钥缺省算法为 **dsa**。
- 客户端到服务器端的首选加密算法，缺省算法为 **aes128**。
- 客户端到服务器端的首选 HMAC 算法，缺省算法为 **sha1-96**。
- 密钥交换首选算法，缺省算法为 **dh-group-exchange**。
- 服务器端到客户端的首选加密算法，缺省算法为 **aes128**。
- 服务器端到客户端的首选 HMAC 算法，缺省算法为 **sha1-96**。

在 FIPS 模式下，缺省的算法如下：

- 公钥缺省算法为 **rsa**。
- 客户端到服务器端的首选加密算法，缺省算法为 **aes128**。
- 客户端到服务器端的首选 HMAC 算法，缺省算法为 **sha1-96**。
- 密钥交换首选算法，缺省算法为 **dh-group14**。
- 服务器端到客户端的首选加密算法，缺省算法为 **aes128**。
- 服务器端到客户端的首选 HMAC 算法，缺省算法为 **sha1-96**。

【举例】

与 IP 地址为 192.168.0.1 的远程 SCP 服务器建立连接，并下载远端的 **remote.bin** 文件，下载到本地后更名为 **local.bin**。

```
<Sysname> scp 192.168.0.1 get remote.bin local.bin
```

1.2.21 sftp

【命令】

在非 FIPS 模式下：


```
sftp server [ port-number ] [ identity-key { dsa | rsa } | prefer-compress { zlib | zlib-openssh } | prefer-ctos-cipher { 3des | aes128 | des } | prefer-ctos-hmac { md5 | md5-96 | sha1 | sha1-96 } | prefer-kex { dh-group-exchange | dh-group1 | dh-group14 } | prefer-stoc-cipher { 3des | aes128 | des } | prefer-stoc-hmac { md5 | md5-96 | sha1 | sha1-96 } ] *
```

在 FIPS 模式下：

```
sftp server [ port-number ] [ identity-key rsa | prefer-ctos-cipher { aes128 | aes256 } | prefer-ctos-hmac { sha1 | sha1-96 } | prefer-kex dh-group14 | prefer-stoc-cipher { aes128 | aes256 } | prefer-stoc-hmac { sha1 | sha1-96 } ] *
```

【视图】

用户视图

【缺省级别】

3: 管理级

【参数】

server: 服务器 IPv4 地址或主机名称，为 1~20 个字符的字符串，不区分大小写。

port-number: 服务器端口号，取值范围为 0~65535，缺省值为 22。

identity-key: publickey 认证采用的公钥算法，在非 FIPS 模式下，可以选择 DSA 或 RSA 任意一种；在 FIPS 模式下只支持 RSA 算法。

- **dsa**: 公钥算法为 DSA。
- **rsa**: 公钥算法为 RSA。

prefer-compress: 首选压缩算法，缺省为无压缩。

- **zlib**: ZLIB 压缩算法。
- **zlib-openssh**: ZLIB@openssh.com 压缩算法。

prefer-ctos-cipher: 客户端到服务器端的首选加密算法，缺省算法为 **aes128**。

- **3des**: 3des-cbc 加密算法，FIPS 模式下不支持该参数。
- **aes128**: aes128-cbc 加密算法。
- **aes256**: aes256-cbc 加密算法，非 FIPS 模式下不支持该参数。
- **des**: des-cbc 加密算法，FIPS 模式下不支持该参数。

prefer-ctos-hmac: 客户端到服务器端的首选 HMAC 算法，缺省算法为 **sha1-96**。

- **md5**: HMAC 算法 hmac-md5，FIPS 模式下不支持该参数。
- **md5-96**: HMAC 算法 hmac-md5-96，FIPS 模式下不支持该参数。
- **sha1**: HMAC 算法 hmac-sha1。
- **sha1-96**: HMAC 算法 hmac-sha1-96。

prefer-kex: 密钥交换首选算法，在非 FIPS 模式下，缺省算法为 **dh-group-exchange**；在 FIPS 模式下缺省算法为 **dh-group14**。

