

目 录

1 登录设备命令	1-1
1.1 登录设备命令	1-1
1.1.1 acl (User interface view)	1-1
1.1.2 activation-key	1-2
1.1.3 auto-execute command	1-3
1.1.4 authentication-mode	1-4
1.1.5 command accounting	1-5
1.1.6 command authorization	1-6
1.1.7 databits	1-6
1.1.8 display ip http	1-7
1.1.9 display ip https	1-8
1.1.10 display user-interface	1-9
1.1.11 display users	1-11
1.1.12 escape-key	1-12
1.1.13 flow-control	1-13
1.1.14 free user-interface	1-14
1.1.15 history-command max-size	1-15
1.1.16 idle-timeout	1-16
1.1.17 ip http acl	1-16
1.1.18 ip http enable	1-17
1.1.19 ip http port	1-18
1.1.20 ip https acl	1-18
1.1.21 ip https certificate access-control-policy	1-19
1.1.22 ip https enable	1-20
1.1.23 ip https port	1-20
1.1.24 ip https ssl-server-policy	1-21
1.1.25 lock	1-21
1.1.26 parity	1-22
1.1.27 protocol inbound	1-23
1.1.28 redirect disconnect	1-24
1.1.29 redirect enable	1-24
1.1.30 redirect listen-port	1-25
1.1.31 redirect refuse-negotiation	1-26
1.1.32 redirect refuse-teltransfer	1-26
1.1.33 redirect return-deal from-telnet	1-27
1.1.34 redirect return-deal from-terminal	1-28
1.1.35 redirect timeout	1-28

1.1.36 screen-length.....	1-29
1.1.37 send.....	1-29
1.1.38 set authentication password.....	1-31
1.1.39 shell	1-32
1.1.40 speed (User interface view).....	1-32
1.1.41 stopbit-error intolerance	1-33
1.1.42 stopbits	1-34
1.1.43 telnet.....	1-34
1.1.44 telnet client source	1-35
1.1.45 telnet ipv6	1-35
1.1.46 telnet server enable.....	1-36
1.1.47 terminal type.....	1-36
1.1.48 user privilege level.....	1-37
1.1.49 user-interface.....	1-38

1 登录设备命令

1.1 登录设备命令

1.1.1 acl (User interface view)

【命令】

基本/高级 ACL 支持:

```
acl [ ipv6 ] acl-number { inbound | outbound }  
undo acl [ ipv6 ] acl-number { inbound | outbound }
```

WLAN/二层 ACL 支持:

```
acl acl-number inbound  
undo acl acl-number inbound
```

【视图】

VTY 用户界面视图

【缺省级别】

2: 系统级

【参数】

ipv6: 支持 IPv6 协议, 不带该参数表示支持 IPv4 协议。

acl-number: 访问控制列表号, 取值范围如下:

100~199: WLAN ACL 编号;

- 2000~2999: 基本 ACL 编号;
- 4000~4999: 二层 ACL 编号。

inbound: 表示对使用该用户界面建立的 Telnet 或者 SSH 连接进行限制, 当设备收到的 Telnet 或者 SSH 连接报文符合 ACL 规则时, 才允许建立连接。当设备作为 Telnet server 或 SSH server 时, 通常使用该参数对 Telnet client 或 SSH client 进行限制。

outbound: 表示对使用该用户界面建立的 Telnet 连接进行限制, 当设备发送的 Telnet 连接报文符合 ACL 规则时, 才允许建立连接。当设备作为 Telnet client 时, 通常使用该参数对可以访问的 Telnet server 进行限制。

【描述】

acl 命令用来引用访问控制列表 (ACL), 对当前用户界面的使用权限进行限制。**undo acl** 命令用来取消指定 ACL 对用户界面的使用权限的限制。(ACL 的相关内容可参考“ACL 和 QoS 配置指导”中的“ACL”。)

缺省情况下, 系统不对用户界面的使用权限进行限制。

- 如果 VTY 用户界面下没有配置 ACL, 则使用该用户界面建立 Telnet 或者 SSH 连接时不进行限制;
- 如果 VTY 用户界面下配置了 ACL, 则只有匹配上 **permit** 规则的允许建立连接。

需要注意的是, 系统将带 **inbound** 参数的基本/高级 ACL、带 **outbound** 参数的基本/高级 ACL、WLAN ACL、二层 ACL 看成是四种不同类型的 ACL, 在同一个 VTY 用户界面下, 不同类型的 ACL 可以共存, 如果同时配置了不同类型的 ACL, 则匹配的顺序由先到后为 WLAN ACL、基本/高级 ACL、二层 ACL; 相同类型的 ACL 只能配置一条, 以最新的配置为准。

【举例】

当使用 Telnet 或者 SSH 方式访问设备时，只允许 IP 地址为 192.168.1.26 的用户访问，不允许其它 IP 地址的用户使用该界面进行访问。

```
<Sysname> system-view
[Sysname] acl number 2001
[Sysname-acl-basic-2001] rule permit source 192.168.1.26 0
[Sysname-acl-basic-2001] quit
[Sysname] user-interface vty 0
[Sysname-ui-vty0] acl 2001 inbound
```

当 UserA (IP 地址为 192.168.1.26) Telnet 到设备时，可以连接成功；当 UserB (IP 地址为 192.168.1.60) Telnet 到设备时，连接建立失败，系统提示“%connection closed by remote host!”。

仅允许 SSID 为 Admin 的无线用户使用用户界面 VTY 0 访问设备。

```
<Sysname> system-view
[Sysname] acl number 100
[Sysname-acl-wlan-100] rule permit ssid Admin
[Sysname-acl-wlan-100] quit
[Sysname] user-interface vty 0
[Sysname-ui-vty0] acl 100 inbound
```

1.1.2 activation-key

【命令】

activation-key *character*

undo activation-key

【视图】

用户界面视图

【缺省级别】

3: 管理级

【参数】

character: 定义启动终端会话的快捷键，可以是字符或者字符对应的 ASCII 码值 (0~127)。如果输入 1~3 个字符的字符串，则只有第一个字符生效。比如，设置时使用的参数是 ASCII 码值 97，系统会将快捷键设置成 <a>；如果设置时使用的参数是字符串 b@c，系统会将快捷键设置成 。

【描述】

activation-key 命令用来配置启动终端会话的快捷键。**undo activation-key** 命令用来恢复缺省情况。

缺省情况下，按 <Enter> 键启动终端会话。

如果使用 **activation-key** 命令设置了别的快捷键，则新的快捷键将代替 <Enter> 键来启动终端会话，新设置的快捷键可以使用 **display current-configuration | include activation-key** 命令查看。



说明

VTY 用户界面不支持该命令。

【举例】

指定启动 Console 口终端会话的快捷键为 <s>。

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

```
[Sysname] user-interface console 0
[Sysname-ui-console0] activation-key s
```

验证过程如下：

- 退出 console 口终端会话。

```
[Sysname-ui-console0] return
<Sysname> quit
```

- 重新使用 Console 口登录设备，能看到如下显示信息。

```
*****
* Copyright (c) 2004-2009 Hangzhou H3C Tech. Co., Ltd. All rights reserved. *
* Without the owner's prior written consent, *
* no decompiling or reverse-engineering shall be allowed. *
*****
```

```
User interface con0 is available.
```

```
Please press ENTER.
```

- 此时，<ENTER>键失效，需要按<s>键才能出现用户视图提示符，启动 Console 口终端会话。

```
<Sysname>
%Mar 2 18:40:27:981 2005 Sysname SHELL/5/LOGIN: Console login from con0
```

1.1.3 auto-execute command

【命令】

auto-execute command *command*

undo auto-execute command

【视图】

用户界面视图

【缺省级别】

3: 管理级

【参数】

command: 需要自动执行的某条命令。

【描述】

auto-execute command 命令用来设置自动执行命令。**undo auto-execute command** 命令用来取消自动执行命令。

缺省情况下，未设定自动执行命令。

- Console 口不支持 **auto-execute command**。
- 如果设备上只有一个 AUX 口，没有 Console 口（Console 口和 AUX 口共用），则此 AUX 口也不支持 **auto-execute command**。
- 对其他类型的接口，该命令不作限制。

用户在登录时自动执行用 **auto-execute command** 配置好的命令，执行完命令后，自动断开用户连接。如果这条命令引发起了一个任务，系统会等这个任务执行完毕后再断开连接。

该命令通常的用法是 **auto-execute command telnet**，使用户登录时能自动连接到指定的主机。



注意

- 在配置 **auto-execute command** 命令之前，要确保可以通过其他方式登录系统，以便出现问题后，能删除该配置。
- 执行 **auto-execute command** 命令后，可能导致用户不能通过该终端线对本系统进行配置，需谨慎使用。

