

H3C S5130S-SI[LI]&S5120V2-SI[LI]&S5110V2-SI& S5000V3-EI&S5000E-X&S3100V3-SI 系列以太网交换机

基础配置指导

新华三技术有限公司
<http://www.h3c.com>

资料版本：6W103-20190822
产品版本：Release 612x 系列

Copyright © 2019 新华三技术有限公司及其许可者 版权所有，保留一切权利。

未经本公司书面许可，任何单位和个人不得擅自摘抄、复制本书内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

前言

本配置指导主要介绍如何使用命令行接口、如何登录设备、对设备进行文件系统管理、设备管理、软件升级等功能的配置，包括 CLI、RBAC 配置、登录设备、FTP 和 TFTP、文件系统管理、配置文件管理、软件升级、设备管理、Tcl、Python、自动配置。

前言部分包含如下内容：

- [读者对象](#)
- [本书约定](#)
- [资料意见反馈](#)

读者对象

本手册主要适用于如下工程师：

- 网络规划人员
- 现场技术支持与维护人员
- 负责网络配置和维护的网络管理员

本书约定

1. 命令行格式约定

格 式	意 义
粗体	命令行关键字（命令中保持不变、必须照输的部分）采用 加粗 字体表示。
<i>斜体</i>	命令行参数（命令中必须由实际值进行替代的部分）采用 <i>斜体</i> 表示。
[]	表示用“[]”括起来的部分在命令配置时是可选的。
{ x y ... }	表示从多个选项中仅选取一个。
[x y ...]	表示从多个选项选取一个或者不选。
{ x y ... } *	表示从多个选项中至少选取一个。
[x y ...] *	表示从多个选项选取一个、多个或者不选。
&<1-n>	表示符号&前面的参数可以重复输入1~n次。
#	由“#”号开始的行表示为注释行。






2. 图形界面格式约定

格 式	意 义
< >	带尖括号“< >”表示按钮名，如“单击<确定>按钮”。
[]	带方括号“[]”表示窗口名、菜单名和数据表，如“弹出[新建用户]窗口”。
/	多级菜单用“/”隔开。如[文件/新建/文件夹]多级菜单表示[文件]菜单下的[新建]子菜单下

格 式	意 义
	的[文件夹]菜单项。

3. 各类标志

本书还采用各种醒目标志来表示在操作过程中应该特别注意的地方，这些标志的意义如下：

 警告	该标志后的注释需给予格外关注，不当的操作可能会对人身造成伤害。
 注意	提醒操作中应注意的事项，不当的操作可能会导致数据丢失或者设备损坏。
 提示	为确保设备配置成功或者正常工作而需要特别关注的操作或信息。
 说明	对操作内容的描述进行必要的补充和说明。
 窍门	配置、操作、或使用设备的技巧、小窍门。

4. 图标约定

本书使用的图标及其含义如下：

	该图标及其相关描述文字代表一般网络设备，如路由器、交换机、防火墙等。
	该图标及其相关描述文字代表一般意义下的路由器，以及其他运行了路由协议的设备。
	该图标及其相关描述文字代表二、三层以太网交换机，以及运行了二层协议的设备。
	该图标及其相关描述文字代表无线控制器、无线控制器业务板和有线无线一体化交换机的无线控制引擎设备。
	该图标及其相关描述文字代表无线接入点设备。
	该图标及其相关描述文字代表无线终结单元。
	该图标及其相关描述文字代表无线终结者。
	该图标及其相关描述文字代表无线Mesh设备。
	该图标代表发散的无线射频信号。
	该图标代表点到点的无线射频信号。
	该图标及其相关描述文字代表防火墙、UTM、多业务安全网关、负载均衡等安全设备。