- **dh-group-exchange**: 密钥交换算法 diffie-hellman-group-exchange-sha1，FIPS 模式下不支持该参数。
- **dh-group1**: 密钥交换算法 diffie-hellman-group1-sha1，FIPS 模式下不支持该参数。
- **dh-group14**: 密钥交换算法 diffie-hellman-group14-sha1。

prefer-stoc-cipher: 服务器端到客户端的首选加密算法，缺省算法为 **aes128**。

prefer-stoc-hmac: 服务器端到客户端的首选 HMAC 算法，缺省算法为 **sha1-96**。

【描述】

sftp 命令用来与远程 IPv4 SFTP 服务器建立连接，并进入 SFTP 客户端视图。

需要注意的是，当服务器端指定客户端的认证方式为 **publickey** 认证时，客户端需要读取本地的私钥进行验证。在非 FIPS 模式下，由于 **publickey** 认证可以采用 RSA 和 DSA 两种公钥算法，所以需要 **identity-key** 关键字指定采用的加密算法，才能得到正确的本地私钥数据。

在非 FIPS 模式下，缺省的算法如下：

- 公钥缺省算法为 **dsa**。
- 客户端到服务器端的首选加密算法，缺省算法为 **aes128**。
- 客户端到服务器端的首选 HMAC 算法，缺省算法为 **sha1-96**。
- 密钥交换首选算法，缺省算法为 **dh-group-exchange**。
- 服务器端到客户端的首选加密算法，缺省算法为 **aes128**。
- 服务器端到客户端的首选 HMAC 算法，缺省算法为 **sha1-96**。

在 FIPS 模式下，缺省的算法如下：

- 公钥缺省算法为 **rsa**。
- 客户端到服务器端的首选加密算法，缺省算法为 **aes128**。
- 客户端到服务器端的首选 HMAC 算法，缺省算法为 **sha1-96**。
- 密钥交换首选算法，缺省算法为 **dh-group14**。
- 服务器端到客户端的首选加密算法，缺省算法为 **aes128**。
- 服务器端到客户端的首选 HMAC 算法，缺省算法为 **sha1-96**。

【举例】

连接 IP 地址为 10.1.1.2 的 SFTP 服务器，采用如下连接策略：

- 首选密钥交换算法为 **dh-group1**；
- 服务器到客户端的首选加密算法为 **aes128**；
- 客户端到服务器的首选 HMAC 算法为 **md5**；
- 服务器到客户端的 HMAC 算法为 **sha1-96**。

```
<Sysname> sftp 10.1.1.2 prefer-kex dh-group1 prefer-stoc-cipher aes128 prefer-ctos-hmac md5 prefer-stoc-hmac sha1-96
```

```
Input Username:
```

1.2.22 sftp client ipv6 source

【命令】

```
sftp client ipv6 source { interface interface-type interface-number | ipv6 ipv6-address }
```

```
undo sftp client ipv6 source
```

【视图】

系统视图

【缺省级别】

3: 管理级

【参数】

interface interface-type interface-number: 源接口类型与源接口编号。

ipv6 ipv6-address: 源 IPv6 地址。

【描述】

sftp client ipv6 source 命令用来为 SFTP 客户端指定源 IPv6 地址或源接口。**undo sftp client ipv6 source** 命令用来取消指定的源 IPv6 地址或源接口。

缺省情况下，客户端用设备路由指定的接口地址访问 SFTP 服务器。

为保证 SFTP 客户端与 SFTP 服务器通信链路的可达性，以及增加认证业务对 SFTP 客户端的可管理性，通常建议指定 Loopback 接口或 Dialer 接口作为源接口。

