

目 录

1 登录设备.....	1-1
1.1 登录设备命令.....	1-1
1.1.1 activation-key.....	1-1
1.1.2 authentication-mode.....	1-3
1.1.3 auto-execute command.....	1-4
1.1.4 command accounting	1-6
1.1.5 command authorization.....	1-7
1.1.6 databits	1-8
1.1.7 display ip http.....	1-8
1.1.8 display ip https.....	1-9
1.1.9 display line	1-10
1.1.10 display telnet client.....	1-12
1.1.11 display user-interface.....	1-13
1.1.12 display users.....	1-15
1.1.13 display web menu	1-16
1.1.14 display web users	1-18
1.1.15 escape-key.....	1-19
1.1.16 flow-control.....	1-20
1.1.17 free line	1-21
1.1.18 free user-interface.....	1-22
1.1.19 free web users.....	1-23
1.1.20 history-command max-size	1-23
1.1.21 idle-timeout.....	1-24
1.1.22 ip http acl	1-25
1.1.23 ip http enable	1-26
1.1.24 ip http port.....	1-27
1.1.25 ip https acl.....	1-27
1.1.26 ip https certificate access-control-policy	1-28
1.1.27 ip https enable.....	1-29
1.1.28 ip https port	1-30
1.1.29 ip https ssl-server-policy.....	1-30
1.1.30 line	1-31
1.1.31 line class.....	1-32

1.1.32 lock	1-33
1.1.33 lock reauthentication	1-34
1.1.34 lock-key	1-36
1.1.35 parity	1-37
1.1.36 protocol inbound	1-38
1.1.37 restful http enable	1-40
1.1.38 restful https enable	1-41
1.1.39 screen-length	1-41
1.1.40 send	1-42
1.1.41 set authentication password	1-43
1.1.42 shell	1-44
1.1.43 speed	1-45
1.1.44 stopbits	1-46
1.1.45 telnet	1-46
1.1.46 telnet client source	1-47
1.1.47 telnet ipv6	1-48
1.1.48 telnet server acl	1-49
1.1.49 telnet server acl-deny-log enable	1-50
1.1.50 telnet server dscp	1-51
1.1.51 telnet server enable	1-51
1.1.52 telnet server ipv6 acl	1-52
1.1.53 telnet server ipv6 dscp	1-53
1.1.54 terminal type	1-54
1.1.55 user-interface	1-55
1.1.56 user-interface class	1-55
1.1.57 user-role	1-57
1.1.58 web captcha	1-58
1.1.59 web https-authorization mode	1-59
1.1.60 web idle-timeout	1-60
1.1.61 webui log	1-60

1 登录设备



说明

设备运行于 FIPS 模式时，本特性部分配置相对于非 FIPS 模式有所变化，具体差异请见本文相关描述。有关 FIPS 模式的详细介绍请参见“安全配置指导”中的“FIPS”。

1.1 登录设备命令

对于同时支持用户线视图和用户线类视图的命令，本文中的命令描述只描述用户线视图下命令的作用，对于用户线类视图下该命令的作用，请按照下列规则进行类推：

- 用户线视图下的配置优先于用户线类视图下的配置。
- 用户线视图下的配置只对该用户线生效。
- 用户线视图下的属性配置为缺省值时，将采用用户线类视图下配置的值。如果用户线类视图下的属性配置也为缺省值时，则直接采用该属性的缺省值。

1.1.1 activation-key

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。

【命令】

activation-key *key-string*

undo activation-key

【缺省情况】

按<Enter>键启动终端会话。

【视图】

用户线视图

用户线类视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

key-string: 定义启动终端会话的快捷键，可以是区分大小写的单个字符，也可以是单个字符或组合键对应的ASCII码（0~127）。比如设置**activation-key 1**，此时生效快捷键为Ctrl+A；如果设置**activation-key a**，生效的快捷键为a。单个字符的快捷键对应的ASCII码与标准的ASCII码表一致，组合键对应的ASCII码请参见 [表 1-1](#)。

【使用指导】

VTY 用户线视图/VTY 用户线类视图不支持该命令。

在用户线/用户线类视图下，该命令的配置结果将立即生效。

如果使用 **activation-key** 命令设置了其他快捷键，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。

如果用户线视图下配置 **activation-key** 为缺省值，并且此时用户线类视图下配置了 **activation-key**，则用户线类视图下的配置生效；如果用户线类视图下未配置，则生效的为缺省值。

表1-1 Ctrl+X 组合键对应的 ASCII 码表

Ctrl+X 组合键	对应的 ASCII 码
CTRL+A	1
CTRL+B	2
CTRL+C	3
CTRL+D	4
CTRL+E	5
CTRL+F	6
CTRL+G	7
CTRL+H	8
CTRL+I	9
CTRL+J	10
CTRL+K	11
CTRL+L	12
CTRL+M	13
CTRL+N	14
CTRL+O	15
CTRL+P	16
CTRL+Q	17
CTRL+R	18
CTRL+S	19
CTRL+T	20
CTRL+U	21
CTRL+V	22
CTRL+W	23
CTRL+X	24
CTRL+Y	25
CTRL+Z	26

【举例】

指定启动 AUX 用户线终端会话的快捷键为<s>。

```
<Sysname> system-view
[Sysname] line aux 0
[Sysname-line-aux0] activation-key s
```

验证过程如下：

- 退出终端会话。

```
[Sysname-line-aux0] return
<Sysname> quit
```

- 重新使用登录设备，能看到如下显示信息。

Press ENTER to get started.

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

```
<Sysname>
```

1.1.2 authentication-mode

authentication-mode 命令用来设置用户登录设备时的认证方式。

undo authentication-mode 命令用来恢复缺省情况。

【命令】

非 FIPS 模式下：

authentication-mode { none | password | scheme }

undo authentication-mode

FIPS 模式下：

authentication-mode scheme

undo authentication-mode

【缺省情况】

非 FIPS 模式下，对于 LSXM1SUPD3 主控板，使用 AUX 用户线和 VTY 用户线登录的用户的认证方式为 password，使用 Console 用户线登录的用户不需要认证；对于其他主控板，使用 VTY 用户线登录的用户的认证方式为 password，使用 AUX 用户线登录的用户不需要认证。

FIPS 模式下，登录设备时的认证方式为 scheme。

【视图】

用户线视图

用户线类视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

none: 不进行认证。

password: 进行密码认证方式。

scheme: 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”。

【使用指导】

当认证方式设置为 **none** 时，用户不需要输入用户名和密码，就可以使用该用户线登录设备，存在安全隐患，请谨慎配置。

用户线视图下，**authentication-mode** 与 **protocol inbound** 相关联：

- 当这两条命令均配置为缺省值，此时该用户线视图下的这两条命令配置值均取该类用户线类视图下的相应的配置；若该类用户线类视图下没有进行相应的配置，则均取缺省值。
- 当两条命令中的任意一条配置了非缺省值，那么另外一条取缺省值。
- 当两条命令都配置成非缺省值，则均取用户线下的配置值。

仅具有 **network-admin**、**mdc-admin** 或者 **level-15** 用户角色的用户可以执行该命令。其他角色的用户，即使授权了该命令的操作权限，也不能执行该命令。

在用户线视图/用户线类视图下，该命令的配置结果将在下次登录设备时生效。

【举例】

设置用户使用 VTY 0 用户线登录设备时，不需要认证。

```
<Sysname> system-view
[Sysname] line vty 0
[Sysname-line-vty0] authentication-mode none
```

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

```
<Sysname> system-view
[Sysname] line vty 0
[Sysname-line-vty0] authentication-mode password
[Sysname-line-vty0] set authentication password simple 321
```

设置用户使用 VTY 0 用户线，采用 Telnet 方式登录设备时采用本地 AAA 认证，用户名为 123，认证密码为 321，服务类型为 Telnet，用户角色为 **network-admin**。

```
<Sysname> system-view
[Sysname] line vty 0
[Sysname-line-vty0] authentication-mode scheme
[Sysname-line-vty0] quit
[Sysname] local-user 123
[Sysname-luser-manage-123] password simple 321
[Sysname-luser-manage-123] service-type telnet
[Sysname-luser-manage-123] authorization-attribute user-role network-admin
```

【相关命令】

- **set authentication password**

1.1.3 auto-execute command

auto-execute command 命令用来设置自动执行命令。

undo auto-execute command 命令用来恢复缺省情况。

【命令】

auto-execute command *command*

undo auto-execute command

【缺省情况】

未配置自动执行命令。

【视图】

用户线视图

用户线类视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

command: 需要自动执行的某条命令。

【使用指导】



注意

- 在配置 **auto-execute command** 命令之前，请确保可以通过其他用户线（例如 AUX 用户线）登录系统，以便出现问题后，能删除该配置。
- 执行该命令后，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。

用户在登录时设备会自动执行 **auto-execute command** 配置好的命令，执行完命令后，自动断开用户连接。

在用户线视图/用户线类视图下配置该命令时，需要注意：

- Console 用户线视图/Console 用户线类视图不支持该命令。
- AUX 用户线视图/AUX 用户线类视图不支持该命令。
- 如果用户线视图下配置 **auto-execute command** 为缺省值，并且此时用户线类视图下配置了 **auto-execute command**，那么用户线类视图下的配置生效；如果用户线类视图下未配置，则用户线视图下的配置生效。

使用该命令设置的自动执行命令将在下次登录设备时生效。

【举例】

配置用户从 VTY0 登录本设备(IP 地址为 192.168.1.40)后,自动 Telnet 到 IP 地址为 192.168.1.41 的设备。

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

结果验证：

重新 Telnet 登录到本设备，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) 2004-2016 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) 2004-2016 Hangzhou H3C Tech. Co., Ltd. All rights reserved. *
* Without the owner's prior written consent, *
* no decompiling or reverse-engineering shall be allowed. *
*****
```

<Sysname>

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 command accounting

command accounting 命令用来开启命令行计费功能。

undo command accounting 命令用来关闭命令行计费功能。

【命令】

command accounting

undo command accounting

【缺省情况】

命令行计费功能处于关闭状态，即计费服务器不会记录用户执行的命令行。

【视图】

用户线视图

用户线类视图

【缺省用户角色】

network-admin

mdc-admin

【使用指导】

开启命令行计费功能后，如果未配置命令行授权功能，则当前用户执行的每一条合法命令都会发送到 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。

在用户线视图/用户线类视图下，该命令的配置结果将在下次登录设备时生效。

如果在用户线类视图下使用 **command accounting** 命令使能了命令行计费功能，则该类型用户线视图都使能命令行计费功能，且用户线视图下无法使用 **undo command accounting** 恢复缺省情况。

【举例】

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