该图标及其相关描述文字代表防火墙插卡、负载均衡插卡、NetStream插卡、SSL VPN插卡、IPS插卡、ACG插卡等安全插卡。

5. 示例约定

由于设备型号不同、配置不同、版本升级等原因，可能造成本手册中的内容与用户使用的设备显示信息不一致。实际使用中请以设备显示的内容为准。

本手册中出现的端口编号仅作示例，并不代表设备上实际具有此编号的端口，实际使用中请以设备上存在的端口编号为准。

资料意见反馈

如果您在使用过程中发现产品资料的任何问题，可以通过以下方式反馈：

E-mail: info@h3c.com

感谢您的反馈，让我们做得更好！

目 录

1 CLI	1-1
1.1 CLI简介	1-1
1.2 命令视图的操作	1-1
1.2.1 命令视图简介	1-1
1.2.2 进入系统视图	1-2
1.2.3 返回上一级视图	1-2
1.2.4 返回用户视图	1-2
1.3 使用命令行在线帮助	1-2
1.4 命令的undo形式	1-3
1.5 命令行输入	1-3
1.5.1 编辑命令行	1-3
1.5.2 STRING和TEXT类型参数的输入	1-4
1.5.3 接口类型的输入	1-4
1.5.4 快速输入命令行	1-5
1.5.5 配置命令字符串的别名	1-5
1.5.6 修改快捷键的绑定关系	1-6
1.5.7 命令行输入回显功能	1-8
1.6 解读输入错误提示信息	1-8
1.7 使用历史命令	1-9
1.7.1 功能简介	1-9
1.7.2 配置限制和指导	1-9
1.7.3 操作历史命令缓冲区	1-9
1.7.4 重复执行历史记录命令	1-10
1.8 便捷地查看显示信息	1-10
1.8.1 控制显示信息的分屏	1-10
1.8.2 查看带行号的显示信息	1-11
1.8.3 使用正则表达式过滤显示信息	1-11
1.8.4 将显示信息保存到指定文件	1-14
1.8.5 各种便捷查看方式的综合应用	1-15

1 CLI

1.1 CLI简介

CLI（Command Line Interface，命令行接口）是用户与设备之间的文本类指令交互界面。用户输入文本类命令，通过输入回车键提交设备执行相应命令，从而对设备进行配置和管理，并可以通过查看输出信息确认配置结果。

设备支持多种方式进入命令行接口界面，例如，通过 **Console** 口和 **Telnet** 登录设备后进入命令行接口界面等，各方式的详细描述请参见“基础配置指导”中的“登录设备”。

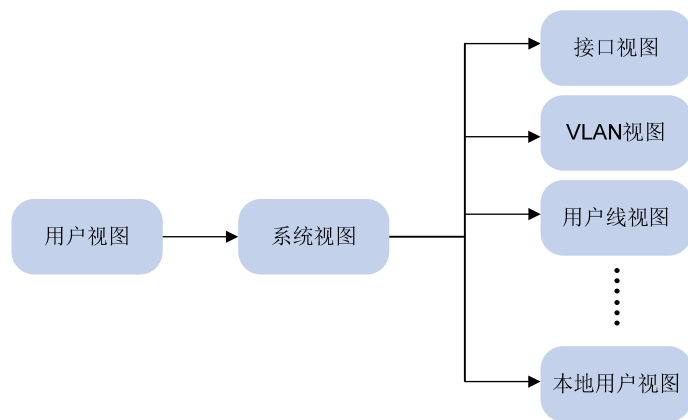
1.2 命令视图的操作

1.2.1 命令视图简介

设备提供了丰富的功能，不同的功能对应不同的配置和查询命令。为便于用户使用这些命令，设备按功能对命令进行分类组织。功能分类与命令视图对应，当要配置某功能的某条命令时，需要先进入这条命令所在的视图。每个视图都有唯一的、含义清晰的提示符，例如提示符[Sysname-vlan100]表示当前的命令视图是 VLAN 视图，VLAN 的编号是 100，在该视图下可对 VLAN 100 的属性进行配置。

命令视图采用分层结构，如 [图 1-1](#) 所示。

图1-1 命令视图示意图



- 用户登录设备后，直接进入用户视图。用户视图下可执行的操作主要包括查看操作、调试操作、文件管理操作、设置系统时间、重启设备、**FTP** 和 **Telnet** 操作等。
- 从用户视图可以进入系统视图。系统视图下能对设备运行参数以及部分功能进行配置，例如配置夏令时、配置欢迎信息、配置快捷键等。
- 在系统视图下输入特定命令，可以进入相应的功能视图，完成相应功能的配置，例如：进入接口视图配置接口参数、进入 VLAN 视图给 VLAN 添加端口、进入用户线视图配置登录用户的属性、创建本地用户并进入本地用户视图配置本地用户的属性等。功能视图下可能还包含子视图，例如 **NQA** 测试组视图下还包含测试类型视图，请参见各功能模块的详细描述。