【举例】

配置用户从 VTY0 登录后，自动 Telnet 到 IP 地址为 192.168.1.41 的设备。

```
<Sysname> system-view
[Sysname] user-interface vty 0
[Sysname -ui-vty0] auto-execute command telnet 192.168.1.41
% This action will lead to configuration failure through ui-vty0. Are you sure?
[Y/N]:y
[Sysname-ui-vty0]
```

结果验证：

重新 Telnet 登录到设备（IP 地址为 192.168.1.40）时，设备会自动执行 telnet 192.168.1.41 命令，在 Telnet 客户端会看到以下显示信息。

```
C:\> telnet 192.168.1.40
*****
* Copyright (c) 2004-2010 Hangzhou H3C Tech. Co., Ltd. All rights reserved. *
* Without the owner's prior written consent, *
* no decompiling or reverse-engineering shall be allowed. *
*****

<Sysname>
Trying 192.168.1.41 ...
Press CTRL+K to abort
Connected to 192.168.1.41 ...
*****
* Copyright (c) 2004-2010 Hangzhou H3C Tech. Co., Ltd. All rights reserved. *
* Without the owner's prior written consent, *
* no decompiling or reverse-engineering shall be allowed. *
*****

<Sysname.41>
```

此时相当于用户直接登录了 192.168.1.41 设备。如果用户断开与 192.168.1.41 的 Telnet 连接，用户与 192.168.1.40 设备的 Telnet 连接也会同时自动断开。

1.1.4 authentication-mode

【命令】

```
authentication-mode { none | password | scheme }
undo authentication-mode
```

【视图】

用户界面视图

【缺省级别】

3: 管理级

【参数】

none: 设置不进行认证。

password: 指定进行本地密码认证方式。

scheme: 指定进行 AAA 认证方式。AAA 的相关内容请参见“安全配置指导”中的“AAA”。

【描述】

authentication-mode 命令用来设置用户使用当前用户界面登录设备时的认证方式。**undo authentication-mode** 命令用来恢复缺省情况。

使用 VTY、AUX 用户界面登录的用户的认证方式为 **password**，使用 Console、TTY 用户界面登录的用户不需要认证。

相关配置可参考命令 **set authentication password**。

【举例】

设置用户使用 VTY 0 用户界面登录设备时，不需要认证。（注意：该方式存在安全隐患。）

```
<Sysname> system-view
[Sysname] user-interface vty 0
[Sysname-ui-vty0] authentication-mode none
```

设置用户使用 VTY 0 用户界面登录设备时，需要密码认证，认证密码为 321。

```
<Sysname> system-view
[Sysname] user-interface vty 0
[Sysname-ui-vty0] authentication-mode password
[Sysname-ui-vty0] set authentication password cipher 321
```

设置用户使用 VTY 0 用户界面登录设备时，需要用户名和密码认证，用户名为 123，认证密码为 321。

```
<Sysname> system-view
[Sysname] user-interface vty 0
[Sysname-ui-vty0] authentication-mode scheme
[Sysname-ui-vty0] quit
[Sysname] local-user 123
[Sysname-luser-123] password cipher 321
[Sysname-luser-123] service-type telnet
[Sysname-luser-123] authorization-attribute level 3
```

1.1.5 command accounting

【命令】

command accounting

undo command accounting

【视图】

用户界面视图

【缺省级别】

3: 管理级

【参数】

无

【描述】

command accounting 命令用来使能命令行计费功能。**undo command accounting** 命令用来恢复缺省情况。

缺省情况下，没有使能命令行计费功能，即计费服务器不会记录用户执行的命令行。

command accounting 命令执行成功后，如果没有配置命令行授权功能，则当前用户执行的每一条命令都会发送到 HWTACACS 服务器上做记录；如果配置了命令行授权功能，则当前用户执行的并且授权成功的命令都会发送到 HWTACACS 服务器上做记录。

【举例】

设置用户使用 VTY 0 用户界面登录设备时，执行的命令需要在 HWTACACS 服务器上做记录。

```
<Sysname> system-view
[Sysname] user-interface vty 0
[Sysname-ui-vty0] command accounting
```

1.1.6 command authorization

【命令】

command authorization
undo command authorization

【视图】

用户界面视图

【缺省级别】

3: 管理级

【参数】

无

【描述】

command authorization 命令用来使能命令行授权功能。**undo command authorization** 命令用来恢复缺省情况。

缺省情况下，没有使能命令行授权功能，即用户登录后执行命令行不需要服务器授权。

使能命令行授权功能后，使用该用户界面登录的用户只能执行服务器授权的命令，服务器没有授权的命令不能执行。

【举例】

设置用户使用 VTY 0 用户界面登录设备时，需要服务器授权才能执行命令。

```
<Sysname> system-view
[Sysname] user-interface vty 0
[Sysname-ui-vty0] command authorization
```

1.1.7 databits

【命令】

databits { 5 | 6 | 7 | 8 }
undo databits

【视图】

用户界面视图

【缺省级别】

2: 系统级

【参数】

- 5: 数据位为 5 位，即使用 5 个比特来表示一个字符。
- 6: 数据位为 6 位，即使用 6 个比特来表示一个字符。
- 7: 数据位为 7 位，即使用 7 个比特来表示一个字符。
- 8: 数据位为 8 位，即使用 8 个比特来表示一个字符。

【描述】

databits 命令用来设置数据位的个数。**undo databits** 命令用来恢复缺省的数据位。缺省情况下，用户界面的数据位为 8 位。



说明

- 本命令只对异步串口（包括 AUX、Console 口）有效。
 - 访问终端和设备相应用户界面下数据位的设置必须一致，双方才能正常通信。
-

【举例】

```
# 设置数据位为 5 位。  
<Sysname> system-view  
[Sysname] user-interface aux 0  
[Sysname-ui-aux0] databits 5
```

1.1.8 display ip http

【命令】

display ip http [| { **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 ip http 命令用来显示 HTTP 的状态信息。

【举例】

```
# 显示 HTTP 的状态信息。  
<Sysname> display ip http  
HTTP port: 80  
WLAN ACL: 100  
Basic ACL: 2222  
Current connection: 0
```

Operation status: Running

表1-1 display ip http 命令显示信息描述表

字段	描述
HTTP port	HTTP 服务使用的端口号
WLAN ACL	与 HTTP 服务关联的 WLAN 访问控制列表号（该行是否显示请以设备的实际情况为准）
Basic ACL	与 HTTP 服务关联的基本访问控制列表号
Current connection	当前连接数
Operation status	操作状态，取值为： <ul style="list-style-type: none">Running: 表示 HTTP 服务处于开启状态Stopped: 表示 HTTP 服务处于关闭状态

1.1.9 display ip https

【命令】

display ip https [| { **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 ip https 命令用来显示 HTTPS 的状态信息。

【举例】

显示 HTTPS 的状态信息。

```
<Sysname> display ip https
HTTPS port: 443
SSL server policy: test
Certificate access-control-policy:
WLAN ACL: 100
Basic ACL: 2222
Current connection: 0
Operation status: Running
```

表1-2 display ip https 命令显示信息描述表

字段	描述
HTTPS port	HTTPS 服务使用的端口号

字段	描述
SSL server policy	与 HTTPS 服务关联的 SSL 服务器端策略
Certificate access-control-policy	与 HTTPS 服务关联的证书属性访问控制策略
WLAN ACL	与 HTTPS 服务关联的 WLAN 访问控制列表号(该行是否显示请以设备的实际情况为准)
Basic ACL	与 HTTPS 服务关联的基本访问控制列表号
Current connection	当前连接数
Operation status	操作状态，取值为： <ul style="list-style-type: none"> Running: 表示 HTTPS 服务处于开启状态 Stopped: 表示 HTTPS 服务处于关闭状态

1.1.10 display user-interface

【命令】

```
display user-interface [ num1 | { aux | console | tty | vty } num2 ] [ summary ] [ | { begin | exclude | include } regular-expression ]
```

【视图】

任意视图

【缺省级别】

1: 监控级

【参数】

num1: 用户界面的编号（绝对编号方式），不同型号的设备支持的取值范围不同，请以设备的实际情况为准，一般从 0 开始。

num2: 用户界面的编号（相对编号方式），不同型号的设备支持的取值范围不同，请以设备的实际情况为准。

summary: 显示用户界面的摘要信息。

|: 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 user-interface 命令用来显示用户界面的相关信息。

- 不输入关键字 **summary**，将显示用户界面类型、绝对/相对编号、传输速率、从该用户界面登录可以访问的命令级别、认证方式及接入接口。
- 输入关键字 **summary**，将显示正在使用和未使用的用户界面数目和类型。

【举例】

显示用户界面 0 的相关信息。

```
<Sysname> display user-interface 0
  Idx  Type   Tx/Rx   Modem Privi Auth  Int
+ 0    CON 0    9600    -     3     N     -
```

+ : Current user-interface is active.
 F : Current user-interface is active and work in async mode.
 Idx : Absolute index of user-interface.
 Type : Type and relative index of user-interface.
 Privi: The privilege of user-interface.
 Auth : The authentication mode of user-interface.
 Int : The physical location of UIs.
 A : Authentication use AAA.
 L : Authentication use local database.
 N : Current UI need not authentication.
 P : Authentication use current UI's password.