```
<Sysname> system-view
[Sysname] line vty 0
[Sysname-line-vty0] command accounting
```

【相关命令】

- **accounting command**（安全命令参考/AAA）
- **command authorization**

1.1.5 command authorization

command authorization 命令用来开启命令行授权功能。

undo command authorization 命令用来关闭命令行授权功能。

【命令】

command authorization
undo command authorization

【缺省情况】

命令行授权功能处于关闭状态，即用户登录后执行命令行不需要服务器授权。

【视图】

用户线视图
用户线类视图

【缺省用户角色】

network-admin
mdc-admin

【使用指导】

开启命令行授权功能后，使用该用户线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。

在用户线视图/用户线类视图下该命令的配置结果将在下次登录设备时生效。

如果在用户线类视图下使用 **command authorization** 命令开启了命令行授权功能，则该类型用户线视图都开启命令行授权功能，且用户线视图下无法使用 **undo command authorization** 恢复缺省情况。

【举例】

设置用户使用 VTY 0 用户线登录设备时，需要服务器授权才能执行命令。

```
<Sysname> system-view
[Sysname] line vty 0
[Sysname-line-vty0] command authorization
```

【相关命令】

- **command accounting**
- **authorization command**（安全命令参考/AAA）

1.1.6 databits

databits 命令用来设置数据位的个数。

undo databits 命令用来恢复缺省情况。

【命令】

databits { 5 | 6 | 7 | 8 }

undo databits

【缺省情况】

用户线的数据位为 8 位。

【视图】

用户线视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

5: 数据位为 5 位，即使用 5 比特来表示一个字符。

6: 数据位为 6 位，即使用 6 比特来表示一个字符。

7: 数据位为 7 位，即使用 7 比特来表示一个字符。

8: 数据位为 8 位，即使用 8 比特来表示一个字符。

【使用指导】

VTY 用户线类视图不支持该命令。

目前暂不支持配置数据位为 **5** 和 **6**。

访问终端和设备相应用户线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 7 位。

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

```
[Sysname] line aux 0
```

```
[Sysname-line-aux0] databits 7
```

1.1.7 display ip http

display ip http 命令用来显示 HTTP 的状态信息。

【命令】

display ip http

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator
mdc-admin
mdc-operator

【举例】

```
# 显示 HTTP 的状态信息。  
<Sysname> display ip http  
HTTP port: 80  
Basic ACL: 2222  
HTTP status: Enabled
```

表1-2 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
Basic ACL	与HTTP服务关联的基本访问控制列表号，0表示未配置
HTTP status	HTTP服务是否开启： Enabled: 表示HTTP服务处于开启状态 Disabled: 表示HTTP服务处于关闭状态

【相关命令】

- **ip http port**
- **ip http acl**
- **ip http enable**

1.1.8 display ip https

display ip https 命令用来显示 HTTPS 的状态信息。

【命令】

display ip https

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
mdc-admin
mdc-operator

【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: Not configured
Basic ACL: 2222
HTTPS status: Enabled

```

表1-3 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
SSL server policy	与HTTPS服务关联的SSL服务器端策略，Not configured表示未配置
Certificate access-control-policy	与HTTPS服务关联的证书属性访问控制策略，Not configured表示未配置
Basic ACL	与HTTPS服务关联的基本访问控制列表号，0表示未配置
HTTPS status	HTTPS服务是否开启： Enabled: 表示HTTPS服务处于开启状态 Disabled: 表示HTTPS服务处于关闭状态

【相关命令】

- **ip https port**
- **ip https acl**
- **ip https enable**
- **ip https ssl-server-policy**
- **ip https certificate access-control-policy**

1.1.9 display line

display line 命令用来显示用户线的相关信息。

【命令】

display line [*number1* | { **aux** | **console** | **vty** } *number2*] [**summary**]

【视图】

任意视图

【缺省用户角色】

```

network-admin
network-operator
mdc-admin
mdc-operator

```

【参数】

number1: 用户线的编号（绝对编号方式），独立运行模式下，*number1*的取值范围为0~73，IRF模式下，*number1*的取值范围为0~6453。

aux: AUX 用户线。

console: Console 用户线。仅LSXM1SUPD3主控板支持该用户线。

vty: VTY 用户线。

number2: 用户线的编号（相对编号方式）。

summary: 显示用户线的摘要信息。不使用该参数时，将显示用户线类型、绝对/相对编号、传输速率、认证方式及接入接口；使用该参数时，将显示正在使用和未使用的用户线数目和类型。

【举例】

显示用户线 0 的相关信息。

```
<Sysname> display line 0
  Idx  Type      Tx/Rx      Modem Auth  Int          Location
F 0    AUX 0      9600      -    N    -           1/0

+      : Line is active.
F      : Line is active and in async mode.
Idx    : Absolute index of line.
Type   : Type and relative index of line.
Auth   : Login authentication mode.
Int    : Physical port of the line.
A      : Authentication use AAA.
N      : No authentication is required.
P      : Password authentication.
```

表1-4 display line 命令显示信息描述表

字段	描述
+	表示当前正在使用的用户线
F	表示当前正在使用的用户线，且工作在异步方式
Idx	用户线的绝对编号
Type	用户线的类型及相对编号
Tx/Rx	用户线的速率
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“-”（表示未配置）
Auth	使用该用户线登录的用户的认证方式，取值有A、L、N和P四种方式
Int	用户线对应的物理接口的简称表示（Console口以及没有对应接口的用户线均显示“-”）
Location	用户线的物理位置，显示为“槽位号/CPU编号”（独立运行模式） 用户线的物理位置，显示为“设备成员编号/槽位号/CPU编号”（IRF模式）
A	表示使用AAA认证方式，对应的 authentication-mode 为 scheme
N	表示无需认证，对应的 authentication-mode 为 none
P	表示使用当前用户线的密码进行认证，对应的 authentication-mode 为 password

显示所有用户线的摘要信息。

```
<Sysname> display line summary
  Line type : [AUX]
            0:XXXX XXXX XX
```

```

Line type : [VTY]
      10:UUXX XXXX XXXX XXXX
      26:XXXX XXXX XXXX XXXX
      42:XXXX XXXX XXXX XXXX
      58:XXXX XXXX XXXX XXXX

```

```

2 lines used.      (U)
72 lines not used. (X)

```

表1-5 display line summary 命令显示信息描述表

字段	描述
Line type	用户线类型： <ul style="list-style-type: none"> • CON 表示 Console 用户线 • AUX 表示 AUX 用户线 • VTY 表示 VTY 用户线
0:UXXX XXXX XX	0表示用户线的绝对编号 X表示当前没有用户使用该用户线 U表示当前有用户使用该用户线
lines used. (U)	当前正在使用的用户线的数目（即U字符数量）
lines not used. (X)	当前未使用的用户线的数目（即X字符数量）

1.1.10 display telnet client

display telnet client 命令用来显示设备作为 Telnet 客户端的配置信息。

【命令】

display telnet client

【视图】

任意视图

【缺省用户角色】

```

network-admin
network-operator
mdc-admin
mdc-operator

```

【使用指导】

目前该命令显示的是 Telnet 客户端源 IPv4 地址或源接口的配置信息。用户可以使用 **telnet client source** 命令指定 Telnet 客户端源 IPv4 地址或源接口。

【举例】

显示设备作为 Telnet 客户端的相关配置信息。

```
<Sysname> display telnet client
```

The source IP address is 1.1.1.1.

以上显示信息表示设备作为 Telnet 客户端时，发送 Telnet 报文的源 IPv4 地址为 1.1.1.1。

【相关命令】

- **telnet client source**

1.1.11 display user-interface

display user-interface 命令用来显示用户线的相关信息。

【命令】

display user-interface [*number1* | { **aux** | **console** | **vty** } *number2*] [**summary**]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
mdc-admin
mdc-operator

【参数】

number1: 用户线的编号（绝对编号方式），独立运行模式下，*number1* 的取值范围为 0~73；IRF 模式下，*number1* 的取值范围为 0~6453。

aux: AUX 用户线。

console: Console 用户线。仅 LSXM1SUPD3 主控板支持该用户线。

vty: VTY 用户线。

number2: 用户线的编号（相对编号方式）。

summary: 显示用户线的摘要信息。不使用该参数时，将显示用户线类型、绝对/相对编号、传输速率、认证方式及接入接口；使用该参数时，将显示正在使用和未使用的用户线数目和类型。

【使用指导】

该命令实现与 **display line** 一致，仅为与旧版本兼容保留，请使用 **display line**。

【举例】

显示用户线 0 的相关信息。

```
<Sysname> display user-interface 0
  Idx  Type    Tx/Rx    Modem Auth  Int      Location
F 0    AUX 0    9600     -    N    -    1/0

+      : Line is active.
F      : Line is active and in async mode.
Idx    : Absolute index of line.
Type   : Type and relative index of line.
Auth   : Login authentication mode.
Int    : Physical port of the line.
```

A : Authentication use AAA.
 N : No authentication is required.
 P : Password authentication.

表1-6 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线
F	表示当前正在使用的用户线，且工作在异步方式
Idx	用户线的绝对编号
Type	用户线的类型及相对编号
Tx/Rx	用户线的速率
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“-”（表示未配置）
Auth	使用该用户线登录的用户的认证方式，取值有A、L、N和P四种方式
Int	用户线对应的物理接口的简称表示（Console口以及没有对应接口的用户线均显示“-”）
Location	用户线的物理位置，显示为“槽位号/CPU编号”（独立运行模式） 用户线的物理位置，显示为“设备成员编号/槽位号/CPU编号”（IRF模式）
A	表示使用AAA认证方式，对应的 authentication-mode 为 scheme
N	表示无需认证，对应的 authentication-mode 为 none
P	表示使用当前用户线的密码进行认证，对应的 authentication-mode 为 password

显示所有用户线的摘要信息。

```
<Sysname> display user-interface summary
  Line type : [AUX]
             0:XXXX XXXX XX
  Line type : [VTY]
             10:UXUX XXXX XXXX XXXX
             26:XXXX XXXX XXXX XXXX
             42:XXXX XXXX XXXX XXXX
             58:XXXX XXXX XXXX XXXX

  2 lines used.      (U)
  72 lines not used. (X)
```

表1-7 display user-interface summary 命令显示信息描述表

字段	描述
Line type	用户线类型： <ul style="list-style-type: none"> • CON 表示 Console 用户线 • AUX 表示 AUX 用户线 • VTY 表示 VTY 用户线

字段	描述
0:UXXX XXXX XX	0表示用户线的绝对编号 X表示当前没有用户使用该用户线 U表示当前有用户使用该用户线
lines used. (U)	当前正在使用的用户线的数目（即U字符数量）
lines not used. (X)	当前未使用的用户线的数目（即X字符数量）

1.1.12 display users

display users 命令用来显示正在使用的用户线以及用户的相关信息。

【命令】

display users [all]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
mdc-admin
mdc-operator