想要了解某命令视图下支持哪些命令，请在该命令视图提示符后输入<?>。

1.2.2 进入系统视图

请在用户视图下执行本命令，进入系统视图。

system-view

1.2.3 返回上一级视图

1. 配置限制和指导

用户视图下执行 **quit** 命令会中断用户终端与设备之间的当前连接。

公共密钥视图下请使用 **peer-public-key end** 命令返回系统视图。

2. 配置步骤

请在任意视图下执行本命令，从当前视图退回到上一层视图。

quit

1.2.4 返回用户视图

1. 功能简介

本设备为用户提供了从任意的非用户视图返回到用户视图的快捷方式，而不需要多次执行 **quit** 命令逐级返回。

2. 配置步骤

返回用户视图。请选择如下一种方式返回用户视图。

- 请在任意非用户视图下执行本命令，返回用户视图。

return

- 按组合键<Ctrl+Z>从任意非用户视图返回用户视图。

1.3 使用命令行在线帮助

在命令行输入过程中，可以在命令行的任意位置输入<?>以获得详尽的在线帮助。下面给出常见的在线帮助应用场景，供参考使用。

- 在任意视图下，输入<?>即可获取该视图下可以使用的所有命令及其简单描述。例如：

```
<Sysname> ?
User view commands:
  archive           Archive configuration
  arp               Address Resolution Protocol (ARP) module
  backup            Backup the startup configuration file to a TFTP server
  boot-loader       Software image file management
  .....略.....
```

- 输入一条命令的关键字，后接以空格分隔的<?>。

如果<?>位置为关键字，则列出全部关键字及其简单描述。例如：

```
<Sysname> terminal ?
debugging  Enable to display debugging logs on the current terminal
```



```
logging      Display logs on the current terminal
monitor      Enable to display logs on the current terminal
```

如果<?>位置为参数，则列出有关的参数描述。例如：

```
<Sysname> system-view
[Sysname] interface vlan-interface ?
    <1-4094>  Vlan-interface interface number
[Sysname] interface vlan-interface 1 ?
    <cr>
```

其中，<1-4094>表示该参数的取值范围为 1~4094；<cr>表示命令行当前位置无参数，直接输入回车即可执行。

- 输入命令的不完整关键字，其后紧接<?>，显示以该字符串开头的所有命令关键字及其帮助信息。例如：

```
<Sysname> f?
fdisk      Partition a storage medium
fixdisk    Check and repair a storage medium
format     Format a storage medium
free       Release a connection
ftp        Open an FTP connection
<Sysname> display ftp?
ftp        FTP module
ftp-server FTP server information
ftp-user   FTP user information
```

1.4 命令的undo形式

命令的 **undo** 形式一般用来恢复缺省情况、关闭某个功能或者删除某项设置。大部分配置命令都有对应的 **undo** 形式。例如，**info-center enable** 命令用来开启信息中心，**undo info-center enable** 命令用来关闭信息中心。

1.5 命令行输入

1.5.1 编辑命令行

编辑命令行时，系统支持如 [表 1-1](#) 所示的单个按键和如 [表 1-4](#) 所示的组合键。

用户通过键盘输入命令行后，按<Enter>键执行该命令。

表1-1 编辑功能表

按键	功能
普通按键	若编辑缓冲区未满，则插入到当前光标位置，并向右移动光标（命令行下发前会暂时缓存在编辑缓冲区，缓冲区的大小为511个字符，如果编辑缓冲区满，则后续输入的字符无效）
退格键<Backspace>	删除光标位置的前一个字符，光标前移
左光标键<←>	光标向左移动一个字符位置
右光标键<→>	光标向右移动一个字符位置

按键	功能
上光标键<↑>	访问上一条历史命令
下光标键<↓>	访问下一条历史命令
<Tab>键	输入不完整的关键字后按下<Tab>键，系统自动补全关键字： <ul style="list-style-type: none"> 如果与之匹配的关键字唯一，则系统用此完整的关键字替代原输入并换行显示 如果与之匹配的关键字不唯一，则多次按<Tab>键，系统会循环显示所有以输入字符串开头的关键字 如果没有与之匹配的关键字，系统会不作任何修改，重新换行显示原输入



说明

在配置文件中，存在#和 **version 7.1.xxx, Release xxx** 这样的特殊命令行配置信息。#用于将两段配置信息隔开；**version 7.1.xxx, Release xxx** 用于记录设备正在运行的软件包的版本信息。这样的命令行不支持在线帮助，但可以在任意视图下执行# xxx 或者 **version xxx**（例如执行# abc 或者 **version abc**），执行后系统不会提示错误信息，也不会修改这些行的值。这样的命令行用户没有必要使用，因此在命令手册中不再描述。

1.5.2 STRING和TEXT类型参数的输入

如果命令行中的参数为 **STRING** 类型，则建议输入除“?”、“”、“\”、空格之外的可见字符（可见字符对应的 **ASCII** 码区间为 32~126），以免设备将该参数传递给其它网络设备时，对端设备无法解析。如果 **STRING** 类型的参数中需要包含字符“”、“\”，则必须使用转义字符“\”辅助输入，即实际应输入“\”、“\\”；如需输入空格，则需要将整个字符串包含在双引号中，例如，若要配置字符串参数为“my device”，则实际应输入“"my device"”。