相关配置可参考命令 **display sftp client source**。

【举例】

指定 SFTP 客户端的源 IPv6 地址为 2:2::2:2。

```
<Sysname> system-view
[Sysname] sftp client ipv6 source ipv6 2:2::2:2
```

1.2.23 sftp client source

【命令】

sftp client source { interface interface-type interface-number | ip ip-address }

undo sftp client source

【视图】

系统视图

【缺省级别】

3: 管理级

【参数】

interface interface-type interface-number: 源接口类型与源接口编号。

ip ip-address: 源 IPv4 地址。

【描述】

sftp client source 命令用来为 SFTP 客户端指定源 IPv4 地址或源接口。**undo sftp client source** 命令用来取消指定的源 IPv4 地址或源接口。

缺省情况下，客户端用设备路由指定的接口地址访问 SFTP 服务器。

为保证 SFTP 客户端与 SFTP 服务器通信链路的可达性，以及增加认证业务对 SFTP 客户端的可管理性，通常建议指定 Loopback 接口或 Dialer 接口作为源接口。

相关配置可参考命令 **display sftp client source**。

【举例】

指定 SFTP 客户端的源 IP 地址为 192.168.0.1。

```
<Sysname> system-view
[Sysname] sftp client source ip 192.168.0.1
```

1.2.24 sftp ipv6

【命令】

在非 FIPS 模式下：

```
sftp ipv6 server [ port-number ] [ identity-key { dsa | rsa } | prefer-compress { zlib | zlib-openssh } | prefer-ctos-cipher { 3des | aes128 | des } | prefer-ctos-hmac { md5 | md5-96 | sha1 | sha1-96 } | prefer-kex { dh-group-exchange | dh-group1 | dh-group14 } | prefer-stoc-cipher { 3des | aes128 | des } | prefer-stoc-hmac { md5 | md5-96 | sha1 | sha1-96 } ] *
```

在 FIPS 模式下：

```
sftp ipv6 server [ port-number ] [ identity-key rsa | prefer-ctos-cipher { aes128 | aes256 } | prefer-ctos-hmac { sha1 | sha1-96 } | prefer-kex dh-group14 | prefer-stoc-cipher { aes128 | aes256 } | prefer-stoc-hmac { sha1 | sha1-96 } ] *
```

【视图】

用户视图

【缺省级别】

3: 管理级

【参数】

server: 服务器的 IPv6 地址或主机名称，为 1~46 个字符的字符串，不区分大小写。

port-number: 服务器的端口号，取值范围为 0~65535，缺省值为 22。

identity-key: publickey 认证采用的公钥算法，在非 FIPS 模式下，可以选择 DSA 或 RSA 任意一种；在 FIPS 模式下只支持 RSA 算法。

- **dsa**: 公钥算法为 DSA。
- **rsa**: 公钥算法为 RSA。

prefer-compress: 首选压缩算法，缺省为无压缩。

- **zlib**: ZLIB 压缩算法。
- **zlib-openssh**: ZLIB@openssh.com 压缩算法。

prefer-ctos-cipher: 客户端到服务器端的首选加密算法，缺省算法为 **aes128**。

- **3des**: 3des-cbc 加密算法，FIPS 模式下不支持该参数。
- **aes128**: aes128-cbc 加密算法。
- **aes256**: aes256-cbc 加密算法，非 FIPS 模式下不支持该参数。
- **des**: des-cbc 加密算法，FIPS 模式下不支持该参数。

prefer-ctos-hmac: 客户端到服务器端的首选 HMAC 算法，缺省算法为 **sha1-96**。

- **md5**: HMAC 算法 hmac-md5，FIPS 模式下不支持该参数。
- **md5-96**: HMAC 算法 hmac-md5-96，FIPS 模式下不支持该参数。
- **sha1**: HMAC 算法 hmac-sha1。
- **sha1-96**: HMAC 算法 hmac-sha1-96。

prefer-kex: 密钥交换首选算法, 在非 FIPS 模式下, 缺省算法为 **dh-group-exchange**; 在 FIPS 模式下缺省算法为 **dh-group14**。