【参数】

all: 显示设备支持的所有用户线以及用户的相关信息。

【举例】

显示正在使用的用户线以及用户的相关信息。

```
<Sysname> display users
  Idx  Line   Idle      Time                Pid   Type
+ 10   VTY 0    00:00:00   Jan 01 00:33:10   484   TEL
  12   VTY 2    00:06:22   Jan 01 00:33:22   495   TEL

Following are more details.
VTY 0   :
        Location: 192.168.1.107
VTY 2   :
        Location: 192.168.1.134
+       : Current operation user.
F       : Current operation user works in async mode.
```

表1-8 display users 命令显示信息描述表

字段	描述
Idx	用户线的绝对编号

字段	描述
Line	用户线的相对编号，第一列（例如VTY）表示用户线的类型，第二列（例如0）表示用户线的相对编号
Idle	空闲时间，表明用户和设备没有报文交互的时间长度，格式为hh:mm:ss。当空闲时间大于等于24小时时，显示为old
Time	用户本次登录的时间
Pid	用户对应的进程ID（CLI用户登录时，系统会自动运行一个用户登录进程来监控用户的操作）
Type	显示用户的登录方式： <ul style="list-style-type: none"> • TEL 表示用户通过 Telnet 方式登录设备 • SSH 表示用户通过 SSH 方式登录设备 • Switchto User 表示用户通过 MDC 的 switchto 命令方式登录设备 • 无显示信息表示用户通过 Console 口、USB Console 口方式登录设备
+	当前操作用户
Location	使用该用户线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

1.1.13 display web menu

display web menu 命令用来显示 Web 的页面菜单树。

【命令】

display web menu [chinese]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
mdc-admin
mdc-operator

【参数】

chinese: 显示 Web 的页面中文菜单树。不指定该参数时，显示 Web 的页面英文菜单树。

【使用指导】

配置用户角色对应的 Web 菜单项时，可以使用该命令查看系统支持的全部菜单树。

【举例】

```
# 显示全部 Web 菜单信息。
<Sysname> display web menu
.
|--Dashboard: ID = m_dashboard
```

```

|--Device: ID = m_device
|
|  |--Maintenance: ID = m_maintenance
|  |
|  |  |--Settings: ID = m_devicesettings
|  |  |
|  |  |--Administrators: ID = m_admin
|  |  |
|  |  |--Configuration: ID = m_config
|  |  |
|  |  |--Upgrade: ID = m_upgrade
|  |  |
|  |  |--Diagnostics: ID = m_diagnostic
|  |  |
|  |  |--Reboot: ID = m_reboot
|  |  |
|  |  `--About: ID = m_about
|  |
|  `--Virtualization: ID = m_virtualdevice
|  |
|  |  `--IRF: ID = m_irf
|
|--Network: ID = m_network
|
|  |--Interfaces: ID = m_if
|  |
|  |  |--Interfaces: ID = m_interface
|  |  |
|  |  |--Link Aggregation: ID = m_lagg
|  |  |
|  |  |--Storm Constrain: ID = m_stormconstrain
|  |  |
|  |  `--Isolation: ID = m_isolation
|  |
|--Links: ID = m_link
|  |
|  |  |--VLAN: ID = m_vlan
|  |  |
|  |  |--MAC: ID = m_mac
|  |  |
|  |  |--STP: ID = m_stp
|  |  |
|  |  |--LLDP: ID = m_lldp
|  |  |
|  |  `--DHCP Snooping: ID = m_dhcpsnooping
|  |
|--IP: ID = m_ip
|  |
|  |  |--IP: ID = m_ip
|  |  |
|  |  |--ARP: ID = m_arp
|  |  |
|  |  |--DNS: ID = m_dns
|  |  |
|  |  `--Dynamic DNS: ID = m_ddns
|  |
|--IPv6: ID = m_ipv6
|  |
|  |  |--IPv6: ID = m_ipv6
|  |  |
|  |  |--ND: ID = m_nd
|  |  |
|  |  `--DNS: ID = m_ipv6dns
|  |
|--Mirroring: ID = m_mirror
|  |
|  |  `--Port Mirroring: ID = m_portmirror
|  |
|--Routing: ID = m_routing
|  |
|  |  |--Routing Table: ID = m_routingtable
|  |  |
|  |  |--Static Routing: ID = m_staticrouting
|  |  |
|  |  |--RIP: ID = m_rip
|  |  |
|  |  `--Policy-Based Routing: ID = m_pbr
|  |
|--Multicast: ID = m_multicast
|  |
|  |  |--IGMP Snooping: ID = m_igmpsnooping
|  |  |
|  |  `--MLD Snooping: ID = m_mldsnooping
|  |
`--Service: ID = m_ipservice
|  |
|  |  |--DHCP: ID = m_dhcp
|  |  |
|  |  |--HTTP/HTTPS: ID = m_http
|  |  |
|  |  |--FTP: ID = m_ftp
|  |  |
|  |  |--Telnet: ID = m_telnet
|  |  |
|  |  `--NTP: ID = m_ntp

```

```

|--Resources: ID = m_resource
|   |--ACLs: ID = m_acl
|   |   |--IPv4: ID = m_ipv4acl
|   |   |--IPv6: ID = m_ipv6acl
|   |   |--Ethernet: ID = m_macacl
|   |   |--User-Defined: ID = m_useracl
|   |--Time Range: ID = m_timerange
|       |--Time Range: ID = m_timerange
|--QoS: ID = m_qos
|   |--QoS: ID = m_qos
|       |--QoS Policies: ID = m_mqc
|       |--Hardware Queuing: ID = m_hardqueue
|       |--Priority Mapping: ID = m_priority
|       |--Rate Limit: ID = m_linerate
|--Security: ID = m_security
|   |--Packet Filter: ID = m_packetfilter
|   |   |--Packet Filter: ID = m_packetfilter
|   |--Access Control: ID = m_access
|   |   |--802.1X: ID = m_8021x
|   |--Authentication: ID = m_authentication
|       |--ISP Domains: ID = m_ispdomain
|       |--RADIUS: ID = m_radius
|       |--Local Users: ID = m_localuser
|--PoE: ID = m_poe
|   |--PoE: ID = m_poe
|   |--PoE: ID = m_poe
|--Log: ID = m_log
|   |--Log: ID = m_log
|       |--System Log: ID = m_syslog
|       |--Settings: ID = m_logsettings

```

1.1.14 display web users

display web users 命令用来显示 Web 用户的相关信息。

【命令】

display web users

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
mdc-admin
mdc-operator

【举例】

显示当前 Web 用户的相关信息。

```
<Sysname> display web users
```

UserID	Name	Type	Language	JobCount	LoginTime	LastOperation
AB2039483271293	Administrator	HTTP	Chinese	3	12:00:23	14:10:05
F09382BA2014AC8	user	HTTPS	English	1	13:05:00	14:11:00

表1-9 display web users 命令显示信息描述表

字段	描述
UserID	Web用户的ID号，用来唯一标识一个登录用户
Name	Web用户的登录用户名
Type	Web用户登录使用的协议类型： <ul style="list-style-type: none">• HTTP 表示 Hypertext Transfer Protocol• HTTPS 表示基于安全套接字的 Hypertext Transfer Protocol
Language	Web用户登录时使用的语言： <ul style="list-style-type: none">• Chinese 表示中文• English 表示英文
JobCount	Web用户建立的连接数量
LoginTime	Web用户的登录时间
LastOperation	Web用户的最后操作时间

1.1.15 escape-key

escape-key 命令用来配置终止运行任务（比如 **ping** 命令等）的快捷键。

undo escape-key 命令用来取消快捷键的配置，包括缺省快捷键。

【命令】

```
escape-key { key-string | default }
```

```
undo escape-key
```

【缺省情况】

按<Ctrl+C>组合键终止运行的任务。

【视图】

用户线视图

用户线类视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

key-string: 定义终止运行任务的快捷键，可以是区分大小写的单个字符（字符“d”和“D”除外），也可以是单个字符或组合键对应的ASCII码（0~127）。比如设置**escape-key 1**，此时生效快捷键为Ctrl+A；如果设置**escape-key a**，生效的快捷键为a。配置字符“d”和“D”作为终止运行任务

的快捷键时系统不会生效，此时<Ctrl+C>为实际的生效快捷键。如确实需要使用字符“d”和“D”作为终止运行任务的快捷键，可以配置`key-string`为字符“d”和“D”对应的ASCII码。单个字符的快捷键对应的ASCII码与标准的ASCII码表一致，组合键对应的ASCII码请参见 [表 1-1](#)。

default: 恢复为缺省的快捷键<Ctrl+C>。

【使用指导】

用户可以按<Ctrl+C>组合键来终止 ping、tracert 等正在执行的任务，以便输入新的命令。如果配置了 `escape-key`，则用户可以用新配置的快捷键来代替<Ctrl+C>。命令行是否支持<Ctrl+C>终止与功能模块的软件实现有关，请参见相关命令行的描述。

如果设置的快捷键为单个字符，且有任务可终止，则输入快捷键会终止命令的执行；如果没有任务可终止，则输入的快捷键会作为普通的编辑字符。

如果在 Device A 某用户线下设置了单个字符 `key-string` 为任务终止快捷键，当使用该用户线登录到 Device A，又通过 Device A 以 telnet 方式到 Device B，这时的 `key-string` 在 Device B 上将被视为编辑字符进行输入。如果 telnet 到 Device B 时所使用的用户线下配置了相同的 `key-string`，此时 `key-string` 在有任务运行时可以中止任务。

新设置的快捷键可以使用 `display current-configuration | include escape-key` 命令来查看。

如果用户线视图下配置 `escape-key` 为缺省值，并且此时用户线类视图下配置了 `escape-key`，则用户线类视图下的配置生效；如果用户线类视图下未配置，则生效的为缺省值。

用户线视图下使用本命令配置的快捷键立即生效；用户线类视图下配置的快捷键将在下次登录时生效。

【举例】

配置 VTY0 终止运行任务的快捷键为 a。

```
<Sysname> system-view
[Sysname] line vty 0
[Sysname-line-vty0] 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>
```

1.1.16 flow-control

`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。

【命令】

```
flow-control { hardware | none | software }  
undo flow-control
```

【缺省情况】

没有配置流量控制方式。

【视图】

用户线视图

【缺省用户角色】

```
network-admin  
mdc-admin
```

【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。

【使用指导】

VTY 用户线视图不支持该命令。

流量控制分为入方向和出方向，入方向表示本设备能够接受远端设备的流量控制，出方向表示本设备能够对远端设备进行流量控制。配置该命令后，流量控制方式对入方向和出方向都生效。