表1-3 display user-interface 命令显示信息描述表

字段	描述
+	表示当前正在使用的用户界面
F	表示当前正在使用的用户界面，且工作在异步方式
Idx	用户界面的绝对编号
Type	用户界面的类型及相对编号
Tx/Rx	用户界面的速率
Modem	Modem 的呼入/呼出开关，取值有 in（允许呼入）、out（允许呼出）、inout（允许呼入呼出）、缺省显示“-”（表示没有配置）
Privi	从该用户界面登录可以访问的命令级别
Auth	使用该用户界面登录的用户的认证方式，取值有 A、L、N 和 P 四种方式
Int	用户界面的物理位置，用用户界面对应的物理接口的简称表示（只有 TTY 用户界面会显示具体的接口信息，Console、AUX 和 VTY 用户界面均显示“-”）
A	表示使用 AAA 认证方式，对应的 authentication-mode 为 scheme
L	表示使用本地认证方式（目前暂时不支持）
N	表示无需认证，对应的 authentication-mode 为 none
P	表示使用当前用户界面的密码进行认证，对应的 authentication-mode 为 password

显示所有用户界面的摘要信息。

```

<Sysname> display user-interface summary
  User interface type : [CON]
    0:X

  User interface type : [TTY]
    1:XXXX XXXX XXXX XXXX
   17:XXXX XXXX XXXX XXXX
   33:XXXX XXXX XXXX XXXX
   49:XXXX XXXX XXXX XXXX
   65:XXXX XXXX XXXX XXXX

  User interface type : [AUX]
    81:X

  User interface type : [VTY]
    82:XUXU U

    3 character mode users.      (U)
   83 UI never used.            (X)
  
```

3 total UI in use

表1-4 display user-interface summary 命令显示信息描述表

字段	描述
User interface type	用户界面类型 (CON/TTY/AUX/VTY)
0:X	0 表示用户界面的绝对编号, X 表示当前没有用户使用该用户界面 (U 表示当前有用户使用该用户界面)。比如 “82:XUXU U” 表示该行第一个用户界面的绝对编号是 82, 没有用户使用; 第 83 号用户界面, 有用户使用; 第 84 号用户界面, 没有用户使用; 第 85、86 号用户界面, 有用户使用
character mode users. (U)	当前配置用户的数量 (即 U 字符的个数)
UI never used. (X)	当前没有被使用的用户界面数 (即 X 字符的个数)
total UI in use.	当前正在被使用的用户界面总数 (即设备当前的用户总数)

1.1.11 display users

【命令】

display users [all] [| { begin | exclude | include } *regular-expression*]

【视图】

任意视图

【缺省级别】

1: 监控级

【参数】

all: 显示设备支持的所有用户界面的相关信息。

|: 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 users 命令用来显示当前正在使用的用户界面的相关信息。

display users all 命令用来显示设备支持的所有用户界面的相关信息。

【举例】

显示当前正在使用的用户界面的相关信息。

```
<Sysname> display users
The user application information of the user interface(s):
  Idx UI      Delay    Type Userlevel
+ 178 VTY 0   00:00:00 TEL    3
  179 VTY 1   00:02:34 TEL    3

Following are more details.
VTY 0   :
        Location: 192.168.1.54
VTY 1   :
```

```

      Location: 192.168.1.58
+   : Current operation user.
F   : Current operation user work in async mode.

```

以上显示信息表明，当前有两个用户已经登录设备，用户自己使用的是 VTY 0 用户界面，用户的 IP 地址为 192.168.1.54；另一个用户使用的是 VTY 1 用户界面，该用户的 IP 地址为 192.168.1.58。

表1-5 display users 命令显示信息描述表

字段	描述
Idx	用户界面的绝对编号
UI	用户界面的相对编号，第一列（比如 VTY）表示用户界面的类型，第二列（比如 0）表示用户界面的相对编号
Delay	表明用户最近一次输入到执行 display users 命令时的时间间隔，格式为 hh:mm:ss
Type	显示用户类型，如 Telnet、SSH、PAD
Userlevel	显示用户的权限，即用户级别（0-VISIT 访问，1-MONITOR 监控，2-SYSTEM 系统，3-MANAGE 管理）
+	当前操作用户
Location	使用该用户界面登录的用户的位置信息（即用户的 IP 地址）
F	当前操作用户工作在异步模式

1.1.12 escape-key

【命令】

```

escape-key { default | character }
undo escape-key

```

【视图】

用户界面视图

【缺省级别】

3: 管理级

【参数】

character: 定义终止当前运行任务的快捷键，可以是字符对应的 ASCII 码值（0~127）或者为 1~3 个字符的字符串，但实际生效的快捷键是参数所标志的第一个字符。比如，设置时使用的参数是 ASCII 码值 113，系统会将快捷键设置成<q>；如果设置时使用的参数是字符串 q@c，系统会将快捷键设置成<q>。

default: 恢复为缺省的快捷键<Ctrl+C>。

【描述】

escape-key 命令用来配置终止当前运行任务（比如 ping 命令、telnet 进程等）的快捷键。**undo escape-key** 命令用来禁止使用该功能，即不能通过快捷键终止当前运行的任务。

缺省情况下，按<Ctrl+C>组合键终止当前运行的任务。

如果使用 **escape-key** 命令设置了别的快捷键，则新的快捷键将代替<Ctrl+C>键来终止当前运行的任务，新设置的快捷键可以使用 **display current-configuration** 命令来查看。

需要注意的是，如果在某用户界面下设置了 **character**，当使用该用户界面登录到设备，又通过该设备 telnet 到别的设备，这时的 **character** 将被视为控制字符，只能用来中止当前的任务，不能作为编辑字符输入。比如，在 Device A 的 VTY 0 用户界面下指定 **character** 为 e，此时，PC（超级终

端)使用 VTY 0 界面登录设备,在 PC 上 e 可以作为编辑字符输入,也可以用 e 来中止 Device A 上正在运行的任务。如果通过 Device A 再 telnet 到 Device B,则此时,PC 上只能使用 e 来中止 Device B 上正在运行的任务,但不能作为编辑字符输入。所以,建议用户尽量将 *character* 指定为组合键。

【举例】

定义终止当前运行任务的快捷键为<a>。

```
<Sysname> system-view
[Sysname] user-interface console 0
[Sysname-ui-console0] escape-key a
验证过程如下:
```

使用 ping 命令检查 IP 地址为 192.168.1.49 的设备是否可达,并用-c 参数指定发送 ICMP 回显请求报文的数目为 20。

```
<Sysname> ping -c 20 192.168.1.49
PING 192.168.1.49: 56 data bytes, press a to break
  Reply from 192.168.1.49: bytes=56 Sequence=1 ttl=255 time=3 ms
  Reply from 192.168.1.49: bytes=56 Sequence=2 ttl=255 time=3 ms
```

键入<a>,任务立即终止,并返回到当前视图。

```
--- 192.168.1.49 ping statistics ---
  2 packet(s) transmitted
  2 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 3/3/3 ms
```

```
<Sysname>
```

1.1.13 flow-control

【命令】

```
flow-control { hardware | none | software }
flow-control hardware flow-control-type1 [ software flow-control-type2 ]
flow-control software flow-control-type1 [ hardware flow-control-type2 ]
undo flow-control
```

【视图】

用户界面视图

【缺省级别】

2: 系统级

【参数】

hardware: 进行硬件方式的流量控制。

none: 不进行流量控制。

software: 进行软件方式的流量控制。

flow-control-type1、*flow-control-type2*: 表示流量控制的方向,取值为 **in** 或 **out**, **in** 表示入方向,即本设备接受远端设备流控; **out** 表示出方向,即本设备流控远端设备。

【描述】

flow-control 命令用来配置流量控制方式。**undo flow-control** 命令用来恢复缺省情况。缺省情况下,不进行流量控制。

流量控制分为 **in** 和 **out** 两个方向，**in** 表示本设备能够接受远端设备流控，**out** 表示本设备能够流控远端设备。流控方式又分为 **hardware**、**software** 和 **none** 三种，同一个方向，只能配置一种流控方式。