- **dh-group-exchange**: 密钥交换算法 diffie-hellman-group-exchange-sha1, FIPS 模式下不支持该参数。
- **dh-group1**: 密钥交换算法 diffie-hellman-group1-sha1, FIPS 模式下不支持该参数。
- **dh-group14**: 密钥交换算法 diffie-hellman-group14-sha1。

prefer-stoc-cipher: 服务器端到客户端的首选加密算法, 缺省算法为 **aes128**。

prefer-stoc-hmac: 服务器端到客户端的首选 HMAC 算法, 缺省算法为 **sha1-96**。

【描述】

sftp ipv6 命令用来与远程 IPv6 SFTP 服务器建立连接, 并进入 SFTP 客户端视图。

需要注意的是, 当服务器端指定客户端的认证方式为 **publickey** 认证时, 客户端需要读取本地的私钥进行验证。在非 FIPS 模式下, 由于 **publickey** 认证可以采用 RSA 和 DSA 两种公钥算法, 所以需要 **identity-key** 关键字指定采用的加密算法, 才能得到正确的本地私钥数据。

在非 FIPS 模式下, 缺省的算法如下:

- 公钥缺省算法为 **dsa**。
- 客户端到服务器端的首选加密算法, 缺省算法为 **aes128**。
- 客户端到服务器端的首选 HMAC 算法, 缺省算法为 **sha1-96**。
- 密钥交换首选算法, 缺省算法为 **dh-group-exchange**。
- 服务器端到客户端的首选加密算法, 缺省算法为 **aes128**。
- 服务器端到客户端的首选 HMAC 算法, 缺省算法为 **sha1-96**。

在 FIPS 模式下, 缺省的算法如下:

- 公钥缺省算法为 **rsa**。
- 客户端到服务器端的首选加密算法, 缺省算法为 **aes128**。
- 客户端到服务器端的首选 HMAC 算法, 缺省算法为 **sha1-96**。
- 密钥交换首选算法, 缺省算法为 **dh-group14**。
- 服务器端到客户端的首选加密算法, 缺省算法为 **aes128**。
- 服务器端到客户端的首选 HMAC 算法, 缺省算法为 **sha1-96**。

【举例】

连接 IPv6 地址为 2:5::8:9 的 SFTP 服务器, 采用如下连接策略:

- 首选密钥交换算法为 **dh-group1**;
- 服务器到客户端的首选加密算法为 **aes128**;
- 客户端到服务器的首选 HMAC 算法为 **md5**;
- 服务器到客户端的 HMAC 算法为 **sha1-96**。

```
<Sysname> sftp ipv6 2:5::8:9 prefer-kex dh-group1 prefer-stoc-cipher aes128
prefer-ctos-hmac md5 prefer-stoc-hmac sha1-96
Input Username:
```

1.2.25 ssh client authentication server

【命令】

```
ssh client authentication server server assign publickey keyname  
undo ssh client authentication server server assign publickey
```

【视图】

系统视图

【缺省级别】

2: 系统级

【参数】

server: 服务器的 IP 地址或名称，为 1~80 个字符的字符串。

assign publickey keyname: 指定服务器端的主机公钥。**keyname** 表示主机公钥名称，为 1~64 个字符的字符串。

【描述】

ssh client authentication server 命令用来在客户端上指定要连接的服务器端的主机公钥名称，以便客户端判断认证连接的服务器是否为可信赖的服务器。**undo ssh client authentication server** 命令用来取消在客户端上指定要连接的服务器端的主机公钥。

缺省情况下，客户端不指定要连接的服务器端的主机公钥名称，而是在客户端登录服务器的时候使用登录服务器时所用的 IP 地址或主机名作其对应的公钥名称。

如果客户端不支持首次认证，客户端将拒绝访问未经认证的服务器。此时，需要在客户端配置服务器端的公钥，并指定该公钥与服务器端的对应关系，以便在客户端对连接的服务器端进行认证时，能够根据该对应关系使用正确的公钥对服务器端进行认证。