要使流量控制生效，双方才能正常通信，对端设备也要配置相同的流量控制方式。

【举例】

配置 AUX 0 用户线视图下，入方向和出方向都采用软件流量控制方式。

```
<Sysname> system-view  
[Sysname] line aux 0  
[Sysname-line-aux0] flow-control software
```

1.1.17 free line

free line 命令用来释放用户线上建立的连接。

【命令】

```
free line { number1 | { aux | console | vty } number2 }
```

【视图】

用户视图

【缺省用户角色】

```
network-admin  
mdc-admin
```

【参数】

number1: 用户线的编号（绝对编号方式）。独立运行模式下，**number1**的取值范围为0~73；IRF模式下，**number1**的取值范围为0~6453。

aux: AUX 用户线。

console: Console 用户线。仅 LSXM1SUPD3 主控板支持该用户线。

vty: VTY 用户线。

number2: 用户线的编号（相对编号方式）。对于 AUX 用户线：独立运行模式下，**number2**的取值范围为0~9。IRF 模式下，**number2**的取值范围为0~6389；对于 VTY 用户线：**number2**的取值范围为0~63。

【使用指导】

用户不能使用该命令释放自己的连接。

【举例】

释放用户线上 VTY 1 建立的连接。

```
<Sysname> free line vty 1
Are you sure to free line vty1? [Y/N]:y
[OK]
```

1.1.18 free user-interface

free user-interface 命令用来释放用户线上建立的连接。

【命令】

```
free user-interface { number1 | { aux | console | vty } number2 }
```

【视图】

用户视图

【缺省用户角色】

```
network-admin
mdc-admin
```

【参数】

number1: 用户线的编号（绝对编号方式）。独立运行模式下，**number1**的取值范围为0~73；IRF模式下，**number1**的取值范围为0~6453。

aux: AUX 用户线。

console: Console 用户线。仅 LSXM1SUPD3 主控板支持该用户线。

vty: VTY 用户线。

number2: 用户线的编号（相对编号方式）。

【使用指导】

用户不能使用该命令释放自己的连接。

该命令实现与 **free line** 一致，仅为与旧版本兼容保留，请使用 **free line**。

【举例】

```
# 释放用户线上 VTY 1 建立的连接。
<Sysname> free user-interface vty 1
Are you sure to free line vty1? [Y/N]:y
[OK]
```

1.1.19 free web users

free web users 命令用来强制在线 Web 用户下线。

【命令】

```
free web users { all | user-id user-id | user-name user-name }
```

【视图】

用户视图

【缺省用户角色】

```
network-admin
mdc-admin
```

【参数】

all: 所有 Web 用户。

user-id: Web 用户的 ID 号，为 15 位十六进制数。系统会自动为每位成功登录的 Web 用户分配一个用户 ID，用户 ID 用于唯一标识 Web 用户。

user-name *user-name*: Web 用户的用户名，为 1~255 个字符的字符串，区分大小写。

【举例】

```
# 强制所有在线 Web 用户下线。
<Sysname> free web users all
```

【相关命令】

- **display web users**

1.1.20 history-command max-size

history-command max-size 命令用来设置可以存储的当前用户线下历史命令的条数。

undo history-command max-size 命令用来恢复缺省情况。

【命令】

```
history-command max-size size-value
undo history-command max-size
```

【缺省情况】

历史命令缓冲区可存储 10 条历史命令。

【视图】

用户线视图
用户线类视图

【缺省用户角色】

network-admin
mdc-admin

【参数】

size-value: 可存储的历史命令的条数，取值范围为 0~256。

【使用指导】

每个用户线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“基础配置命令参考”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。

如果用户线视图下配置 **history-command max-size** 为缺省值，并且此时用户线类视图下配置了 **history-command max-size**，那么用户线视图下的生效配置值为用户线类视图下的配置；如果用户线类视图下未配置，则生效的为缺省值。

在用户线视图下使用本命令配置的当前用户线下可存储的历史命令条数立即生效；用户线类视图下配置的可存储的历史命令条数将在下次登录时生效。

【举例】

设置 VTY0 用户线下历史命令缓冲区最多可以存储 20 条历史命令。

```
<Sysname> system-view  
[Sysname] line vty 0  
[Sysname-line-VTY0] history-command max-size 20
```

1.1.21 idle-timeout

idle-timeout 命令用来设置用户连接的超时时间。

undo idle-timeout 命令用来恢复缺省情况。

【命令】

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

【缺省情况】

超时时间为 10 分钟。

【视图】

用户线视图
用户线类视图

【缺省用户角色】

network-admin
mdc-admin

【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。

【使用指导】

用户登录后，如果在超时时间内设备和用户间没有消息交互，则超时时间到达时设备会自动断开用户连接。

当超时时间设置为 0 时，表示设备不会因为超时自动断开用户连接。

如果用户线视图下配置 **idle-timeout** 为缺省值，并且此时用户线类视图下配置了 **idle-timeout**，那么用户线视图下的生效配置值为用户线类视图下的配置；如果用户线类视图下未配置，则生效的为缺省值。

用户线视图下使用本命令配置的连接超时时间立即生效；用户线类视图下配置的连接超时时间将在下次登录时生效。

【举例】

设置 VTY0 用户线下用户连接超时时间为 1 分钟 30 秒。

```
<Sysname> system-view
[Sysname] line vty 0
[Sysname-line-VTY0] idle-timeout 1 30
```

1.1.22 ip http acl

ip http acl 命令用来配置 HTTP 服务与 ACL 关联。

undo ip http acl 命令用来恢复缺省情况。

【命令】

```
ip http acl { acl-number | name acl-name }
undo ip http acl
```

【缺省情况】

HTTP 服务没有与 ACL 关联。

【视图】

系统视图

【缺省用户角色】

```
network-admin
mdc-admin
```

【参数】

acl-number: ACL 的编号，取值范围为 2000~2999（基本 IPv4 ACL）。

name acl-name: 指定 ACL 的名称。**acl-name** 表示 ACL 的名称，为 1~63 个字符的字符串，不区分大小写，必须以英文字母 a~z 或 A~Z 开头。为避免混淆，ACL 的名称不允许使用英文单词 **all**。仅当指定名称的 ACL 存在且为基本 IPv4 ACL 时生效。

【使用指导】

FIPS 模式下，不支持本命令。

多次执行该命令最新配置生效。

配置 HTTP 服务与 ACL 关联后，只有 ACL 允许通过的 HTTP 客户端能够通过 Web 方式登录设备。
不匹配 ACL 或 ACL 拒绝通过的 HTTP 客户端将不能通过 Web 方式登录设备。

【举例】

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 basic 2001
[Sysname-acl-ipv4-basic-2001] rule permit source 10.10.0.0 0.0.255.255
[Sysname-acl-ipv4-basic-2001] quit
[Sysname] ip http acl 2001
```

【相关命令】

- **acl** (ACL 和 QoS 命令参考/ACL)

1.1.23 ip http enable

ip http enable 命令用来开启 HTTP 服务。

undo ip http enable 命令用来关闭 HTTP 服务。

【命令】

ip http enable

undo ip http enable

【缺省情况】

HTTP 服务处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

mdc-admin

【使用指导】

FIPS 模式下，不支持本命令。

开启 HTTP 服务后，用户才能通过 Web 使用 HTTP 方式登录设备。

开启 HTTP 服务后，为了增强设备的安全性，HTTPS 服务的端口号也会被自动打开，且在 HTTP 服务开启的状态下无法通过 **undo ip https enable** 命令关闭。

【举例】

使能 HTTP 服务。

```
<Sysname> system-view
[Sysname] ip http enable
```

【相关命令】

- **ip https enable**

1.1.24 ip http port

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。

【命令】

ip http port *port-number*

undo ip http port

【缺省情况】

HTTP 服务的端口号为 80。

【视图】

系统视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

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

【使用指导】

FIPS 模式下，不支持本命令。

如果修改端口号前 HTTP 服务是开启的，则修改端口号后系统会自动重启 HTTP 服务，正在访问的用户将被断开，用户需要在浏览器的地址栏中重新输入新的地址后才可以继续访问。

【举例】

配置 HTTP 服务的端口号为 80。

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

```
[Sysname] ip http port 80
```

1.1.25 ip https acl

ip https acl 命令用来配置 HTTPS 服务与 ACL 关联。

undo ip https acl 命令用来恢复缺省情况。

【命令】

ip https acl {*acl-number* | **name** *acl-name*}

undo ip https acl

【缺省情况】

HTTPS 服务未与 ACL 关联。

【视图】

系统视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

acl-number: ACL 的编号，取值范围为 2000~2999（基本 IPv4 ACL）。

name acl-name: 指定 ACL 的名称。**acl-name** 表示 ACL 的名称，为 1~63 个字符的字符串，不区分大小写，必须以英文字母 a~z 或 A~Z 开头。为避免混淆，ACL 的名称不允许使用英文单词 **all**。仅当指定名称的 ACL 存在且为基本 IPv4 ACL 时生效。

【使用指导】

配置 HTTPS 服务与 ACL 关联后，只有 ACL 允许通过的 HTTPS 客户端能够通过 Web 方式登录设备。不匹配 ACL 或 ACL 拒绝通过的 HTTPS 客户端将不能通过 Web 方式登录设备。

需要注意的是，Web 登录时用户输入的用户名和密码属于敏感信息，Web 登录请求采用 HTTPS 方式发送到 Web 服务器。所以，如果本命令中的 ACL 规则拒绝客户端通过 HTTPS 服务访问 Web 页面，那么该客户端也无法通过 HTTP 服务访问 Web 页面。

多次执行该命令最新配置生效。

【举例】

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 basic 2001
[Sysname-acl-ipv4-basic-2001] rule permit source 10.10.0.0 0.0.255.255
[Sysname-acl-ipv4-basic-2001] quit
[Sysname] ip https acl 2001
```

【相关命令】

- **acl**（ACL 和 QoS 命令参考/ACL）

1.1.26 ip https certificate access-control-policy

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 命令用来恢复缺省情况。

【命令】

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

undo ip https certificate access-control-policy

【缺省情况】

HTTPS 服务未与证书属性访问控制策略关联。

【视图】

系统视图

【缺省用户角色】

network-admin
mdc-admin

【参数】

policy-name: 证书属性访问控制策略名，为 1~31 个字符的字符串，区分大小写。

【使用指导】

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。证书属性访问控制策略的相关介绍请参见“安全配置指导”中“PKI”。

【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
```

【相关命令】

- **pki certificate access-control-policy**（PKI 命令参考/PKI）

1.1.27 ip https enable

ip https enable 命令用来开启 HTTPS 服务。

undo ip https enable 命令用来关闭 HTTPS 服务。

【命令】

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

【缺省情况】

HTTPS 服务处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin
mdc-admin

【使用指导】

只有使能该功能后，用户才能通过 Web 方式使用 HTTPS 登录设备。

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。

【举例】