- 如果要给 **in** 和 **out** 方向配置相同的流控方式，请使用命令 **flow-control { hardware | software | none }**。
- 如果要给 **in** 和 **out** 方向配置不同的流控方式，请使用命令 **flow-control hardware flow-control-type1 [software flow-control-type2]** 或 **flow-control software flow-control-type1 [hardware flow-control-type2]**。当不指定可选参数时，表示另一个方向的流量控制方式为 **none**（比如配置 **flow-control hardware in**，则系统会自动将 **out** 方向配置为无流控）。

要使流量控制生效，双方才能正常通信，本设备上 **in** (**out**) 方向配置的流控方式和对端设备上 **out** (**in**) 方向配置的流控方式必须相同。



说明

本命令只对异步串口（包括 AUX、Console 口）有效。

【举例】

配置 Console0 用户界面视图下，入方向采用硬件流量控制方式，出方向不进行流量控制。（支持 *flow-control-type1*、*flow-control-type2* 参数的设备才支持该举例）

```
<Sysname> system-view
[Sysname] user-interface console 0
[Sysname-ui-console0] flow-control hardware in
```

配置 Console0 用户界面视图下，入方向采用硬件流量控制方式，出方向采用软件流量控制方式。（支持 *flow-control-type1*、*flow-control-type2* 参数的设备才支持该举例）

```
<Sysname> system-view
[Sysname] user-interface console 0
[Sysname-ui-console0] flow-control hardware in software out
```

1.1.14 free user-interface

【命令】

```
free user-interface { num1 | { aux | console | tty | vty } num2 }
```

【视图】

用户视图

【缺省级别】

3：管理级

【参数】

num1：用户界面的编号（绝对编号方式），不同型号的设备支持的取值范围不同，请以设备的实际情况为准，一般从 0 开始。

num2：用户界面的编号（相对编号方式），不同型号的设备支持的取值范围不同，请以设备的实际情况为准。

【描述】

free user-interface 命令用来释放指定用户界面上建立的连接。

需要注意的是，用户不能使用该命令释放自己的连接。

【举例】

```
# 释放用户界面上 VTY 1 建立的连接。
<Sysname> display users
The user application information of the user interface(s):
  Idx UI      Delay    Type Userlevel
+ 82 VTY 0    00:00:00 TEL    3
  83 VTY 1    00:00:03 TEL    3
Following are more details.
VTY 0   :
        Location: 192.168.1.26
VTY 1   :
        Location: 192.168.1.20
+       : Current operation user.
F       : Current operation user work in async mode.
// 通过以上操作可以查看当前有哪些用户正在操作设备
<Sysname> free user-interface vty 1
Are you sure to free user-interface vty1? [Y/N]:y
// 如果 VTY 1 用户的操作影响到网络管理员当前的操作，使用以上步骤可以将他强制下线
```

1.1.15 history-command max-size

【命令】

history-command max-size size-value

undo history-command max-size

【视图】

用户界面视图

【缺省级别】

2: 系统级

【参数】

size-value: 历史缓冲区的容量，取值范围为 0~256。

【描述】

history-command max-size 命令用来设置当前用户界面历史命令缓冲区的容量。**undo history-command max-size** 命令用来恢复缺省情况。

缺省情况下，历史命令缓冲区可存储 10 条历史命令。

每个用户界面对应一个历史命令缓冲区，缓冲区里保存了当前用户最近执行成功的命令，缓冲区的容量决定了可以保存的历史命令的数目。用户使用 **display history-command** 命令、上光标键 ↑ 或下光标键 ↓ 可以随时了解近期成功执行了哪些操作（**display history-command** 命令的详细介绍请参见“基础命令参考”中的“CLI”）。同时登录设备的不同用户拥有不同的历史命令缓冲区，互不影响。

用户退出当前会话时，系统会自动清除相应历史命令缓冲区内保存的历史命令。

【举例】

```
# 设置历史命令缓冲区的容量为 20。
<Sysname> system-view
[Sysname] user-interface console 0
[Sysname-ui-console0] history-command max-size 20
```

1.1.16 idle-timeout

【命令】

```
idle-timeout minutes [ seconds ]  
undo idle-timeout
```

【视图】

用户界面视图

【缺省级别】

2: 系统级

【参数】

minutes: 指定超时时间，取值范围为 0~35791，单位为分钟。

seconds: 指定超时时间，取值范围为 0~59，单位为秒，缺省值为 0 秒。

【描述】

idle-timeout 命令用来设置用户连接的超时时间。**undo idle-timeout** 命令用来恢复超时时间的缺省值。

缺省情况下，超时时间为 10 分钟。



说明

- 如果在超时时间段内设备和用户间没有消息交互，设备就自动断开用户连接。
 - 当超时时间设置为 0 时，表示关闭超时断开连接的功能。
-

【举例】

设置超时时间为 1 分钟 30 秒。

```
<Sysname> system-view  
[Sysname] user-interface console 0  
[Sysname-ui-console0] idle-timeout 1 30
```

1.1.17 ip http acl

【命令】

同时支持 WLAN ACL 和基本 ACL 的产品：

```
ip http acl acl-number  
undo ip http acl acl-number
```

只支持基本 ACL 的产品：

```
ip http acl acl-number  
undo ip http acl
```

【视图】

系统视图

【缺省级别】

2: 系统级

【参数】

acl-number: ACL 的编号，取值范围为：

100~199: WLAN ACL

- 2000~2999: 基本 IPv4 ACL

【描述】

ip http acl 命令用来配置 HTTP 服务与 ACL 关联。**undo ip http acl** 命令用来取消 HTTP 服务与 ACL 的关联。

缺省情况下，没有 ACL 与 HTTP 服务关联。

配置 HTTP 服务与 ACL 关联后，将只允许通过 ACL 过滤的客户端访问设备。

需要注意的是：

- HTTP 服务可以与 WLAN ACL 和基本 ACL 关联，且两种类型的 ACL 之间不会相互覆盖。但是，同种类型的 ACL 之间会相互覆盖，即如果重复执行 **ip http acl** 命令关联同种类型的 ACL，HTTP 服务将只与最后一次配置的 ACL 关联。
- HTTP 服务与 WLAN ACL 关联时，HTTP 服务仅利用该 ACL 过滤无线客户端，不会利用该 ACL 过滤有线方式访问的客户端。

相关配置可参考命令 **display ip http** 和“安全命令参考/ACL”中的命令 **acl number**。

【举例】

配置 HTTP 服务与 ACL 100 关联，只允许 SSID 为 user-ssid-name 的无线客户端通过 Web 访问设备。

```
<Sysname> system-view
[Sysname] acl number 100
[Sysname-acl-wlan-100] rule permit ssid user-ssid-name
[Sysname-acl-wlan-100] quit
[Sysname] ip http acl 100
```

配置 HTTP 服务与 ACL 2001 关联，只允许 10.10.0.0/16 网段的客户端通过 Web 访问设备。

```
<Sysname> system-view
[Sysname] acl number 2001
[Sysname-acl-basic-2001] rule permit source 10.10.0.0 0.0.255.255
[Sysname-acl-basic-2001] quit
[Sysname] ip http acl 2001
```

1.1.18 ip http enable

【命令】

ip http enable

undo ip http enable

【视图】

系统视图

【缺省级别】

2: 系统级

【参数】

无

【描述】

ip http enable 命令用来使能 HTTP 服务。**undo ip http enable** 命令用来关闭 HTTP 服务。

只有使能该功能后，设备才能作为 HTTP 服务器，允许用户通过 Web 功能访问和控制设备。

相关配置可参考命令 **display ip http**。

【举例】

```
# 使能 HTTP 服务。
<Sysname> system-view
[Sysname] ip http enable
# 关闭 HTTP 服务。
<Sysname> system-view
[Sysname] undo ip http enable
```

1.1.19 ip http port

【命令】

```
ip http port port-number
undo ip http port
```

【视图】

系统视图

【缺省级别】

3: 管理级

【参数】

port-number: HTTP 服务的端口号，取值范围为 1~65535。

【描述】

ip http port 命令用来配置 HTTP 服务的端口号。**undo ip http port** 命令用来恢复缺省情况。

缺省情况下，HTTP 服务的端口号为 80。

需要注意的是，此命令不会检查配置的端口是否与已有服务使用的端口冲突，修改前必须保证该端口没有被其他服务使用。

相关配置可参考命令 **display ip http**。

【举例】

```
# 配置 HTTP 服务的端口号为 8080。
<Sysname> system-view
[Sysname] ip http port 8080
```