如果命令行中的参数为 **TEXT** 类型，则除了“?”外的其他字符均可输入。

各业务模块可能对参数有更多的输入限制，详情请参见命令的提示信息以及命令参考中的参数描述。

1.5.3 接口类型的输入

输入接口类型时，设备支持使用接口类型的全称和简称。使用接口类型的全称时，支持不完整的字符输入；使用接口类型简称时，必须输入完整的简称。两种方式输入的接口类型均不区分大小写。例如在输入**interface gigabitethernet 1/0/1** 时，可以使用接口类型全称的不完整字符**interface g 1/0/1**，也可以使用接口类型简称**interface ge 1/0/1**。接口类型和接口编号之间无论输入空格与否，都可以成功进入接口视图。关于接口全名与简名的对应关系，如 [表 1-2](#) 所示。

表1-2 接口类型的全称和简称对应表

接口类型全称	接口类型简称
Bridge-Aggregation	BAGG
Ethernet	Eth

接口类型全称	接口类型简称
GigabitEthernet	GE
InLoopBack	InLoop
LoopBack	Loop
M-Ethernet	ME
Multicast Tunnel	MTunnel
NULL	NULL
Ten-GigabitEthernet	XGE
Vlan-interface	Vlan-int

1.5.4 快速输入命令行

设备支持不完整关键字输入，即在当前视图下，当输入的字符足够匹配唯一的关键字时，可以不必输入完整的关键字。该功能提供了一种快捷的输入方式，有助于提高操作效率。

例如用户视图下以 **s** 开头的命令有 **startup saved-configuration**、**system-view** 等。

- 如果要输入 **system-view**，可以直接输入 **sy**（不能只输入 **s**，因为只输入 **s** 时，匹配到的关键字不唯一）。
- 如果要输入 **startup saved-configuration**，可以直接输入 **st s**。

可以按<Tab>键由系统自动补全关键字的全部字符，以确认系统的选择是否为所需输入的关键字。

1.5.5 配置命令字符串的别名

1. 功能简介

通过本命令用户可以为命令行指定一个或多个别名，也可以为命令行开头的一个或多个关键字配置多个别名，使其符合用户的使用习惯。例如：

- 将命令 **display ip routing-table** 的别名配置为 **shiprt** 后，就可以使用别名命令 **shiprt** 来代替执行命令 **display ip routing-table**。
- 将命令关键字 **display ip** 的别名配置为 **ship**，就可以用别名命令 **ship** 执行所有以 **display ip** 开头的命令行，如可以使用 **ship routing-table** 代替执行 **display ip routing-table**，使用 **ship interface** 代替执行 **display ip interface**。

用户成功执行的带别名的命令将以系统原始的命令形式被显示或存储。

为了方便用户使用，系统定义了部分常用的关键字作为缺省别名，如 [表 1-3](#) 所示。

表1-3 系统定义的缺省别名

缺省别名	命令
access-list	acl
end	return
erase	delete
exit	quit

缺省别名	命令
hostname	sysname
logging	info-center
no	undo
show	display
write	save

2. 配置限制和指导

使用本特性，只有当命令行第一个关键字或者 **undo** 命令的第二个关键字是别名时，才按照别名命令替换执行，否则按照非别名命令执行。例如：

用户成功执行的带别名的命令将以系统原始的命令形式被显示或存储。

配置别名时，可以使用 **\$n** 表示命令行中的参数或者关键字，这样既可以用别名替代部分关键字来简化输入，又可以根据实际需要指定不同的参数或者关键字，增加了灵活性。**\$n** 最多可以使用 9 次，**n** 为 1~9 的整数，表示参数或关键字出现的顺序。如果别名命令中定义了参数，则参数必须输入完整。比如，将命令 **display ip \$1 | include \$2** 的别名配置为 **shinc** 后，如果需要执行 **display ip routing-table | include Static** 命令来筛选并查看路由表中的所有静态路由信息，可直接执行 **shinc routing-table Static**。

系统定义的缺省别名无法取消。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 给指定的命令字符串配置别名。

```
alias alias command
```

系统定义的缺省别名命令，请参见 [表 1-3](#)。

- (3) （可选）可在任意视图下执行本命令，显示命令字符串别名功能的相关配置。

```
display alias [ alias ]
```

1.5.6 修改快捷键的绑定关系

1. 功能简介

为方便用户快捷操作设备，设备支持 24 个快捷键。用户按下快捷键后，设备会立即执行对应的命令行或者功能。如果这些快捷键和用户登录终端定义的快捷键冲突，或者不符合用户的使用习惯，用户可使用该命令重新定义快捷键，甚至取消快捷键的绑定关系。