```
# 使能 HTTPS 服务。
```

```
<Sysname> system-view
[Sysname] ip https enable
```

【相关命令】

- **ip https ssl-server-policy**
- **ip https certificate access-control-policy**

1.1.28 ip https port

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。

【命令】

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

```
undo ip https port
```

【缺省情况】

HTTPS 服务的端口号为 443。

【视图】

系统视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

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

【使用指导】

如果修改端口号前 HTTPS 服务是开启的，则修改端口号后系统会自动重启 HTTPS 服务，正在访问的用户将被断开，用户需要在浏览器的地址栏中重新输入新的地址后才可以继续访问。

【举例】

配置 HTTPS 服务的端口号为 8080。

```
<Sysname> system-view
[Sysname] ip https port 8080
```

1.1.29 ip https ssl-server-policy

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 命令用来恢复缺省情况。

【命令】

```
ip https ssl-server-policy policy-name
```

```
undo ip https ssl-server-policy
```

【缺省情况】

HTTPS 服务未与 SSL 服务器端策略关联，HTTPS 使用自签名证书。

【视图】

系统视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

policy-name: SSL 服务器端策略名，为 1~31 个字符的字符串。

【使用指导】

HTTP 服务和 HTTPS 服务处于使能状态时，对与 HTTPS 服务关联的 SSL 服务器端策略进行的修改不会生效。如需修改 HTTPS 服务与 SSL 服务器端的关联策略，首先执行 **undo ip http enable** 和 **undo ip https enable** 两条命令，再执行 **ip https ssl-server-policy *policy-name*** 命令，最后重新使能 HTTP 服务和 HTTPS 服务，新的策略即可生效。

如需恢复缺省情况，必须先执行 **undo ip http enable** 和 **undo ip https enable** 两条命令，再执行 **undo ip https ssl-server-policy**，最后重新使能 HTTP 服务和 HTTPS 服务即可。

【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
```

【相关命令】

- **ssl server-policy**（安全命令参考/SSL）

1.1.30 line

line 命令用来进入一个或多个用户线视图。

【命令】

```
line { first-number1 [ last-number1 ] | { aux | console | vty } first-number2 [ last-number2 ] }
```

【视图】

系统视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

first-number1: 第一个用户线的编号（绝对编号方式）。独立运行模式下，*first-number1* 的取值范围为 0~73；IRF 模式下，*first-number1* 的取值范围为 0~6453。

last-number1: 最后一个用户线的编号（绝对编号方式），该参数不能小于 *first-number1*。

aux: AUX 用户线。

console: Console 用户线。仅 LSXM1SUPD3 主控板支持该用户线。

vty: VTY 用户线。

first-number2: 第一个用户线的编号（相对编号方式）。

last-number2: 最后一个用户线的编号（相对编号方式），该参数不能小于 *first-number2*。

【举例】

进入 VTY 0 用户线视图。

```
<Sysname> system-view
[Sysname] line vty 0
[Sysname-line-VTY0]
```

进入 VTY 0~63 用户线视图。

```
<Sysname> system-view
[Sysname] line vty 0 63
[Sysname-line-vty0-63]
```

【相关命令】

- **line class**

1.1.31 line class

line class 命令用来进入用户线类视图。

【命令】

```
line class { aux | console | vty }
```

【视图】

系统视图

【缺省用户角色】

```
network-admin
mdc-admin
```

【参数】

aux: AUX 用户线类。

console: Console 用户线类。仅 LSXM1SUPD3 主控板支持该用户线类。

vty: VTY 用户线类。

【使用指导】

用户线视图下的配置只对该用户线生效。

用户线类视图下的配置修改不会立即生效，当用户下次登录后所修改的配置值才会生效。

line class 命令用来进入用户线类视图，**line** 命令用来进入一个或多个用户线视图。对于同时支持这两种视图的命令：

- 用户线视图下的配置优先于用户线类视图下的配置。
- 用户线视图下的属性配置为缺省值时，将采用用户线类视图下配置的值。如果用户线类视图下的属性配置也为缺省值时，则直接采用该属性的缺省值。

用户线类视图下支持的命令有：

- **activation-key**
- **auto-execute command**

- **authentication-mode**
- **command accounting**
- **command authorization**
- **escape-key**
- **history-command max-size**
- **idle-timeout**
- **protocol inbound**
- **screen-length**
- **set authentication password**
- **shell**
- **terminal type**
- **user-role**

【举例】

在 VTY 用户线类视图下，将用户连接的超时时间的缺省值设置为 15 分钟。

```
<Sysname> system-view
[Sysname] line class vty
[Sysname-line-class-vty] idle-timeout 15
```

在 AUX 用户线类视图下，将终端会话的快捷键设置为<s>。

```
<Sysname> system-view
[Sysname] line class aux
[Sysname-line-class-AUX] activation-key s
[Sysname-line-class-AUX] quit
```

- 在 AUX 用户线视图下，将终端会话的快捷键设置为缺省值（可以使用 `undo activation-key` 或者直接使用 `activation-key 13` 进行配置）。

```
[Sysname] line aux 0
[Sysname-line-aux0] undo activation-key
```

- 此时生效的快捷键为用户线类视图下的配置，验证过程如下：

- 退出终端会话。

```
[Sysname-line-aux0] return
<Sysname> quit
```

- 重新登录设备，能看到如下显示信息。

```
Press ENTER to get started.
```

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

```
<Sysname>
```

【相关命令】

- **line**

1.1.32 lock

lock 命令用来锁定当前用户线并配置解锁密码，防止未授权的用户操作该用户线。

【命令】

lock

【缺省情况】

系统不会自动锁定当前用户线。

【视图】

用户视图

【缺省用户角色】

network-admin

mdc-admin

【使用指导】

FIPS 模式下，不支持本命令。

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。如果用户线被锁定，用户需要输入解锁密码才能结束锁定，进入系统。

【举例】

锁住当前用户线然后解锁。

```
<Sysname> lock
Please input password<1 to 16> to lock current line:
Password:
Again:
```

```
locked !
```

此时，命令行用户线被锁定。键入回车，并输入正确的密码后，可以解锁。

```
Password:
<Sysname>
```

1.1.33 lock reauthentication

lock reauthentication 命令用来锁定当前用户线并对其进行重新认证。

【命令】

lock reauthentication

【缺省情况】

系统不会对当前用户线进行重新认证。

【视图】

任意视图

【缺省用户角色】

network-admin

mdc-admin

【使用指导】

执行该命令后，当前用户线会被锁定。用户需要输入设备登录密码对当前用户线进行重新认证才能结束锁定，进入系统。如果设备未配置登录密码，用户按回车键后将直接进入系统。

需要注意的是，如果在设备登录后修改了登录设备的认证方式或密码，那么锁定用户线后的解锁过程将使用新配置的认证方式及密码。

【举例】

输入命令锁定当前用户线，并使用设备登录密码重新登录设备。

```
<Sysname> lock reauthentication
```

```
Please press Enter to unlock the screen.
```

按回车键后，提示输入密码对当前用户线进行重新认证并登录设备。

```
Password:
```

<Sysname>

【相关命令】

- **lock-key**

1.1.34 lock-key

lock-key 命令用来配置对当前用户线进行锁定并重新认证的快捷键。

undo lock-key 命令用来恢复缺省情况。

【命令】

lock-key *key-string*

undo lock-key

【缺省情况】

未设置对当前用户线进行锁定并重新认证的快捷键。

【视图】

用户线视图

用户线类视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

key-string: 指定对当前用户线进行重新认证的快捷键。可以是区分大小写的单个字符，也可以是单个字符或组合键对应的ASCII码(0~127)。例如设置**lock-key 1**，则快捷键为Ctrl+A；如设置**lock-key a**，生效的快捷键为a。使用ASCII码设置快捷键时，单个字符对应的ASCII码与标准ASCII码表一致，组合键对应的ASCII码请参照 [表 1-1](#)。

【使用指导】

通常情况下，建议用户使用组合键而不使用单个字符作为快捷键，避免用户在输入命令时输入完快捷键字符后出现锁定，影响正常命令行的输入。用户设置了快捷键之后，可以输入对应的快捷键代替 **lock reauthentication** 命令完成对当前用户线进行锁定并重新认证的操作。

在用户线/用户线类视图下，该命令的配置的快捷键将立即生效。

新设置的快捷键可以使用 **display current-configuration | include lock-key** 命令来查看。

【举例】

配置锁定当前用户线的快捷键为 Ctrl+A。

```
<Sysname> system-view
[Sysname] line vty 0
[Sysname-line-vty0] lock-key 1
[Sysname-line-vty] quit
```

验证过程如下：

- 用户键入 **Ctrl+A** 组合键后，系统锁定当前用户线并切换到重新认证界面：
[Sysname]

Please press Enter to unlock the screen.

- 按回车键后，系统提示输入密码对当前用户线进行重新认证并登录设备。
Password:

[Sysname]

【相关命令】

- **lock reauthentication**

1.1.35 parity

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。

【命令】

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

undo parity

【缺省情况】

设备校验位的校验方式为 **none**，即不进行校验。

【视图】

用户线视图

【缺省用户角色】

network-admin

mdc-admin

【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。

【使用指导】

VTY 用户线视图不支持该命令。

访问终端和设备相应用户线下校验位的设置必须一致，双方才能正常通信。

【举例】

将 AUX 用户线传输校验位设为奇校验。

```
<Sysname> system-view
[Sysname] line aux 0
[Sysname-line-aux0] parity odd
```

1.1.36 protocol inbound

protocol inbound 命令用来指定所在用户线支持的协议。

undo protocol inbound 命令用来恢复缺省情况。

【命令】

非 FIPS 模式下:

protocol inbound { all | ssh | telnet }

undo protocol inbound

FIPS 模式下:

protocol inbound ssh

undo protocol inbound

【缺省情况】

非 FIPS 模式下: 系统支持所有协议。

FIPS 模式下: 系统支持 SSH 协议。

【视图】

VTY 用户线视图

VTY 用户线类视图

【缺省用户角色】

network-admin
mdc-admin

【参数】

all: 支持所有的协议，包括 Telnet、SSH。

ssh: 支持 SSH 协议。

telnet: 支持 Telnet 协议。

【使用指导】

用户线视图下，该命令的配置结果将在下次登录时生效。

如果要配置用户线支持 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。

用户线视图下，对 **authentication-mode** 和 **protocol inbound** 进行关联绑定。

- 当这两条命令均配置为缺省值，此时该用户线视图下的这两条命令配置值均取该类用户线类视图下的相应的配置；若该类用户线类视图下没有进行相应的配置，则均取缺省值。
- 当两条命令中的任意一条配置了非缺省值，那么另外一条取缺省值。当两条命令都配置成非缺省值，则均取用户线下的配置值。