1.1.20 ip https acl

【命令】

同时支持 WLAN ACL 和基本 ACL 的产品：

```
ip https acl acl-number
undo ip https acl acl-number
```

只支持基本 ACL 的产品：

```
ip https acl acl-number
undo ip https acl
```

【视图】

系统视图

【缺省级别】

3: 管理级

【参数】

acl-number: ACL 的编号, 取值范围为:

- 100~199: WLAN ACL
- 2000~2999: 基本 IPv4 ACL

【描述】

ip https acl 命令用来配置 HTTPS 服务与 ACL 关联。**undo ip https acl** 命令用来取消 HTTPS 服务与 ACL 的关联。

缺省情况下, 没有 ACL 与 HTTPS 服务关联。

配置 HTTPS 服务与 ACL 关联后, 将只允许通过 ACL 过滤的客户端访问设备。

需要注意的是:

- HTTPS 服务可以与 WLAN ACL 和基本 ACL 关联, 且两种类型的 ACL 之间不会相互覆盖。但是, 同种类型的 ACL 之间会相互覆盖, 即如果重复执行 **ip https acl** 命令关联同种类型的 ACL, HTTPS 服务将只与最后一次配置的 ACL 关联。
- HTTPS 服务与 WLAN ACL 关联, HTTPS 服务仅利用该 ACL 过滤无线客户端, 不会利用该 ACL 过滤有线方式访问的客户端。

相关配置可参考命令 **display ip https** 和“安全命令参考/ACL”中的命令 **acl number**。

【举例】

配置 HTTPS 服务与 ACL 100 关联, 只允许 SSID 为 user-ssid-name 的无线客户端通过 Web 访问设备。

```
<Sysname> system-view
[Sysname] acl number 100
[Sysname-acl-wlan-100] rule permit ssid user-ssid-name
[Sysname-acl-wlan-100] quit
[Sysname] ip https acl 100
```

配置 HTTPS 服务与 ACL 2001 关联, 只允许 10.10.0.0/16 网段的客户端通过 Web 访问设备。

```
<Sysname> system-view
[Sysname] acl number 2001
[Sysname-acl-basic-2001] rule permit source 10.10.0.0 0.0.255.255
[Sysname-acl-basic-2001] quit
[Sysname] ip https acl 2001
```

1.1.21 ip https certificate access-control-policy

【命令】

ip https certificate access-control-policy *policy-name*

undo ip https certificate access-control-policy

【视图】

系统视图

【缺省级别】

3: 管理级

【参数】

policy-name: 证书属性访问控制策略名, 为 1~16 个字符的字符串。

【描述】

ip https certificate access-control-policy 命令用来配置 HTTPS 服务与证书属性访问控制策略关联。**undo ip https certificate access-control-policy** 命令用来取消 HTTPS 服务与证书属性访问控制策略的关联。

缺省情况下，没有证书属性访问控制策略与 HTTPS 服务关联。

通过将 HTTPS 服务与已配置的客户端证书属性访问控制策略关联，可以实现对客户端的访问权限进行控制。

相关配置可参考命令 **display ip https** 和“安全命令参考/PKI”中的命令 **pki certificate access-control-policy**。

【举例】

```
# 设置 HTTPS 服务使用的证书属性访问控制策略为 myacl。  
<Sysname> system-view  
[Sysname] ip https certificate access-control-policy myacl
```

1.1.22 ip https enable

【命令】

```
ip https enable  
undo ip https enable
```

【视图】

系统视图

【缺省级别】

3: 管理级

【参数】

无

【描述】

ip https enable 命令用来使能 HTTPS 服务。**undo ip https enable** 命令用来关闭 HTTPS 服务。缺省情况下，HTTPS 服务处于关闭状态。

只有使能该功能后，设备才能作为 HTTPS 服务器，允许用户通过 Web 功能访问和控制设备。

需要注意的是，使能 HTTPS 服务，会触发 SSL 的握手协商过程。在 SSL 握手协商过程中，如果设备的本地证书已经存在，则 SSL 协商可以成功，HTTPS 服务可以正常启动；如果设备的本地证书不存在，则 SSL 协商过程会触发证书申请流程。由于证书申请需要较长的时间，会导致 SSL 协商不成功，从而无法正常启动 HTTPS 服务。因此，在这种情况下，需要多次执行 **ip https enable** 命令，这样 HTTPS 服务才能正常启动。

相关配置可参考命令 **display ip https**

【举例】

```
# 使能 HTTPS 服务。  
<Sysname> system-view  
[Sysname] ip https enable
```

1.1.23 ip https port

【命令】

```
ip https port port-number  
undo ip https port
```

【视图】

系统视图

【缺省级别】

3: 管理级

【参数】

port-number: HTTPS 服务的端口号, 取值范围为 1~65535。

【描述】

ip https port 命令用来配置 HTTPS 服务的端口号。**undo ip https port** 命令用来恢复缺省情况。缺省情况下, HTTPS 服务的端口号为 443。

需要注意的是, 此命令不会检查配置的端口是否与已有服务使用的端口冲突, 修改前必须保证该端口没有被其他服务使用。

相关配置可参考命令 **display ip https**。

【举例】

配置 HTTPS 服务的端口号为 6000。

```
<Sysname> system-view
[Sysname] ip https port 6000
```

1.1.24 ip https ssl-server-policy

【命令】

ip https ssl-server-policy *policy-name*
undo ip https ssl-server-policy

【视图】

系统视图

【缺省级别】

3: 管理级

【参数】

policy-name: SSL 服务器端策略名, 为 1~16 个字符的字符串。

【描述】

ip https ssl-server-policy 命令用来配置 HTTPS 服务与 SSL 服务器端策略关联。**undo ip https ssl-server-policy** 命令用来取消 HTTPS 服务与 SSL 服务器端策略的关联。

缺省情况下, 没有 SSL 服务器端策略与 HTTPS 服务关联。

需要注意的是:

- 只有此命令设置成功, 才能使能 HTTPS 服务。
- HTTPS 服务使能后不允许修改 SSL 服务器端策略, 也不允许取消 HTTPS 服务与 SSL 服务器端策略的关联。

相关配置可参考命令 **display ip https** 和“安全命令参考/SSL”中的命令 **ssl server-policy**。

【举例】

设置 HTTPS 服务使用的 SSL 服务器端策略为 myssl。

```
<Sysname> system-view
[Sysname] ip https ssl-server-policy myssl
```

1.1.25 lock

【命令】

lock

【视图】

用户视图

【缺省级别】

3: 管理级

【参数】

无

【描述】

lock 命令用来锁住当前用户界面，防止未授权的用户操作该界面。

用户输入 **lock** 命令后，系统提示输入密码（密码最大长度为 16 个字符），并提示再次输入密码，只有两次输入的密码相同，**Lock** 操作才能成功。之后，如果用户要再进入系统，需要先按回车键，并输入刚才配置的密码后，才能结束锁定，进入系统。

缺省情况下，系统不会自动锁住当前用户界面。

【举例】

锁住当前用户界面。

```
<Sysname> lock
Please input password<1 to 16> to lock current user terminal interface:
Password:
Again:
```

```
locked !
```

```
Password:
<Sysname>
```

1.1.26 parity

【命令】

```
parity { even | mark | none | odd | space }
undo parity
```

【视图】

用户界面视图

【缺省级别】

2: 系统级

【参数】

even: 进行偶校验。

mark: 进行标记校验。

none: 无校验。

odd: 进行奇校验。

space: 进行空格校验。

【描述】

parity 命令用来设置校验位的解析和生成方式。**undo parity** 命令用来恢复缺省情况。缺省情况下，设备校验位的校验方式为 **none**，即不进行校验。



说明

- 本命令只对异步串口（包括 AUX、Console 口）有效。
 - 访问终端和设备相应用户界面下校验位的设置必须一致，双方才能正常通信。
-

【举例】

将 AUX 口传输校验位设为奇校验。

```
<Sysname> system-view
[Sysname] user-interface aux 0
[Sysname-ui-aux0] parity odd
```

1.1.27 protocol inbound

【命令】

protocol inbound { all | pad | ssh | telnet }

【视图】

VTY 用户界面视图

【缺省级别】

3: 管理级

【参数】

all: 支持所有的协议，包括 Telnet、SSH 和 PAD。

pad: 支持 PAD 协议。

ssh: 支持 SSH 协议。

telnet: 支持 Telnet 协议。

【描述】

protocol inbound 命令用来指定所在用户界面支持的协议。

缺省情况下，系统支持所有协议。

配置结果将在下次登录时生效。



说明

- 如果要配置用户界面支持 SSH 协议，必须先将该用户的认证方式配置为 **scheme**，否则 **protocol inbound ssh** 命令会执行失败。相关配置可参考命令 **authentication-mode**。
 - Telnet 协议的缺省认证方式是 **password**。
-