需要注意的是，指定的服务器端的主机公钥必须已经存在。

相关配置可参考命令 **ssh client first-time enable**。

【举例】

```
# 服务器的 IP 地址为 192.168.0.1，在客户端指定该服务器的公钥名称为 key1。  
<Sysname> system-view  
[Sysname] ssh client authentication server 192.168.0.1 assign publickey key1
```

1.2.26 ssh client first-time enable

【命令】

```
ssh client first-time enable  
undo ssh client first-time
```

【视图】

系统视图

【缺省级别】

2: 系统级

【参数】

无

【描述】

ssh client first-time enable 命令用来设置 SSH 客户端支持首次认证。**undo ssh client first-time** 命令用来取消 SSH 客户端对首次认证的支持。

缺省情况下，SSH 客户端支持首次认证。

所谓支持首次认证，是指当 SSH 客户端首次访问服务器，而客户端没有配置服务器端的公钥时，用户可以选择继续访问该服务器，并在客户端保存该主机公钥；当用户下次访问该服务器时，就以保存的主机公钥来认证该服务器。

如果不支持首次认证，则当客户端没有配置服务器端的公钥时，客户端将被拒绝访问该服务器。用户必须事先通过其它途径将要访问的服务器端的主机公钥配置在本地，同时指定要连接的服务器端的主机公钥名称，以便客户端认证连接的服务器是否为可信赖的服务器。

需要注意的是，由于服务器端可能会定期更新密钥对，为保证服务器认证成功，客户端需要及时获取最新的服务器主机公钥。

【举例】

设置 SSH 客户端支持首次认证。

```
<Sysname> system-view  
[Sysname] ssh client first-time enable
```

1.2.27 ssh client ipv6 source

【命令】

ssh client ipv6 source { interface *interface-type interface-number* | ipv6 *ipv6-address* }
undo ssh client ipv6 source

【视图】

系统视图

【缺省级别】

3: 管理级

【参数】

interface *interface-type interface-number*: 源接口类型与源接口编号。

ipv6 *ipv6-address*: 源 IPv6 地址。

【描述】

ssh client ipv6 source 命令用来为 Stelnet 客户端指定源 IPv6 地址或源接口。**undo ssh client ipv6 source** 命令用来清除指定的源 IPv6 地址或源接口。

缺省情况下，客户端用设备路由指定的接口地址访问 Stelnet 服务器。

为保证 Stelnet 客户端与 Stelnet 服务器通信链路的可达性，以及增加认证业务对 Stelnet 客户端的可管理性，通常建议指定 Loopback 接口或 Dialer 接口作为源接口。

相关配置可参考命令 **display ssh client source**。

【举例】

```
# 指定 Stelnet 客户端的源 IPv6 地址为 2:2::2:2。
<Sysname> system-view
[Sysname] ssh client ipv6 source ipv6 2:2::2:2
```

1.2.28 ssh client source

【命令】

```
ssh client source { interface interface-type interface-number | ip ip-address }
undo ssh client source
```

【视图】

系统视图

【缺省级别】

3: 管理级

【参数】

interface *interface-type interface-number*: 源接口类型与源接口编号。
ip *ip-address*: 源 IPv4 地址。

【描述】

ssh client source 命令用来为 Stelnet 客户端指定源 IPv4 地址或源接口。**undo ssh client source** 命令用来清除指定的源 IPv4 地址或源接口。

缺省情况下，客户端用设备路由指定的接口地址访问 Stelnet 服务器。

为保证 Stelnet 客户端与 Stelnet 服务器通信链路的可达性，以及增加认证业务对 Stelnet 客户端的可管理性，通常建议指定 Loopback 接口或 Dailer 接口作为源接口。