仅具有 **network-admin**、**mdc-admin** 或者 **level-15** 用户角色的用户可以执行该命令。其他角色的用户，即使授权了该命令的操作权限，也不能执行该命令。

【举例】

设置用户线 VTY 0 到 VTY 4 只支持 SSH 协议。

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

设置 VTY 用户线类支持 SSH 协议，认证方式为 **scheme**。同时设置用户线 VTY 0 到 VTY 4 不进行登陆认证，支持所有的协议。

```
<Sysname> system-view
[Sysname] line class vty
[Sysname-line-class-vty] authentication-mode scheme
[Sysname-line-class-vty] protocol inbound ssh
[Sysname-line-class-vty] line vty 0 4
[Sysname-line-vty0-4] authentication-mode none
```

验证过程如下：

- 使用 Telnet 方式登陆，无需认证即可成功登陆。

```
<Client> telnet 192.168.1.241
Trying 192.168.1.241 ...
Press CTRL+K to abort
Connected to 192.168.1.241 ...
```

```
* Copyright (c) 2004-2016 Hangzhou H3C Tech. Co., Ltd. All rights reserved. *
* Without the owner's prior written consent, *
* no decompiling or reverse-engineering shall be allowed. *
*****
```

<Server>

- 查看当前正在使用的用户线以及用户的相关信息，用户线为 **line 0**，则证明该配置下用户线下配置生效。

<Server> display users

Idx	Line	Idle	Time	Pid	Type
+ 50	VTY 0	00:00:00	Jan 17 15:29:27	189	TEL

Following are more details.

```
VTY 0 :
      Location: 192.168.1.186
+    : Current operation user.
F    : Current operation user works in async mode.
```

【相关命令】

- **authentication-mode**

1.1.37 restful http enable

restful http enable 命令用来开启基于 HTTP 的 RESTful 功能。

undo restful http enable 命令用来关闭基于 HTTP 的 RESTful 功能。

【命令】

restful http enable

undo restful http enable

【缺省情况】

基于 HTTP 的 RESTful 功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

mdc-admin

【使用指导】

FIPS 模式下，不支持本命令。

开启该功能后，用户才可以通过 RESTful HTTP 方式登录设备并采用 RESTful API 对设备进行配置和维护。

【举例】

开启基于 HTTP 的 RESTful 功能。

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

```
[Sysname] restful http enable
```

1.1.38 restful https enable

restful https enable 命令用来开启基于 HTTPS 的 RESTful 功能。

undo restful https enable 命令用来关闭基于 HTTPS 的 RESTful 功能。

【命令】

restful https enable

undo restful https enable

【缺省情况】

基于 HTTPS 的 RESTful 功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

mdc-admin

【使用指导】

开启该功能后，用户才可以通过 RESTful HTTPS 方式登录设备并采用 RESTful API 对设备进行配置和维护。

【举例】

开启基于 HTTPS 的 RESTful 功能。

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

```
[Sysname] restful https enable
```

1.1.39 screen-length

screen-length 命令用来设置分屏显示时，每屏所显示的行数。

undo screen-length 命令用来恢复缺省情况。

【命令】

screen-length *screen-length*

undo screen-length

【缺省情况】

每屏显示 24 行数据。

【视图】

用户线视图

用户线类视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

screen-length: 指定每屏所显示的行数，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，此时与执行 **screen-length disable** 命令效果相同。

【使用指导】

该命令设置的是每一屏所显示的行数，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。

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。

缺省情况下，分屏显示功能处于开启状态。

如果用户线视图下配置 **screen-length** 为缺省值，并且此时用户线类视图下配置了 **screen-length**，则用户线类视图下的配置生效；如果用户线类视图下未配置，则生效的为缺省值。

用户线视图下使用本命令配置的分屏显示信息行数立即生效；在用户线类视图下配置的分屏显示信息行数将在下次登录时生效。

【举例】

设置 VTY 用户线分屏显示时，每屏显示 30 行数据。

```
<Sysname> system-view
[Sysname] line vty 0
[Sysname-line-vty0] screen-length 30
```

【相关命令】

- **screen-length disable**（基础配置指导/CLI）

1.1.40 send

send 命令用来向用户线发送消息。

【命令】

```
send { all | number1 | { aux | console | vty } number2 }
```

【视图】

用户视图

【缺省用户角色】

```
network-admin
mdc-admin
```

【参数】

all: 所有的用户线。

number1: 用户线的编号（绝对编号方式）。独立运行模式下，**number1** 的取值范围为 0~73；IRF 模式下，**number1** 的取值范围为 0~6453。

aux: AUX 用户线。

console: Console 用户线。仅 LSXM1SUPD3 主控板支持该用户线。

vtty: VTY 用户线。

number2: 用户线的编号（相对编号方式）。

【使用指导】

输入本命令后回车，系统会提示您可以输入消息内容。在输入消息内容时，按<Enter>键结束输入，按<Ctrl+C>组合键取消此次操作。

【举例】

使用 VTY 0 用户线上线的用户想重启设备，于是发信息 “Note please, I will reboot the system in 3 minutes.” 来提醒 VTY 1。

```
<Sysname> send vty 1
Input message, end with Enter; abort with CTRL+C:
Your attention, please. I will reboot the system in 3 minutes.
Send message? [Y/N]:y
```

使用 VTY 1 用户线登录的用户将收到如下消息：

```
[Sysname]

***
***
***Message from vty0 to vty1
***
Your attention, please. I will reboot the system in 3 minutes.
```

1.1.41 set authentication password

set authentication password 命令用来设置认证密码。

undo set authentication password 命令用来恢复缺省情况。

【命令】

set authentication password { hash | simple } string

undo set authentication password

【缺省情况】

未配置认证密码。

【视图】

用户线视图

用户线类视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

hash: 以哈希方式设置密码。

simple: 以明文方式设置密码，该密码将以密文方式存储。

string: 密码字符串，区分大小写。明文密码为 1~16 个字符的字符串，哈希密码为 1~110 个字符的字符串。

【使用指导】

FIPS 模式下，不支持本命令。

以明文或哈希方式设置的密码，均以哈希计算后的密文形式保存在配置文件中。

如果用户线视图下配置 **set authentication password** 为缺省值，并且此时用户线类视图下配置了 **set authentication password**，则用户线类视图下的配置生效；如果用户线类视图下未配置，则生效的为缺省值。

仅具有 **network-admin**、**mdc-admin** 或者 **level-15** 用户角色的用户可以执行该命令。其他角色的用户，即使授权了该命令的操作权限，也不能执行该命令。

在用户线视图/用户线类视图下，使用该命令设置的认证密码将在下次登录设备时生效。

【举例】

设置用户线 VTY 0 的认证密码为 **hello**。

```
<Sysname> system-view
[Sysname] line vty 0
[Sysname-line-vty0] authentication-mode password
[Sysname-line-vty0] set authentication password simple hello
```

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

【相关配置】

- **authentication-mode**

1.1.42 shell

shell 命令用来在当前用户线上开启终端服务。

undo shell 命令用来在当前用户线上关闭终端服务。

【命令】

shell

undo shell

【缺省情况】

所有用户线的终端服务功能处于开启状态。

【视图】

用户线视图

用户线类视图

【缺省用户角色】

network-admin

mdc-admin

【使用指导】

Console 用户线视图/Console 用户线类视图不支持 **undo shell** 命令。

AUX 用户线视图/AUX 用户线类视图不支持 **undo shell** 命令。

用户不能在自己登录的用户线上使用 **undo shell** 命令。

当设备作为 Telnet/SSH 服务器的时候，不能配置 **undo shell** 命令。

如果在用户线类视图下使用 **undo shell** 命令关闭了终端服务，那么用户线视图下无法使用 **shell** 启动终端服务。

当设备作为重定向服务器时，如果使用本命令在用户线上关闭了终端服务，则该用户线只能用于重定向服务功能，其他设备无法通过该用户线登录到本设备；如果未关闭终端服务，则该用户线既能用于重定向服务，也能用于终端服务使其他设备通过该用户线登录到本设备，但需要注意的是两者不能同时占用该用户线。

【举例】

在 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] line vty 0 4
[Sysname-line-vty0-4] undo shell
Disable line-vty0-4 , are you sure? [Y/N]:y
[Sysname-line-vty0-4]
```

1.1.43 speed

speed 命令用来设置用户线的传输速率。

undo speed 命令用来恢复缺省情况。

【命令】

speed *speed-value*

undo speed

【缺省情况】

用户线的传输速率为 9600bps。

【视图】

用户线视图

【缺省用户角色】

network-admin

mdc-admin

【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。

【使用指导】

VTY 用户线视图不支持该命令。

访问终端和设备相应用户线下传输速率的设置必须一致，双方才能正常通信。

【举例】

将用户线 AUX 0 的传输速率设置为 19200bps。

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

```
[Sysname] line aux 0
[Sysname-line-aux0] speed 19200
```

1.1.44 stopbits

stopbits 命令用来设置停止位的个数。

undo stopbits 命令用来恢复缺省情况。

【命令】

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

```
undo stopbits
```

【缺省情况】

停止位为 1 比特。

【视图】

用户线视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

1: 停止位为 1 比特。

1.5: 停止位为 1.5 比特。目前，设备不支持该参数，配置后实际生效的是命令行 **stopbits 2**。

2: 停止位为 2 比特。

【使用指导】

VTY 用户线视图不支持该命令。

访问终端和设备相应用户线下停止位的设置必须一致，双方才能正常通信。

【举例】

设置 AUX 用户线的停止位为 1 比特。

```
<Sysname> system-view
[Sysname] line aux 0
[Sysname-line-aux0] stopbits 1
```

1.1.45 telnet

telnet 命令用于 Telnet 登录到远端设备，以便进行远程管理。

【命令】

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

【视图】

用户视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

remote-host: 远端设备的 IPv4 地址或主机名。其中，主机名为 1~253 个字符的字符串，不区分大小写，字符串仅可包含字母、数字、“-”、“_”或“.”。

service-port: 远端设备提供 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: 指定远端设备所属的 VPN 实例。*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。如果未指定本参数，则表示远端设备位于公网中。

source: 指定 Telnet 报文的源接口或源 IPv4 地址。如果未指定本参数，则使用路由出接口的主 IP 地址作为设备发送的 Telnet 报文的源 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。

dscp-value: Telnet 客户端向服务器端发送 Telnet 报文的 DSCP 优先级，取值范围为 0~63，缺省值为 48。

【使用指导】

FIPS 模式下，不支持本命令。

用户可以使用<Ctrl+K>组合键或 **quit** 命令来中断本次 Telnet 登录。

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
```

【相关命令】

- **telnet client source**

1.1.46 telnet client source

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 命令用来恢复缺省情况。

【命令】

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

```
undo telnet client source
```