2. 配置限制和指导

一个快捷键对应一个命令或功能，如果使用本命令多次定义同一快捷键，则最新配置生效。如果多次使用本命令将多个快捷键和同一命令、功能绑定，则这些绑定的快捷键均生效。

当用户使用终端软件与设备进行交互时，如果终端软件定义快捷键（包括用户可定义和系统保留快捷键），则快捷键会遵从终端软件的定义。

3. 配置步骤

- (1) 进入系统视图。

system-view

- (2) 修改快捷键的绑定关系。

hotkey *hotkey* { *command* | **function** *function* | **none** }

缺省情况下，各快捷键的绑定关系见 [表 1-4](#)。

- (3) （可选）可在任意视图下执行本命令，显示系统中快捷键的分配信息。

display hotkey

表1-4 快捷键的缺省绑定关系

快捷键	缺省绑定的功能或命令
CTRL_A	move_the_cursor_to_the_beginning_of_the_line，表示将光标移动到当前行的开头
CTRL_B	move_the_cursor_one_character_to_the_left，表示将光标向左移动一个字符
CTRL_C	stop_the_current_command，表示停止当前正在执行的功能
CTRL_D	erase_the_character_at_the_cursor，表示删除当前光标所在位置的字符
CTRL_E	move_the_cursor_to_the_end_of_the_line，表示将光标移动到当前行的末尾
CTRL_F	move_the_cursor_one_character_to_the_right，表示将光标向右移动一个字符
CTRL_G	display current-configuration ，表示显示当前配置
CTRL_H	erase_the_character_to_the_left_of_the_cursor，表示删除光标左侧的一个字符
CTRL_K	abort_the_connection_request，表示终止呼出的连接
CTRL_L	display ip routing-table ，表示显示IPv4路由表信息
CTRL_N	display_the_next_command_in_the_history_buffer，表示显示历史缓冲区中的下一条命令
CTRL_O	undo debugging all ，表示关闭所有功能项的调试开关
CTRL_P	display_the_previous_command_in_the_history_buffer，表示显示历史缓冲区中的上一条命令
CTRL_R	redisplay_the_current_line，表示重新显示当前行信息
CTRL_T	未绑定任何命令行或功能
CTRL_U	未绑定任何命令行或功能
CTRL_V	（暂不支持）paste_text_from_the_clipboard，表示粘贴剪贴板的内容
CTRL_W	delete_the_word_to_the_left_of_the_cursor，表示删除光标左侧连续字符串内的所有字符
CTRL_X	delete_all_characters_from_the_beginning_of_the_line_to_the_cursor，表示删除光标左侧所有的字符
CTRL_Y	delete_all_characters_from_the_cursor_to_the_end_of_the_line，表示删除光标所在位置及其右侧所有的字符
CTRL_Z	return_to_the_User_View，表示退回到用户视图

快捷键	缺省绑定的功能或命令
CTRL_]	kill_incoming_connection_or_redirect_connection，表示终止当前连接
ESC_B	move_the_cursor_back_one_word，表示将光标移动到左侧连续字符串的首字符处
ESC_D	delete_all_characters_from_the_cursor_to_the_end_of_the_word，表示删除光标所在位置及其右侧连续字符串内的所有字符
ESC_F	move_the_cursor_forward_one_word，表示将光标向右移到下一个连续字符串之前
ESC_N	（暂不支持）move_the_cursor_down_a_line，表示将光标向下移动一行（输入回车前有效）
ESC_P	（暂不支持）move_the_cursor_up_a_line，表示将光标向上移动一行（输入回车前有效）
ESC_<	（暂不支持）move_the_cursor_to_the_beginning_of_the_clipboard，表示将光标所在位置指定为剪贴板的开始位置
ESC_>	（暂不支持）move_the_cursor_to_the_end_of_the_clipboard，表示将光标所在位置指定为剪贴板的结束位置

1.5.7 命令行输入回显功能

1. 功能简介

当用户未完成输入操作却被大量的系统信息打断时，开启此功能可以回显用户已经输入而未提交执行的信息，方便用户继续完成未输入的内容。

2. 配置步骤

- (1) 进入系统视图。

system-view

- (2) 打开命令行输入回显功能。

info-center synchronous

缺省情况下，命令行输入回显功能处于关闭状态。

本命令的详细介绍请参见“网络管理和监控命令参考”中的“信息中心”。

1.6 解读输入错误提示信息

命令行输入完毕后，请按<Enter>键执行该命令。设备执行命令的过程中，首先会对命令行进行合法性检查。如果通过合法性检查，则正确执行；否则，输出错误信息，常见的错误信息如 [表 1-5](#) 所示。