相关配置可参考命令 **display ssh client source**。

【举例】

```
# 指定 Stelnet 客户端的源 IPv4 地址为 192.168.0.1。
<Sysname> system-view
[Sysname] ssh client source ip 192.168.0.1
```

1.2.29 ssh2

【命令】

在非 FIPS 模式下：

```
ssh2 server [ port-number ] [ identity-key { dsa | rsa } | prefer-compress { zlib | zlib-openssh } | prefer-ctos-cipher { 3des | aes128 | des } | prefer-ctos-hmac { md5 | md5-96 | sha1 | sha1-96 } | prefer-kex { dh-group-exchange | dh-group1 | dh-group14 } | prefer-stoc-cipher { 3des | aes128 | des } | prefer-stoc-hmac { md5 | md5-96 | sha1 | sha1-96 } ] *
```

在 FIPS 模式下：

```
ssh2 server [ port-number ] [ vpn-instance vpn-instance-name ] [ identity-key rsa | prefer-ctos-cipher { aes128 | aes256 } | prefer-ctos-hmac { sha1 | sha1-96 } | prefer-kex
```


dh-group14 | prefer-stoc-cipher { aes128 | aes256 } | prefer-stoc-hmac { sha1 | sha1-96 } }
*

【视图】

用户视图

【缺省级别】

0: 访问级

【参数】

server: 服务器 IPv4 地址或主机名称，为 1~20 个字符的字符串，不区分大小写。

port-number: 服务器端口号，取值范围为 0~65535，缺省值为 22。

identity-key: publickey 认证采用的公钥算法，在非 FIPS 模式下，可以选择 DSA 或 RSA 任意一种；在 FIPS 模式下只支持 RSA 算法。

- **dsa:** 公钥算法为 DSA。
- **rsa:** 公钥算法为 RSA。

prefer-compress: 首选压缩算法，缺省为无压缩。

- **zlib:** ZLIB 压缩算法。
- **zlib-openssh:** ZLIB@openssh.com 压缩算法。

prefer-ctos-cipher: 客户端到服务器端的首选加密算法，缺省算法为 **aes128**。

- **3des:** 3des-cbc 加密算法，FIPS 模式下不支持该参数。
- **aes128:** aes128-cbc 加密算法。
- **aes256:** aes256-cbc 加密算法，非 FIPS 模式下不支持该参数。
- **des:** des-cbc 加密算法，FIPS 模式下不支持该参数。

prefer-ctos-hmac: 客户端到服务器端的首选 HMAC 算法，缺省算法为 **sha1-96**。

- **md5:** HMAC 算法 hmac-md5，FIPS 模式下不支持该参数。
- **md5-96:** HMAC 算法 hmac-md5-96，FIPS 模式下不支持该参数。
- **sha1:** HMAC 算法 hmac-sha1。
- **sha1-96:** HMAC 算法 hmac-sha1-96。

prefer-kex: 密钥交换首选算法，在非 FIPS 模式下，缺省算法为 **dh-group-exchange**；在 FIPS 模式下缺省算法为 **dh-group14**。

- **dh-group-exchange:** 密钥交换算法 diffie-hellman-group-exchange-sha1，FIPS 模式下不支持该参数。
- **dh-group1:** 密钥交换算法 diffie-hellman-group1-sha1，FIPS 模式下不支持该参数。
- **dh-group14:** 密钥交换算法 diffie-hellman-group14-sha1。

prefer-stoc-cipher: 服务器端到客户端的首选加密算法，缺省算法为 **aes128**。

prefer-stoc-hmac: 服务器端到客户端的首选 HMAC 算法，缺省算法为 **sha1-96**。

【描述】

ssh2 命令用来建立 Stelnet 客户端和 IPv4 Stelnet 服务器端的连接，并指定公钥算法、客户端和服务器的首选加密算法、首选 HMAC 算法和首选密钥交换算法。