【缺省情况】

未指定发送 Telnet 报文的源 IPv4 地址和源接口，使用报文路由出接口的主 IPv4 地址作为 Telnet 报文的源地址。

【视图】

系统视图

【缺省用户角色】

network-admin

mdc-admin

【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。

【使用指导】

FIPS 模式下，不支持本命令。

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。

【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
```

【相关命令】

- **display telnet client configuration**

1.1.47 telnet ipv6

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。

【命令】

```
telnet ipv6 remote-host [ -i interface-type interface-number ] [ port-number ] [ vpn-instance vpn-instance-name ] [ source { interface interface-type interface-number | ipv6 ipv6-address } | dscp dscp-value ] *
```

【视图】

用户视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

remote-host: 远端设备的 IPv6 地址或主机名。其中，主机名为 1~253 个字符的字符串，不区分大小写，字符串仅可包含字母、数字、“-”、“_”或“.”。

-i interface-type interface-number: 指定 Telnet 报文的出接口。*interface-type interface-number* 为接口类型和接口编号。当 Telnet 指定的服务端 IPv6 地址是全球单播地址时，则不能指定该参数；当指定的服务端 IPv6 地址为链路本地地址时，必须指定该参数。

port-number: 远端设备提供 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: 指定远端设备所属的 VPN 实例。*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。如果未指定本参数，则表示远端设备位于公网中。

source: 指定 Telnet 报文的源接口或源 IPv6 地址。如果未指定本参数，则使用路由出接口的主 IPv6 地址作为 Telnet 报文的源 IPv6 地址。

interface interface-type interface-number: 指定源接口，发送的 Telnet 报文的源 IPv6 地址为该接口的主地址。*interface-type interface-number* 为接口类型和接口编号。

ipv6 ipv6-address: 指定 Telnet 报文的源 IPv6 地址。

dscp-value: IPv6 Telnet 客户端向服务器端发送 Telnet 报文的 DSCP 优先级，取值范围为 0~63，缺省值为 48。

【使用指导】

FIPS 模式下，不支持本命令。

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
```

Telnet 登录到远程主机，IPv6 地址为 2000::1，并指定 Telnet 报文的源 IPv6 地址为 1000::1。

```
<Sysname> telnet ipv6 2000::1 source ipv6 1000::1
```

1.1.48 telnet server acl

telnet server acl 命令用来使用 ACL（Access Controle List，访问控制列表）限制哪些 Telnet 客户端可以访问设备。

undo telnet server acl 命令用来恢复缺省情况。

【命令】

```
telnet server acl [ mac ] acl-number
```

```
undo telnet server acl
```

【缺省情况】

未使用 ACL 限制 Telnet 客户端。

【视图】

系统视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

mac: 指定二层 ACL。若不指定该关键字，则表示 IPv4 ACL。

acl-number: ACL 的编号，取值范围及其代表的 ACL 类型如下：

- 2000~2999: 表示 IPv4 基本 ACL。
- 3000~3999: 表示 IPv4 高级 ACL。
- 4000~4999: 需指定 **mac** 关键字，表示二层 ACL。

【使用指导】

FIPS 模式下，不支持本命令。

配置 ACL 限制 Telnet 客户端时：

- 当未引用 ACL、或者引用的 ACL 不存在、或者引用的 ACL 为空时，允许所有登录用户访问设备；
- 当引用的 ACL 非空时，则只有 ACL 中 **permit** 的用户才能访问设备，其他用户不允许访问设备，以免非法用户使用 Telnet 访问设备。
- 如果多次使用该命令配置 Telnet 服务与 ACL 关联，最新配置生效。

关于 ACL 的详细描述和介绍请参见“ACL 和 QoS 配置指导”中的“ACL”。

该配置只过滤新建立的 Telnet 连接，不会对已建立的 Telnet 连接和操作造成影响。

【举例】

仅允许地址为 1.1.1.1 的用户通过 Telnet 访问本设备。

```
<Sysname> system-view
[Sysname] acl basic 2001
[Sysname-acl-ipv4-basic-2001] rule permit source 1.1.1.1 0
[Sysname-acl-ipv4-basic-2001] quit
[Sysname] telnet server acl 2001
```

1.1.49 telnet server acl-deny-log enable

telnet server acl-deny-log enable 命令用来开启匹配 ACL deny 规则后打印日志信息功能。

undo telnet server acl-deny-log enable 命令用来关闭匹配 ACL deny 规则后打印日志信息功能。

【命令】

telnet server acl-deny-log enable

undo telnet server acl-deny-log enable

【缺省情况】

匹配 ACL deny 规则后打印日志信息功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

mdc-admin

【使用指导】

通过配置 **telnet server acl** 或 **telnet server ipv6 acl** 命令，可限制 Telnet 客户端对设备的访问。此时，可通过开启 Telnet 客户端匹配 ACL deny 规则后打印日志信息功能，记录访问 Telnet 服务器受限的 Telnet 客户端信息。

执行本配置后，Telnet 客户端匹配 ACL deny 规则时，将产生日志信息。生成的日志信息将被发送到设备的信息中心，通过设置信息中心的参数，决定日志信息的输出规则（即是否允许输出以及输出方向）。

【举例】

开启 Telnet 客户端匹配 ACL deny 规则后打印日志信息功能。

```
<Sysname> system-view
[Sysname] telnet server acl-deny-log enable
```

1.1.50 telnet server dscp

telnet server dscp 命令用来配置 Telnet 服务器发送 Telnet 报文的 DSCP 优先级。

undo telnet server dscp 命令用来恢复缺省情况。

【命令】

```
telnet server dscp dscp-value
undo telnet server dscp
```

【缺省情况】

Telnet 服务器发送 Telnet 报文的 DSCP 优先级为 48。

【视图】

系统视图

【缺省用户角色】

```
network-admin
mdc-admin
```

【参数】

dscp-value: Telnet 报文的 DSCP 优先级，取值范围为 0~63。

【使用指导】

FIPS 模式下不支持该命令。

DSCP 携带在 IP 报文中的 ToS 字段，用来体现报文自身的优先等级，决定报文传输的优先程度。

【举例】

配置 Telnet 服务器发送报文的 DSCP 优先级为 30。

```
<Sysname> system-view
[Sysname] telnet server dscp 30
```

1.1.51 telnet server enable

telnet server enable 命令用来开启 Telnet 服务。

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

【命令】

```
telnet server enable
undo telnet server enable
```

【缺省情况】

Telnet 服务处于关闭状态。

【视图】

系统视图

【缺省用户角色】

```
network-admin
mdc-admin
```

【使用指导】

FIPS 模式下，不支持本命令。

只有使能 Telnet 服务后，才允许网络管理员通过 Telnet 协议登录设备。

【举例】

```
# 使能 Telnet 服务。
<Sysname> system-view
[Sysname] telnet server enable
```

1.1.52 telnet server ipv6 acl

telnet server ipv6 acl 命令用来使用 ACL 限制哪些 IPv6 Telnet 客户端可以访问设备。

undo telnet server ipv6 acl 命令用来恢复缺省情况。

【命令】

```
telnet server ipv6 acl { ipv6 | mac } acl-number
undo telnet server ipv6 acl
```

【缺省情况】

未使用 ACL 限制 Telnet 客户端。

【视图】

系统视图

【缺省用户角色】

```
network-admin
mdc-admin
```

【参数】

ipv6: 指定 IPv6 ACL。

mac: 指定二层 ACL。

acl-number: ACL 的编号，取值范围及其代表的 ACL 类型如下：

- 2000~2999: 需指定 **ipv6** 关键字, 表示 IPv6 基本 ACL。
- 3000~3999: 需指定 **ipv6** 关键字, 表示 IPv6 高级 ACL。
- 4000~4999: 需指定 **mac** 关键字, 表示二层 ACL。

【使用指导】

FIPS 模式下, 不支持本命令。

配置 ACL 限制 IPv6 Telnet 客户端时:

- 当未引用 ACL、或者引用的 ACL 不存在、或者引用的 ACL 为空时, 允许所有登录用户访问设备;
- 当引用的 ACL 非空时, 则只有 ACL 中 **permit** 的用户才能访问设备, 其他用户不允许访问设备, 以免非法用户使用 Telnet 访问设备。
- 如果多次使用该命令配置 Telnet 服务与 ACL 关联, 最新配置生效。

关于 ACL 的详细描述和介绍请参见“ACL 和 QoS 配置指导”中的“ACL”。

该配置只过滤新建立的 Telnet 连接, 不会对已建立的 Telnet 连接和操作造成影响。

【举例】

仅允许地址为 2000::1 的用户通过 Telnet 访问本设备。

```
<Sysname> system-view
[Sysname] acl ipv6 basic 2001
[Sysname-acl6-ipv6-basic-2001] rule permit source 2000::1 128
[Sysname-acl6-ipv6-basic-2001] quit
[Sysname] telnet server ipv6 acl ipv6 2001
```

1.1.53 telnet server ipv6 dscp

telnet server ipv6 dscp 命令用来配置 IPv6 Telnet 服务器发送报文的 DSCP 优先级。

undo telnet server ipv6 dscp 命令用来恢复缺省情况。

【命令】

```
telnet server ipv6 dscp dscp-value
undo telnet server ipv6 dscp
```

【缺省情况】

IPv6 Telnet 服务器发送 IPv6 Telnet 报文的 DSCP 优先级为 48。

【视图】

系统视图

【缺省用户角色】

```
network-admin
mdc-admin
```

【参数】

dscp-value: IPv6 Telnet 报文的 DSCP 优先级, 取值范围为 0~63。

【使用指导】

FIPS 模式下不支持该命令。

DSCP 携带在 IPv6 报文中的 Traffic class 字段，用来体现报文自身的优先等级，决定报文传输的优先程度。

【举例】

配置 IPv6 Telnet 服务器发送的报文的 DSCP 优先级为 30。

```
<Sysname> system-view
[Sysname] telnet server ipv6 dscp 30
```

1.1.54 terminal type

terminal type 命令用来设置当前用户线下的终端显示类型。

undo terminal type 命令用来恢复缺省情况。

【命令】

```
terminal type { ansi | vt100 }
undo terminal type
```

【缺省情况】

终端显示类型为 ANSI。

【视图】

用户线视图
用户线类视图

【缺省用户角色】

```
network-admin
mdc-admin
```

【参数】

ansi: 终端显示类型为 ANSI 类型。

vt100: 终端显示类型为 VT100 类型。

【使用指导】

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，并且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。

当用户线视图下的配置为缺省值时，将采用用户线类视图下配置的值；如果用户线类视图下的属性配置也为缺省值时，则采用该用户线下配置的缺省值。

用户线视图/用户线类视图下配置的终端显示类型都在下次登录时生效。

【举例】

设置终端显示类型为 VT100 类型。

```
<Sysname> system-view
[Sysname] line vty 0
[Sysname-line-vty0] terminal type vt100
```