【举例】

设置用户界面 VTY 0 到 VTY 4 只支持 SSH 协议。

```
<Sysname> system-view
[Sysname] user-interface vty 0 4
[Sysname-ui-vty0-4] authentication-mode scheme
[Sysname-ui-vty0-4] protocol inbound ssh
```

1.1.28 redirect disconnect

【命令】

redirect disconnect

【视图】

用户界面视图

【缺省级别】

2: 系统级

【参数】

无

【描述】

redirect disconnect 命令用来强制断开已经建立的 Telnet 重定向连接。



说明

- 目前只有 AUX 和 TTY 类型的用户界面支持本命令。
 - 执行该命令前，请先执行 **redirect enable** 命令使能用户界面的重定向功能。
-

【举例】

强制断开已经建立的 Telnet 重定向连接。

```
<Sysname> system-view
[Sysname] user-interface tty 1
[Sysname-ui-tty1] redirect disconnect
```

1.1.29 redirect enable

【命令】

redirect enable

undo redirect enable

【视图】

用户界面视图

【缺省级别】

2: 系统级

【参数】

无

【描述】

redirect enable 命令用来使能当前异步串口的重定向功能。**undo redirect enable** 命令用来禁止当前异步串口的重定向功能。

缺省情况下，异步串口重定向功能被禁止。



说明

- 目前只有 AUX 和 TTY 类型的用户界面支持本命令。
- 如果要使用重定向功能或配置重定向的相关参数，必须先使用该命令使能用户界面的重定向功能。
- 重定向设备与被登录设备相连端口对应的用户界面的停止位设置（stopbits）必须相同，否则重定向将失败。可以在重定向前，使用 **stopbit-error intolerance** 命令检测重定向设备与被登录设备的停止位设置是否相同。

相关配置可参考命令 `telnet` 和 `display tcp status`。

【举例】

使能用户界面 TTY 7 的重定向功能。

```
<Sysname> system-view
[Sysname] user-interfac tty 7
[Sysname-ui-tty7] redirect enable
```

1.1.30 redirect listen-port

【命令】

redirect listen-port *port-number*

undo redirect listen-port

【视图】

用户界面视图

【缺省级别】

2: 系统级

【参数】

port-number: 监听端口号，取值范围为 2000~50000。

【描述】

redirect listen-port 命令用来设置 Telnet 重定向的监听端口。设备只对该端口收到的数据包进行重定向。**undo redirect listen-port** 命令用来恢复缺省的监听端口。

缺省情况下，Telnet 重定向的监听端口号为用户界面的绝对编号加 2000。



说明

- 目前只有 AUX 和 TTY 类型的用户界面支持本命令。
- 执行该命令前，请先执行 **redirect enable** 命令使能用户界面的重定向功能。

【举例】

设置 Telnet 重定向的监听端口号为 3000。

```
<Sysname> system-view
[Sysname] user-interface tty 1
[Sysname-ui-tty1] redirect listen-port 3000
```

1.1.31 redirect refuse-negotiation

【命令】

redirect refuse-negotiation
undo redirect refuse-negotiation

【视图】

用户界面视图

【缺省级别】

2: 系统级

【参数】

无

【描述】

redirect refuse-negotiation 命令用来强制设置在建立 Telnet 重定向连接时不进行 Telnet 选项协商。**undo redirect refuse-negotiation** 命令用来设置在建立 Telnet 重定向连接时进行 Telnet 选项协商。

缺省情况下, 进行 Telnet 选项协商。



说明

- 目前只有 AUX 和 TTY 类型的用户界面支持本命令。
 - 执行该命令前, 请先执行 **redirect enable** 命令使能用户界面的重定向功能。
-

【举例】

设置在建立 Telnet 重定向连接时不进行 Telnet 选项协商。

```
<Sysname> system-view  
[Sysname] user-interface tty 1  
[Sysname-ui-tty1] redirect refuse-negotiation
```

1.1.32 redirect refuse-teltransfer

【命令】

redirect refuse-teltransfer
undo redirect refuse-teltransfer

【视图】

用户界面视图

【缺省级别】

2: 系统级

【参数】

无

【描述】

redirect refuse-teltransfer 命令用来设置在建立 Telnet 重定向连接时不对 ACSII 码 0xff 进行转义。**undo redirect refuse-teltransfer** 命令用来恢复缺省情况。

缺省情况下, 在建立 Telnet 重定向连接时会将 ACSII 码 0xff 转义为 0xff 0xff。

- Telnet 重定向设备收到 Telnet 客户端发送的 0xff 字符时,会将 0xff 作为 Telnet 协议字过滤掉,从而导致 0xff 字符的丢失。为了保证字符能正确发送到 Telnet 服务器,需要在 Telnet 重定向设备上将 0xff 转义为 0xff 0xff,转义后,Telnet 重定向设备会过滤掉一个 0xff,将另一个 0xff 发送给 Telnet 服务器,以保证 0xff 字符不丢失。
 - 如果确定 Telnet 客户端不会发送 0xff 字符,则可以不对 ACSII 码 0xff 进行转义。
-

说明

- 目前只有 AUX 和 TTY 类型的用户界面支持本命令。
 - 执行该命令前,请先执行 **redirect enable** 命令使能用户界面的重定向功能。
-

【举例】

设置在建立 Telnet 重定向连接时不对 ACSII 码 0xff 进行转义。

```
<Sysname> system-view
[Sysname] user-interface tty 1
[Sysname-ui-tty1] redirect refuse-teltransfer
```

1.1.33 redirect return-deal from-telnet

【命令】

redirect return-deal from-telnet
undo redirect return-deal from-telnet

【视图】

用户界面视图

【缺省级别】

2: 系统级

【参数】

无

【描述】

redirect return-deal from-telnet 命令用来设置 Telnet 重定向设备对从 Telnet 客户端接收到的回车符进行处理,即将接收到的“0x0d 0x0a”和“0x0d 0x00”统一修改为“0x0d”。**undo redirect return-deal from-telnet** 命令用来恢复缺省情况。

缺省情况下,设备不对从 Telnet 客户端接收到的回车符进行处理。

说明

- 目前只有 AUX 和 TTY 类型的用户界面支持本命令。
 - 执行该命令前,请先执行 **redirect enable** 命令使能用户界面的重定向功能。
-

【举例】

设置 Telnet 重定向设备对从 Telnet 客户端接收到的回车符进行处理。

```
<Sysname> system-view
[Sysname] user-interface tty 1
[Sysname-ui-tty1] redirect return-deal from-telnet
```

1.1.34 redirect return-deal from-terminal

【命令】

redirect return-deal from-terminal
undo redirect return-deal from-terminal

【视图】

用户界面视图

【缺省级别】

2: 系统级

【参数】

无

【描述】

redirect return-deal from-terminal 命令用来设置当设备进行 Telnet 重定向时对从终端（例如从 Console 口连接的 PC）接收到的回车符进行处理，即将接收到的“0x0d 0x0a”和“0x0d 0x00”统一修改为“0x0d”。**undo redirect return-deal from-terminal** 命令用来恢复缺省情况。缺省情况下，当设备进行 Telnet 重定向时不会对从终端接收到的回车符进行处理，而是直接转发。



说明

- 目前只有 AUX 和 TTY 类型的用户界面支持本命令。
- 执行该命令前，请先执行 **redirect enable** 命令使能用户界面的重定向功能。

【举例】

当设备进行 Telnet 重定向时对从终端接收到的回车符进行处理。

```
<Sysname> system-view  
[Sysname] user-interface tty 1  
[Sysname-ui-tty1] redirect return-deal from-terminal
```

1.1.35 redirect timeout

【命令】

redirect timeout time
undo redirect timeout

【视图】

用户界面视图

【缺省级别】

2: 系统级

【参数】

time: 超时时间，取值范围为 30~86400，单位为秒。

【描述】

redirect timeout 命令用来设置 Telnet 重定向的空闲超时时间。如果在指定的时间内没有从 Telnet 客户端接收到数据，则断开 Telnet 重定向连接。**undo redirect timeout** 命令用来设置 Telnet 重定向连接永远不超时。

缺省情况下，设备 Telnet 重定向的空闲超时时间为 360 秒。

说明

- 目前只有 AUX 和 TTY 类型的用户界面支持本命令。
 - 执行该命令前，请先执行 **redirect enable** 命令使能用户界面的重定向功能。
-

【举例】

设置 Telnet 重定向的空闲超时时间为 200 秒。

```
<Sysname> system-view
[Sysname] user-interface tty 1
[Sysname-ui-tty1] redirect timeout 200
```