表1-5 命令行常见错误信息表

英文错误信息	错误原因
% Unrecognized command found at '^' position.	命令无法解析，符号“^”指示位置出错
% Incomplete command found at '^' position.	符号“^”指示位置的参数输入不完整
% Ambiguous command found at '^' position.	符号“^”指示位置的关键字不明确，存在二义性

英文错误信息	错误原因
% Too many parameters.	输入参数太多
% Wrong parameter found at '^' position.	在符号 “^” 指示位置的参数错误

1.7 使用历史命令

1.7.1 功能简介

用户在设备上成功执行的命令，会同时保存到用户独享的历史命令缓冲区和所有用户共享的历史命令缓冲区。

表1-6 历史命令缓冲区描述表

选项	独享历史命令缓冲区	共享历史命令缓冲区
内容	当前用户执行成功的命令	所有用户执行成功的命令
查看	支持	支持
调用	支持	不支持
保存	不保存	保存
调整大小	支持	大小固定为1024条

1.7.2 配置限制和指导

设备保存用户执行过的命令时，遵循以下原则：

- 如果用户使用了命令的不完整形式，保存的历史命令也是不完整形式。
- 如果用户使用了命令字符串的别名形式，保存的历史命令是原始命令形式。
- 如果用户连续多次执行同一条命令，设备的历史命令中只保留一次。但如果执行时输入的形式不同，将作为不同的命令对待。例如：连续多次执行 **display current-configuration** 命令，设备只保存一条历史命令；如果分别执行 **display current-configuration** 命令和它的不完整形式 **display cu**，设备将保存为两条历史命令。
- 如果当前历史命令缓冲区满且有新的命令需要缓存，则自动删除最早的记录，来保存新命令。

1.7.3 操作历史命令缓冲区

1. 查看历史命令缓冲区

- 可在任意视图下执行本命令，查看独享历史命令缓冲区。
display history-command
- 可在任意视图下执行本命令，查看共享历史命令缓冲区。
display history-command all

2. 调用历史命令缓冲区

使用上光标键↑并回车，调用上一条历史命令；使用下光标键↓并回车，可调用下一条历史命令。

3. 配置命令缓冲区的大小

在用户线/用户线类视图下执行 **history-command max-size** 命令，可调整独享历史命令缓冲区大小。具体配置请参见“基础配置命令参考”中的“登录设备”。

1.7.4 重复执行历史记录命令

1. 功能简介

当需要重复执行最近的历史记录命令时，使用 **repeat** 命令可以重复多次执行多条历史命令，并且可以设置每次重复执行历史命令的时间间隔。

2. 配置限制和指导

- 重复执行历史命令时，系统将按照历史命令的下发顺序执行。例如，用户在某视图下依次执行命令 **a**、**b** 和 **c** 后，再执行 **repeat 3** 命令，则系统将按照 **a**、**b** 和 **c** 的顺序重复执行。
- 重复执行某条历史命令时，需要先进入该命令所在的视图。重复执行多条历史命令时，需要先进入第一条命令所在的视图。
- 如果用户重复执行的历史命令中存在交互式命令，需要用户手动处理此交互式命令，直到交互式命令执行结束，历史命令才会继续被重复执行。

3. 配置步骤

可在任意视图下执行本命令，重复执行历史记录命令。

repeat [*number*] [**count times**] [**delay seconds**]

1.8 便捷地查看显示信息

1.8.1 控制显示信息的分屏

1. 功能简介

缺省情况下，设备支持分屏显示功能，即当显示信息超过一屏时，系统会将信息分屏显示，并在屏间显示“----more----”信息，表示这一屏信息已经显示完毕，自动暂停，方便查看显示信息。这时用户可以使用 [表 1-7](#) 所示的按键来选择下一步操作。

表1-7 分屏显示功能表

按键	功能
空格键	继续显示下一屏信息
回车键	继续显示下一行信息
<Ctrl+C>	停止显示，退回到命令行编辑状态
<PageUp>	显示上一页信息
<PageDown>	显示下一页信息

如果想要一次查看全部显示信息，可以通过以下配置关闭当前登录用户的分屏显示功能。分屏显示功能处于关闭状态时，如果信息较多，则会连续刷屏，不方便查看。

2. 关闭分屏显示功能

请在用户视图下执行本命令，关闭当前用户的分屏显示功能。

screen-length disable

缺省情况下，用户登录后将遵循用户线下的 **screen-length** 设置。**screen-length** 设置的缺省情况为：允许分屏显示，下一屏显示 24 行数据。**screen-length** 命令的详细介绍请参见“基础配置命令参考”中的“登录设备”