1.1.55 user-interface

user-interface 命令用来进入一个或多个用户线视图。

【命令】

```
user-interface { first-number1 [ last-number1 ] | { aux | console | vty } first-number2 [ last-number2 ] }
```

【视图】

系统视图

【缺省用户角色】

```
network-admin  
mdc-admin
```

【参数】

first-number1: 第一个用户线的编号（绝对编号方式）。独立运行模式下，**first-number1** 的取值范围为 0~73；IRF 模式下，**first-number1** 的取值范围为 0~6453。

last-number1: 最后一个用户线的编号（绝对编号方式），该参数不小于 **first-number1**。

aux: AUX 用户线。

console: Console 用户线。仅 LSXM1SUPD3 主控板支持该用户线。

vty: VTY 用户线。

first-number2: 第一个用户线的编号（相对编号方式）。

last-number2: 最后一个用户线的编号（相对编号方式），该参数不小于 **first-number2**。

【使用指导】

该命令实现与 **line** 一致，仅为与旧版本兼容保留，请使用 **line**。

进入一个用户线视图进行配置后，该配置只对该用户视图有效。

进入多个用户线视图进行配置后，该配置对这些用户视图均有效。

【举例】

进入 AUX 0 用户线视图。

```
<Sysname> system-view  
[Sysname] user-interface aux 0  
[Sysname-line-aux0]
```

进入 VTY 0~4 用户线视图。

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

【相关命令】

- **user-interface class**

1.1.56 user-interface class

user-interface class 命令用来进入用户线类视图。

【命令】

```
user-interface class { aux | console | vty }
```

【视图】

系统视图

【缺省用户角色】

```
network-admin  
mdc-admin
```

【参数】

aux: AUX 用户线类。

console: Console 用户线类。仅 LSXM1SUPD3 主控板支持该用户线类。

vty: VTY 用户线类。

【使用指导】

该命令实现与 **line class** 一致，仅为与旧版本兼容保留，请使用 **line class**。

用户线视图下的配置只对该用户线生效。

用户线类视图下的配置修改不会立即生效，当用户下次登录后所修改的配置值才会生效。

user-interface class 命令用来进入用户线类视图，**user-interface** 命令用来进入一个或多个用户线视图。对于同时支持这两种视图的命令：

- 用户线视图下的配置优先于用户线类视图下的配置。
- 用户线视图下的属性配置为缺省值时，将采用用户线类视图下配置的值。如果用户线类视图下的属性配置也为缺省值时，则直接采用该属性的缺省值。

用户线类视图下支持的命令有：

- **activation-key**
- **auto-execute command**
- **authentication-mode**
- **command accounting**
- **command authorization**
- **escape-key**
- **history-command max-size**
- **idle-timeout**
- **protocol inbound**
- **screen-length**
- **set authentication password**
- **shell**
- **terminal type**
- **user-role**

【举例】

在 VTY 用户线类视图下，将用户连接的超时时间的缺省值设置为 15 分钟。

```
<Sysname> system-view
[Sysname] user-interface class vty
[Sysname-line-class-vty] idle-timeout 15
# 在 AUX 用户线类视图下，将终端会话的快捷键设置为<s>。
```

```
<Sysname> system-view
[Sysname] user-interface class aux
[Sysname-line-class-aux] activation-key s
[Sysname-line-class-aux] quit
```

- 在 AUX 用户线视图下，将终端会话的快捷键设置为缺省值（可以使用 `undo activation-key` 或者直接使用 `activation-key 13` 进行配置）。

```
[Sysname] user-interface aux 0
[Sysname-line-aux0] undo activation-key
```

- 此时生效的快捷键为用户线类视图下的配置，验证过程如下：
- 退出终端会话。

```
[Sysname-line-aux0] return
<Sysname> quit
```

- 重新登录设备，能看到如下显示信息。

```
Press ENTER to get started.
```

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

```
<Sysname>
```

【相关命令】

- **user-interface**

1.1.57 user-role

user-role 命令用来配置从当前用户线登录系统的用户角色。

undo user-role 命令用来删除用户角色或恢复缺省情况。

【命令】

```
user-role role-name
```

```
undo user-role [role-name]
```

【缺省情况】

如果用户登录于缺省 MDC，通过 Console 口登录系统的缺省用户角色为 `network-admin`，通过其他方式登录系统的用户角色为 `network-operator`；如果用户登录于非缺省 MDC，通过 `switchto mdc` 命令登录用户的缺省角色为 `mdc-admin`，其他登录用户的缺省角色均为 `mdc-operator`。

【视图】

用户线视图

用户线类视图

【缺省用户角色】

`network-admin`

`mdc-admin`

【参数】

role-name: 用户角色名称，为 1~63 个字符的字符串，区分大小写。可以是系统预定义的角色名称，包括 **network-admin**、**network-operator**、**mdc-admin**、**mdc-operator**、**level-0~level-15**，也可以是自定义的用户角色名称。不指定该参数时，表示恢复到缺省情况。系统预定义角色 **security-audit** 和 **guest-manager** 不支持在用户线/用户线类视图下进行配置。

【使用指导】

FIPS 模式下，不支持本命令。

在用户线视图/用户线类视图下使用该命令设置的用户角色将在下次登录设备时生效。

当用户线视图下的属性配置为缺省值时，将采用该用户线类视图下配置的用户角色。如果用户线类视图下配置的用户角色也为缺省值时，则直接采用该用户线下的缺省值。

仅具有 **network-admin**、**mdc-admin** 或者 **level-15** 用户角色的用户可以执行该命令。其他角色的用户，即使授权了该命令的操作权限，也不能执行该命令。

可通过多次执行本命令，配置多个用户角色，最多可配置 64 个。用户登录后具有的权限是这些角色权限的集合。

关于用户角色的详细介绍请参见“基础配置指导”中的“RBAC”。

【举例】

设置从 AUX 用户线登录系统的用户角色为 **network-admin**。

```
<Sysname> system-view
[Sysname] line aux 0
[Sysname-line-aux0] user-role network-admin
```

1.1.58 web captcha

web captcha 命令用来配置用户访问 Web 的固定校验码。

undo web captcha 命令用来恢复缺省情况。

【命令】

web captcha verification-code

undo web captcha

【缺省情况】

用户只能使用 Web 页面显示的校验码访问 Web。

【视图】

用户视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

verification-code: 访问 Web 的固定校验码，为 4 个字符的字符串，区分大小写。

【使用指导】

配置该命令后，不管 Web 登录页面显示的校验码是什么，用户只要输入该固定的校验码，即可访问设备。本命令主要用于测试环境，当需要对设备的 Web 功能进行测试时，可以配置一个固定的校验码，使用脚本即可登录设备，以免每次测试都要手工输入变化的校验码，影响测试效率。

设备在网络中正常使用的时候，建议不要配置该命令，以免降低 Web 访问的安全性。

多次配置该命令，最新配置生效。

该命令不能保存到配置文件，设备重启后失效。

【举例】

```
# 设置访问 Web 的固定校验码为 test。
```

```
<Sysname> web captcha test
```

1.1.59 web https-authorization mode

web https-authorization mode 命令用来设置使用 HTTPS 登录设备的认证模式。

undo web https-authorization mode 命令用来恢复缺省情况。

【命令】

```
web https-authorization mode { auto | manual }
```

```
undo web https-authorization mode
```

【缺省情况】

使用 HTTPS 登录设备的认证模式为 manual。

【视图】

系统视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

auto: 表示用户通过 HTTPS 登录设备时，使用客户端的 PKI 证书自动认证登录。

manual: 表示用户通过 HTTPS 登录设备时，设备给出登录页面，用户必须输入合法的用户名和密码后才能登录。

【使用指导】

当选用 **auto** 认证模式时，设备客户端的 PKI 证书自动认证登录：

- 当用户侧的证书正确且未超期，则读取证书中的 CN 字段作为用户名，进行 AAA 认证。如果认证成功，则自动进入设备的 Web 界面；
- 当用户侧的证书有效且未超期，但 AAA 认证失败，则回到登录界面（如果此时用户输入合法的用户名和密码仍然能够登录）；
- 当用户侧的证书错误或超期，则断开 HTTPS 连接。

【举例】

```
# 设置 Web 的 HTTPS 认证模式为 auto。
```

```
<Sysname> system-view
[Sysname] web https-authorization mode auto
```

1.1.60 web idle-timeout

web idle-timeout 命令用来设置 Web 闲置超时时间。

undo web idle-timeout 命令用来恢复缺省情况。

【命令】

web idle-timeout *idle-time*

undo web idle-timeout

【缺省情况】

Web 闲置超时时间为 10 分钟。

【视图】

系统视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

idle-time: Web 闲置超时时间，取值范围为 1~999，单位为分钟。

【使用指导】

当某 Web 用户在 *idle-time* 内一直没有操作 Web 页面，包括点击鼠标或键盘操作（只是移动鼠标，不会延长用户的下线时间），则系统会强制断开该用户的 Web 链接，使该用户下线。从而尽量避免在用户离开登录终端期间，非法用户对设备进行配置。

需要注意的是，修改 Web 线的闲置超时时间，会影响正在访问的用户。

【举例】

设置 Web 闲置超时时间为 100 分钟。

```
<Sysname> system-view
[Sysname] web idle-timeout 100
```

1.1.61 webui log

webui log enable 命令用来开启 Web 操作日志功能。

undo webui log enable 命令用来关闭 Web 操作日志功能。

【命令】

webui log enable

undo webui log enable

【缺省情况】

Web 操作日志功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

mdc-admin

【使用指导】

开启 Web 操作日志功能，比较关键的 Web 操作（比如修改系统时间）会产生对应的 Web 操作日志，输出到信息中心。通过设置信息中心的参数，最终决定 Web 操作日志的输出规则（即是否允许输出以及输出方向）

能够触发 Web 操作日志的 Web 操作动作和设备相关，请以实际设备情况为准。

Web 操作日志，采用固定的模块名“WEB”；日志助记符有统一的前缀“WEBOPT_”；同时 Web 操作日志还包含 Web 用户信息：Web 客户端 IP 地址和 Web 用户名。

【举例】

开启 Web 操作日志功能，Web 用户执行修改系统时间的操作。

```
<Sysname> system-view  
[Sysname] webui log enable
```

当 Web 用户执行修改系统时间的操作时，设备上将输出如下日志：

```
%Mar 25 14:32:38:802 2013 H3C WEB/6/WEBOPT_SET_TIME: -HostIP=192.168.100.235-User=Admin;  
Set the system date and time to 2013-05-27T10:00:00.
```