1.1.36 screen-length

【命令】

screen-length *screen-length*

undo screen-length

【视图】

用户界面视图

【缺省级别】

2: 系统级

【参数】

screen-length: 指定下一屏所显示的行数，取值范围为 0~512，0 表示一次性显示全部信息，即不进行分屏显示。

【描述】

screen-length 命令用来设置下一屏所显示的行数。**undo screen-length** 命令用来恢复缺省情况。缺省情况下，下一屏显示 24 行数据。

设备支持分屏显示信息，在暂停显示时按空格键，能继续显示下一屏信息。该命令设置的是下一屏所显示的行数，但显示终端实际显示的行数由终端的规格决定。比如，设置 **screen-length** 的值为 40，但显示终端的规格为 24 行，当暂停显示按空格键时，设备发送给显示终端的信息为 40 行，但当前屏幕显示的是第 18~第 40 行的信息，前面的 17 行信息，需要通过<Page Up>/<Page Down>键来翻看。

该命令设置的是指定用户界面的分屏显示行数，但用户可以使用 **screen-length disable** 命令关闭当前界面的分屏显示功能。**screen-length disable** 命令的详细介绍请参见“基础命令参考”中的“CLI”。

【举例】

设置 Console 用户界面下一屏显示的行数为 30。

```
<Sysname> system-view
[Sysname] user-interface console 0
[Sysname-ui-console0] screen-length 30
```

1.1.37 send

【命令】

```
send { all | num1 | { aux | console | tty | vty } num2 }
```

【视图】

用户视图

【缺省级别】

1: 监控级

【参数】

all: 所有的用户界面。

num1: 用户界面的编号（绝对编号方式），不同型号的设备支持的取值范围不同，请以设备的实际情况为准，一般从 0 开始。

num2: 用户界面的编号（相对编号方式），不同型号的设备支持的取值范围不同，请以设备的实际情况为准。

【描述】

send 命令用来向指定的用户界面发送消息。

在输入消息内容时，按<Ctrl+Z>组合键结束输入，按<Ctrl+C>组合键取消此次操作。

【举例】

Console 用户界面给自己发送消息 hello abc。

```
<Sysname> send console 0
Enter message, end with CTRL+Z or Enter; abort with CTRL+C:
hello abc^Z
Send message? [Y/N]:y
<Sysname>
```

```
***
***
***Message from con0 to con0
***
hello abc
```

```
<Sysname>
```

使用 VTY 0 用户界面上线的用户想重启设备，为了提醒其它并行操作用户做好相应准备（比如保存当前配置），于是向其它用户界面发送消息“Note please, I will reboot the system!”。

- VTY 0 终端上的配置。

```
<Sysname> display users
The user application information of the user interface(s):
   Idx UI      Delay      Type Userlevel
+  82 VTY 0    00:00:00 TEL      3
   83 VTY 1    00:00:03 TEL      3
```

Following are more details.

```
VTY 0  :
        Location: 192.168.1.26
VTY 1  :
        Location: 192.168.1.20
+      : Current operation user.
F      : Current operation user work in async mode.
```

// 通过以上操作可以查看当前有哪些用户正在操作设备


```
<Sysname> send vty 1
Enter message, end with CTRL+Z or Enter; abort with CTRL+C:
Note please, I will reboot the system in 3 minutes!^Z
Send message? [Y/N]:y
// 通过以上操作可以给 VTY 1 发送消息, 告诉他“我将在 3 分钟内重启系统”, 以便其他用户做好
相关备份工作
```

- 如果有用户使用 VTY 1 用户界面登录, 则用户的终端上将收到如下消息 (该例为 VTY 1 正在输入 `interface ethernet` 命令的过程中收到了 VTY 0 的消息):

```
[Sysname] interface eth

***
***
***Message from vty0 to vty1
***
Note please, I will reboot the system in 3 minutes!
```

1.1.38 set authentication password

【命令】

```
set authentication password { cipher | simple } password
undo set authentication password
```

【视图】

用户界面视图

【缺省级别】

3: 管理级

【参数】

cipher: 配置密文密码。

simple: 配置明文密码。

password: 密码字符串, 区分大小写。

- 如果采用明文 (**simple**) 形式, 为 1~16 个字符的字符串;
- 如果采用密文 (**cipher**) 形式, 既可以是 1~16 个字符的明文, 也可以是 24 个字符的密文。如: 明文 “1234567” 对应的密文是 “_(TT8FJY\5SQ=^Q`MAF4<1!!”。

【描述】

set authentication password 命令用来设置本地认证的口令。**undo set authentication password** 命令用来取消本地认证的口令。

缺省情况下, 没有设置本地认证的密码。

- 如果指定 **simple** 参数, 则配置文件中保存的是明文密码;
- 如果指定 **cipher** 参数, 如果用户输入的是明文密码, 在配置文件中会加密后保存。
- 不论配置的是明文密码还是密文密码, 认证时必须输入明文形式的密码。
- 明文密码容易被盗取, 建议用户使用密文形式。

相关配置可参考命令 **authentication-mode**。

【举例】

设置用户界面 Console 0 的本地认证口令为 hello。

```
<Sysname> system-view
[Sysname] user-interface console 0
```

```
[Sysname-ui-console0] authentication-mode password
[Sysname-ui-console0] set authentication password cipher hello
```

设置完后如果退出系统，只有在密码提示信息后输入 **hello** 字符串才能再进入系统。

1.1.39 shell

【命令】

```
shell
undo shell
```

【视图】

用户界面视图

【缺省级别】

3: 管理级

【参数】

无

【描述】

shell 命令用来在当前用户界面上启动终端服务。**undo shell** 命令用来在当前用户界面上禁止终端服务。

缺省情况下，系统在所有的用户界面上启动终端服务。

undo shell 命令有以下几点限制：

- Console 口不支持该命令；
- 如果设备上只有一个 AUX 口，而没有 Console 口（Console 口与 AUX 口共用），则此 AUX 口不支持该命令；
- 用户不能在自己登录的用户界面上使用该命令。

【举例】

在虚拟终端 VTY0 到 VTY4 上终止终端服务（用户将不能通过 VTY0-4 登录设备）。

```
<Sysname> system-view
[Sysname] user-interface vty 0 4
[Sysname-ui-vty0-4] undo shell
% Disable ui-vty0-4 , are you sure? [Y/N]:y
[Sysname-ui-vty0-4]
```

对于 Telnet 终端，登录后将提示：

```
The connection was closed by the remote host!
```

1.1.40 speed (User interface view)

【命令】

```
speed speed-value
undo speed
```

【视图】

用户界面视图

【缺省级别】

2: 系统级

【参数】

speed-value: 传输速率, 单位为 bps。异步串口的传输速率有: 300bps、600bps、1200bps、2400bps、4800bps、9600bps、19200bps、38400bps、57600bps 和 115200bps。设备对以上速率的支持由产品和配置时的网络环境决定。

【描述】

speed 命令用来设置用户界面的传输速率。**undo speed** 命令用来恢复缺省情况。缺省情况下, 用户界面的传输速率为 9600bps。



说明

- 本命令只对异步串口 (包括 AUX、Console 口) 有效。
 - 访问终端和设备相应用户界面下传输速率的设置必须一致, 双方才能正常通信。
-

【举例】

将用户界面 AUX 0 的传输速率设置为 19200bps。

```
<Sysname> system-view
[Sysname] user-interface aux 0
[Sysname-ui-aux0] speed 19200
```

1.1.41 stopbit-error intolerance

【命令】

stopbit-error intolerance
undo stopbit-error intolerance

【视图】

用户界面视图

【缺省级别】

2: 系统级

【参数】

无

【描述】

stopbit-error intolerance 命令用来检测停止位。**undo stopbit-error intolerance** 命令用来恢复缺省情况。

缺省情况下, 不检测停止位。



说明

本命令只对异步串口 (包括 AUX、Console 口) 有效。

【举例】

设置对用户界面 AUX 0 检测停止位。

```
<Sysname> system-view
[Sysname] user-interface aux 0
[Sysname-ui-aux0] stopbit-error intolerance
```

1.1.42 stopbits

【命令】

```
stopbits { 1 | 1.5 | 2 }  
undo stopbits
```

【视图】

用户界面视图

【缺省级别】

2: 系统级

【参数】

- 1: 停止位为 1 个比特。
- 1.5: 停止位为 1.5 个比特。
- 2: 停止位为 2 个比特。

【描述】

stopbits 命令用来设置停止位的个数。**undo stopbits** 命令用来恢复缺省的用户界面停止位。缺省情况下，停止位为 1 个比特。



说明

- 本命令只对异步串口（包括 AUX、Console 口）有效。
- 访问终端和设备相应用户界面下停止位的设置必须一致，双方才能正常通信。

【举例】

设置 AUX 用户界面的停止位为 1.5 个比特。

```
<Sysname> system-view  
[Sysname] user-interface aux 0  
[Sysname-ui-aux0] stopbits 1.5
```