命令的执行仅对当前用户本次登录有效，用户重新登录后将恢复到缺省情况。

1.8.2 查看带行号的显示信息

1. 功能简介

在用 **display** 命令查看显示信息时，用户可以用 **by-linenum** 参数在显示信息的同时显示信息行号，方便定位显示信息。

行号占 5 个字符，通常行号后面接“:”。当 **by-linenum** 和 **begin** 参数一起使用时，行号后面还可能接“-”，其中“:”表示该行符合匹配规则，“-”表示该行不符合匹配规则。

2. 配置步骤

按行显示 **display** 命令执行结果。

display command | by-linenum

3. 配置举例

显示 VLAN 999 信息的同时显示行号。

```
<Sysname> display vlan 999 | by-linenum
1:  VLAN ID: 999
2:  VLAN type: Static
3:  Route interface: Configured
4:  IPv4 address: 192.168.2.1
5:  IPv4 subnet mask: 255.255.255.0
6:  Description: For LAN Access
7:  Name: VLAN 0999
8:  Tagged ports:  None
9:  Untagged ports: None
```

1.8.3 使用正则表达式过滤显示信息

1. 功能简介

在执行 **display** 命令查看显示信息时，可以使用正则表达式来过滤显示信息，以便快速的找到自己关注的信息。

在 **display** 命令中通过输入 **| { begin | exclude | include } regular-expression** 参数的方式来过滤显示。**begin**、**exclude** 和 **include** 关键字的含义如下：

- **begin**: 显示特定行及其以后的所有行，该特定行必须包含指定正则表达式。
- **exclude**: 显示不包含指定正则表达式的所有行。

- **include:** 只显示包含指定正则表达式的所有行。

正则表达式 (*regular-expression*) 为 1~256 个字符的字符串, 区分大小写, 它支持多种特殊字符, 特殊字符的匹配规则如 [表 1-8](#) 所示。

表1-8 正则表达式中的特殊字符描述表

特殊字符	含义	举例
^	匹配以指定字符开始的行	<code>^u</code> 只能匹配以u开始的行, 不能匹配以Au开始的行
\$	匹配以指定字符结束的行	<code>u\$</code> 只能匹配以u结尾的行, 不能匹配以uA结尾的行
.	通配符, 可代表任何一个字符	<code>.s</code> 可以匹配as和bs等
*	匹配星号前面的字符或字符串零次或多次	<ul style="list-style-type: none"> • <code>zo*</code>可以匹配z 以及 zoo • <code>(zo)*</code>可以匹配 zo 以及 zozo
+	匹配+前面的字符或字符串一次或多次	<code>zo+</code> 可以匹配zo以及zoo, 但不能匹配z
 	匹配 左边或右边的整个字符串	<code>def int</code> 只能匹配包含def或者int的字符串所在的行
()	表示字符串, 一般与“+”或“*”等符号一起使用	<code>(123A)</code> 表示字符串123A; <code>408(12)+</code> 可以匹配40812或408121212等字符串, 但不能匹配408
\index	表示重复一次指定字符串, 字符串是指\前用()括起来的字符串, index对应\前字符串的顺序号按从左至右的顺序从1开始编号: 如果\前面只有一个字符串, 则index只能为1; 如果\前面有n个字符串, 则index可以为1到n中的任意整数	<code>(string)\1</code> 表示把string重复一次, 匹配的字符串必须包含stringstring; <code>(string1)(string2)\2</code> 表示把string2重复一次, 匹配的字符串必须包含string1string2string2; <code>(string1)(string2)\1\2</code> 表示先把string1重复一次, 再重复一次string2, 匹配的字符串必须包含string1string2string1string2
[]	表示字符选择范围, 将以选择范围内的单个字符为条件进行匹配, 只要字符串里包含该范围的某个字符就能匹配到	<ul style="list-style-type: none"> • <code>[16A]</code>表示可以匹配到的字符串只需要包含 1、6 或 A 中任意一个 • <code>[1-36A]</code> 表示可以匹配到的字符串只需要包含 1、2、3、6 或 A 中任意一个 (-为连接符) <p>如果]需要作为普通字符出现在[]内时, 必须把]写在[]中字符的最前面, 形如<code>[]string</code>, 才能匹配到]。[没有这样的限制</p>
[^]	表示选择范围外的字符, 将以单个字符为条件进行匹配, 只要字符串里包含该范围外的某个字符就能匹配到	<code>[^16A]</code> 表示可匹配的字符串只需要包含1、6和A之外的任意字符, 该字符串也可以包含字符1、6或A, 但不能只包含这三个字符。例如 <code>[^16A]</code> 可以匹配abc、m16, 不能匹配1、16、16A
{n}	n是一个非负整数, 匹配n次	<code>o{2}</code> 不能匹配Bob, 但是能匹配food
{n,}	n是一个非负整数, 至少匹配n次	<code>o{2,}</code> 不能匹配Bob, 但能匹配foooooo
{n,m}	m和n均为非负整数, 其中n小于等于m。只要字符串里包含n到m个某字符就能匹配到	<code>o{1,3}</code> 能匹配fod、food、foood、foooooo, 但不能匹配fd
\<	匹配包含指定字符串的字符串, 字符串前面如果有字符则不能是数字、字母和下划线	<code>\<do</code> 匹配单词domain, 还可以匹配字符串doa
\>	匹配包含指定字符串的字符串, 字符串后面如果有字符则不能是数字、字母和下划线	<code>do\></code> 匹配单词undo, 还可以匹配字符串cdo