需要注意的是，当服务器端对客户端的认证方式为 `publickey` 认证时，客户端需要读取本地的私钥进行数字签名。在 FIPS 模式下，由于 `publickey` 认证可以采用 RSA 和 DSA 两种公钥算法，所以需要通过 `identity-key` 关键字指定客户端采用的公钥算法，才能得到正确的本地私钥数据。

在非 FIPS 模式下，缺省的算法如下：

- 公钥缺省算法为 `dsa`。
- 客户端到服务器端的首选加密算法，缺省算法为 `aes128`。
- 客户端到服务器端的首选 HMAC 算法，缺省算法为 `sha1-96`。
- 密钥交换首选算法，缺省算法为 `dh-group-exchange`。
- 服务器端到客户端的首选加密算法，缺省算法为 `aes128`。
- 服务器端到客户端的首选 HMAC 算法，缺省算法为 `sha1-96`。

在 FIPS 模式下，缺省的算法如下：

- 公钥缺省算法为 `rsa`。
- 客户端到服务器端的首选加密算法，缺省算法为 `aes128`。
- 客户端到服务器端的首选 HMAC 算法，缺省算法为 `sha1-96`。
- 密钥交换首选算法，缺省算法为 `dh-group14`。
- 服务器端到客户端的首选加密算法，缺省算法为 `aes128`。
- 服务器端到客户端的首选 HMAC 算法，缺省算法为 `sha1-96`。

【举例】

登录地址为 10.214.50.51 的远程 Stelnet 服务器，采用如下连接策略：

- 首选密钥交换算法为 `dh-group1`；
- 服务器到客户端的首选加密算法为 `aes128`；
- 客户端到服务器的首选 HMAC 算法为 `md5`；
- 服务器到客户端的 HMAC 算法为 `sha1-96`。

```
<Sysname> ssh2 10.214.50.51 prefer-kex dh-group1 prefer-stoc-cipher aes128  
prefer-ctos-hmac md5 prefer-stoc-hmac sha1-96
```

1.2.30 ssh2 ipv6

【命令】

在非 FIPS 模式下：

```
ssh2 ipv6 server [ port-number ] [ identity-key { dsa | rsa } | prefer-compress { zlib |  
zlib-openssh } | prefer-ctos-cipher { 3des | aes128 | des } | prefer-ctos-hmac { md5 |  
md5-96 | sha1 | sha1-96 } | prefer-kex { dh-group-exchange | dh-group1 | dh-group14 } |  
prefer-stoc-cipher { 3des | aes128 | des } | prefer-stoc-hmac { md5 | md5-96 | sha1 |  
sha1-96 } ] *
```

在 FIPS 模式下：

```
ssh2 ipv6 server [ port-number ] [ identity-key rsa | prefer-ctos-cipher { aes128 | aes256 } |  
prefer-ctos-hmac { sha1 | sha1-96 } | prefer-kex dh-group14 | prefer-stoc-cipher { aes128  
| aes256 } | prefer-stoc-hmac { sha1 | sha1-96 } ] *
```

【视图】

用户视图

【缺省级别】

0: 访问级

【参数】

server: 服务器的 IPv6 地址或主机名称, 为 1~46 个字符的字符串, 不区分大小写。

port-number: 服务器的端口号, 取值范围为 0~65535, 缺省值为 22。

identity-key: **publickey** 认证采用的公钥算法, 在非 FIPS 模式下, 可以选择 DSA 或 RSA 任意一种; 在 FIPS 模式下只支持 RSA 算法。