1.1.43 telnet

【命令】

```
telnet remote-host [ service-port ] [ vpn-instance vpn-instance-name ] [ source { interface  
interface-type interface-number | ip ip-address } ]
```

【视图】

用户视图

【缺省级别】

0: 访问级

【参数】

- remote-host**: 远端系统的 IPv4 地址或主机名，为 1~20 个字符的字符串，不区分大小写。
- service-port**: 远端系统提供 Telnet 服务的 TCP 端口号，取值范围为 0~65535，缺省值为 23。
- vpn-instance vpn-instance-name**: 指定 VPN 实例。**vpn-instance-name** 为 VPN 实例的名称，为 1~31 个字符的字符串，区分大小写。
- source**: 指定 Telnet 报文的源接口或源 IPv4 地址。

interface interface-type interface-number: 指定源接口，发送的 Telnet 报文的源 IPv4 地址为该接口的地址。*interface-type interface-number* 为接口类型和接口编号。

ip ip-address: 指定 Telnet 报文的源 IPv4 地址。

【描述】

telnet 命令用于 Telnet 登录到远程主机，以便进行远程管理。用户可以使用 <Ctrl+K> 组合键或 **quit** 命令来中断本次 Telnet 登录。

需要注意的是，本命令指定的源 IPv4 地址或源接口只对当前 Telnet 连接有效。

【举例】

Telnet 登录到远程主机（IP 地址为 1.1.1.2），并指定发送 Telnet 报文的源 IP 地址为 1.1.1.1。

```
<Sysname> telnet 1.1.1.2 source ip 1.1.1.1
```

1.1.44 telnet client source

【命令】

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

undo telnet client source

【视图】

系统视图

【缺省级别】

2: 系统级

【参数】

interface interface-type interface-number: 指定源接口，发送的 Telnet 报文的源 IPv4 地址为该接口的地址。*interface-type interface-number* 为接口类型和接口编号。

ip ip-address: 指定发送 Telnet 报文的源 IPv4 地址。

【描述】

telnet client source 命令用来指定设备作为 Telnet 客户端时，发送 Telnet 报文的源 IPv4 地址或源接口。**undo telnet client source** 命令用来删除发送 Telnet 报文的源 IPv4 地址和源接口的配置。

缺省情况下，没有指定发送 Telnet 报文的源 IPv4 地址和源接口，此时通过路由选择源 IPv4 地址。

需要注意的是：

- 本命令指定的源 IPv4 地址或源接口对所有 Telnet 连接有效。
- 若同时使用本命令和 **telnet** 命令指定源 IPv4 地址或源接口，则以 **telnet** 命令指定的源 IP 地址或源接口为准。

相关配置可参考命令 **display telnet client configuration**。

【举例】

设备作为 Telnet 客户端时，指定发送的 Telnet 报文的源 IP 地址为 1.1.1.1。

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

```
[Sysname] telnet client source ip 1.1.1.1
```

1.1.45 telnet ipv6

【命令】

telnet ipv6 remote-host [-i interface-type interface-number] [port-number]

【视图】

用户视图

【缺省级别】

0: 访问级

【参数】

remote-host: 远端系统的 IPv6 地址或主机名, 为 1~46 个字符的字符串, 不区分大小写。

-i interface-type interface-number: Telnet 报文的出接口。*interface-type interface-number* 为接口类型和接口编号。当目的地址是链路本地地址时, 需要指定此参数。

port-number: 远端系统提供 Telnet 服务的 TCP 端口号, 取值范围为 0~65535, 缺省值为 23。

【描述】

telnet ipv6 命令用于 IPv6 组网环境下, Telnet 登录到远程主机, 以便进行远程管理。用户可以使用 <Ctrl+K> 组合键或 **quit** 命令来中断本次 Telnet 登录。

【举例】

Telnet 登录到远程主机, IPv6 地址为 5000::1。

```
<Sysname> telnet ipv6 5000::1
```

1.1.46 telnet server enable

【命令】

telnet server enable

undo telnet server enable

【视图】

系统视图

【缺省级别】

3: 管理级

【参数】

无

【描述】

telnet server enable 命令用来启动 Telnet 服务。**undo telnet server enable** 命令用来关闭 Telnet 服务。

缺省情况下, Telnet 服务处于关闭状态。

【举例】

启动 Telnet 服务。

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

```
[Sysname] telnet server enable
```

1.1.47 terminal type

【命令】

terminal type { ansi | vt100 }

undo terminal type

【视图】

用户界面视图

【缺省级别】

2: 系统级

【参数】

ansi: 终端显示类型为 ANSI 类型。

vt100: 终端显示类型为 VT100 类型。

【描述】

terminal type 命令用来设置当前用户界面下的终端显示类型。**undo terminal type** 命令用来恢复缺省情况。

缺省情况下，终端显示类型为 ANSI。

需要注意的是，设备支持 ANSI 和 VT100 两种终端显示类型。当设备的终端类型与客户端（如超级终端或者 Telnet 客户端等）的终端类型不一致，或者均设置为 ANSI 时，但当前编辑行的总字符数超过 80 个字符时，客户端会出现光标错位、终端屏幕不能正常显示的现象。建议两端都设置为 VT100 类型。

【举例】

设置终端显示类型为 VT100 类型。

```
<Sysname> system-view
[Sysname] user-interface vty 0
[Sysname-ui-vty0] terminal type vt100
```

1.1.48 user privilege level

【命令】

user privilege level *level*

undo user privilege level

【视图】

用户界面视图

【缺省级别】

3: 管理级

【参数】

level: 命令级别，取值范围为 0~3。



说明

命令级别共分为访问、监控、系统、管理 4 个级别，分别对应标识 0、1、2、3。管理员可以根据需要改变用户所能访问的命令级别，使其在相应的权限下工作。

【描述】

user privilege level 命令用来配置从当前用户界面登录系统的用户所能访问的命令级别。**undo user privilege level** 命令用来恢复缺省情况。

缺省情况下，通过 Console 口登录系统的用户所能访问的命令级别是 3，通过其它用户界面登录系统所能访问的命令级别是 0。

【举例】

设置通过用户界面 VTY 0 登录系统的用户能访问的命令级别为 0。

```
<Sysname> system-view
[Sysname] user-interface vty 0
```

```
[Sysname-ui-vty0] user privilege level 0
```

以 Telnet 方式从 VTY 0 用户界面登录设备后, 通过帮助信息可以看到终端上只显示了命令级别为 0 级的命令, 具体操作和显示信息如下:

```
<Sysname> ?
User view commands:
  cluster  Run cluster command
  display  Display current system information
  ping     Ping function
  quit     Exit from current command view
  rsh      Establish one RSH connection
  ssh2     Establish a secure shell client connection
  super    Set the current user priority level
  telnet   Establish one TELNET connection
  tracert  Trace route function
```

1.1.49 user-interface

【命令】

```
user-interface { first-num1 [ last-num1 ] | { aux | console | tty | vty } first-num2 [ last-num2 ] }
```

【视图】

系统视图

【缺省级别】

2: 系统级

【参数】

first-num1: 第一个用户界面的编号 (绝对编号方式), 不同型号的设备支持的取值范围不同, 请以设备的实际情况为准, 一般从 0 开始。

last-num1: 最后一个用户界面的编号 (绝对编号方式), 不同型号的设备支持的取值范围不同, 请以设备的实际情况为准, 一般从 0 开始, 但不能小于 **first-num1**。

first-num2: 第一个用户界面的编号 (相对编号方式), 不同型号的设备支持的取值范围不同, 请以设备的实际情况为准。

last-num2: 最后一个用户界面的编号 (相对编号方式), 不同型号的设备支持的取值范围不同, 请以设备的实际情况为准, 但不能小于 **first-num2**。

【描述】

user-interface 命令用来进入单一或多个用户界面视图。

- 进入单一用户界面视图进行配置后, 该配置只对该用户视图有效。
- 进入多个用户界面视图进行配置后, 该配置对这些用户视图均有效。

【举例】

进入 Console 用户界面视图。

```
<Sysname> system-view
[Sysname] user-interface console 0
[Sysname-ui-console0]
```

进入 VTY 0~4 用户界面视图。

```
<Sysname> system-view
[Sysname] user-interface vty 0 4
[Sysname-ui-vty0-4]
```