- **dsa**: 公钥算法为 DSA。
- **rsa**: 公钥算法为 RSA。

prefer-compress: 首选压缩算法, 缺省为无压缩。

- **zlib**: ZLIB 压缩算法。
- **zlib-openssh**: ZLIB@openssh.com 压缩算法。

prefer-ctos-cipher: 客户端到服务器端的首选加密算法, 缺省算法为 **aes128**。

- **3des**: 3des-cbc 加密算法, FIPS 模式下不支持该参数。
- **aes128**: aes128-cbc 加密算法。
- **aes256**: aes256-cbc 加密算法, 非 FIPS 模式下不支持该参数。
- **des**: des-cbc 加密算法, FIPS 模式下不支持该参数。

prefer-ctos-hmac: 客户端到服务器端的首选 HMAC 算法, 缺省算法为 **sha1-96**。

- **md5**: HMAC 算法 hmac-md5, FIPS 模式下不支持该参数。
- **md5-96**: HMAC 算法 hmac-md5-96, FIPS 模式下不支持该参数。
- **sha1**: HMAC 算法 hmac-sha1。
- **sha1-96**: HMAC 算法 hmac-sha1-96。
- **prefer-kex**: 密钥交换首选算法, 在非 FIPS 模式下, 缺省算法为 **dh-group-exchange**; 在 FIPS 模式下缺省算法为 **dh-group14**。
- **dh-group-exchange**: 密钥交换算法 diffie-hellman-group-exchange-sha1, FIPS 模式下不支持该参数。
- **dh-group1**: 密钥交换算法 diffie-hellman-group1-sha1, FIPS 模式下不支持该参数。
- **dh-group14**: 密钥交换算法 diffie-hellman-group14-sha1。

prefer-stoc-cipher: 服务器端到客户端的首选加密算法, 缺省算法为 **aes128**。

prefer-stoc-hmac: 服务器端到客户端的首选 HMAC 算法, 缺省算法为 **sha1-96**

【描述】

ssh2 ipv6 命令用来建立 Stelnet 客户端和 IPv6 Stelnet 服务器端的连接, 并指定公钥算法、客户端和服务器的首选加密算法、首选 HMAC 算法和首选密钥交换算法。

需要注意的是, 当服务器端对客户端的认证方式为 **publickey** 认证时, 客户端需要读取本地的私钥进行数字签名。在非 FIPS 模式下, 由于 **publickey** 认证可以采用 RSA 和 DSA 两种公钥算法, 所以需要通过 **identity-key** 关键字指定客户端采用的加密算法, 才能得到正确的本地私钥数据。

在非 FIPS 模式下，缺省的算法如下：

- 公钥缺省算法为 **dsa**。
- 客户端到服务器端的首选加密算法，缺省算法为 **aes128**。
- 客户端到服务器端的首选 HMAC 算法，缺省算法为 **sha1-96**。
- 密钥交换首选算法，缺省算法为 **dh-group-exchange**。
- 服务器端到客户端的首选加密算法，缺省算法为 **aes128**。
- 服务器端到客户端的首选 HMAC 算法，缺省算法为 **sha1-96**。

在 FIPS 模式下，缺省的算法如下：

- 公钥缺省算法为 **rsa**。
- 客户端到服务器端的首选加密算法，缺省算法为 **aes128**。
- 客户端到服务器端的首选 HMAC 算法，缺省算法为 **sha1-96**。
- 密钥交换首选算法，缺省算法为 **dh-group14**。
- 服务器端到客户端的首选加密算法，缺省算法为 **aes128**。
- 服务器端到客户端的首选 HMAC 算法，缺省算法为 **sha1-96**。

【举例】

登录地址为 2000::1 的远程 Stelnet 服务器，采用如下连接策略：

- 首选密钥交换算法为 **dh-group1**；
- 服务器到客户端的首选加密算法为 **aes128**；
- 客户端到服务器的首选 HMAC 算法为 **md5**；
- 服务器到客户端的 HMAC 算法为 **sha1-96**。

```
<Sysname> ssh2 ipv6 2000::1 prefer-kex dh-group1 prefer-stoc-cipher aes128  
prefer-ctos-hmac md5 prefer-stoc-hmac sha1-96
```