特殊字符	含义	举例
\b	匹配一个单词边界，也就是指单词和空格间的位置	er\b可以匹配never，但不能匹配verb \ber可以匹配erase，但不能匹配verb
\B	匹配非单词边界	er\B能匹配verb，但不能匹配never
\w	\w等效于[A-Za-z0-9_]，是数字、字母或下划线	\w能匹配vlan，\w还能匹配service
\W	\W等效于[^A-Za-z0-9_]，是除了数字、字母和下划线之外的任意字符	\Wa可以匹配-a，但是不能匹配2a和ba等
\	转义操作符，\后紧跟本表中罗列的单个特殊字符时，将去除特殊字符的特定含义	<ul style="list-style-type: none"> • \\可以匹配包含\的字符串 • \^可以匹配包含^的字符串 • \\b 可以匹配包含\b 的字符串

2. 配置限制和指导

正则表达式的执行时间和正则表达式的复杂程度成正比，对于复杂的正则表达式，执行时间会比较长，如有需要，可按<CTRL+C>键终止。

3. 配置举例

查看当前生效的配置中，从包含“line”字符串的行开始到最后一行的配置信息（该显示信息与设备型号以及用户的当前配置有关）。

```
<Sysname> display current-configuration | begin line
line class aux
    user-role network-admin
#
line class vty
    user-role network-operator
#
line aux 0
    user-role network-admin
#
line vty 0 63
    authentication-mode none
    user-role network-admin
    user-role network-operator
#
.....略.....
```

查看设备当前处于 UP 状态的接口概要信息。

```
<Sysname> display interface brief | exclude DOWN
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface          Link Protocol Primary IP      Description
InLoop0            UP    UP(s)    --
NULL0              UP    UP(s)    --
```

```
Vlan1                UP    UP        192.168.1.83
```

Brief information on interfaces in bridge mode:

Link: ADM - administratively down; Stby - standby

Speed: (a) - auto

Duplex: (a)/A - auto; H - half; F - full

Type: A - access; T - trunk; H - hybrid

Interface	Link	Speed	Duplex	Type	PVID	Description
GE1/0/1	UP	1000M(a)	F(a)	A	1	

查看 SNMP 相关配置。

```
<Sysname> display current-configuration | include snmp
```

```
snmp-agent
```

```
snmp-agent community write private
```

```
snmp-agent community read public
```

```
snmp-agent sys-info version all
```

```
snmp-agent target-host trap address udp-domain 192.168.1.26 params securityname public
```

1.8.4 将显示信息保存到指定文件

1. 功能简介

display 命令显示的内容通常是统计信息、功能是否开启以及功能的相关参数配置，这些信息在设备运行过程中会随着时间的变化或者用户的配置而改变。使用本配置可以将当前显示信息保存到指定文件，方便随时比对和查看。

有两种方式将显示信息保存到文件中：

- 将显示信息独立保存到指定文件：使用该方式时，该文件只包含该显示信息的内容。
- 将显示信息以追加方式保存到已有文件：使用该方式时，该命令的显示信息会追加在指定文件的尾部保存，该文件能包含多条显示信息的内容。

2. 配置步骤

- 请在任意视图下执行本命令，将显示信息独立保存到指定文件。

```
display command > filename
```

- 请在任意视图下执行本命令，将显示信息以追加方式保存到已有文件。

```
display command >> filename
```

3. 配置举例

将 **display vlan 1** 命令的显示信息保存到指定文件 **vlan.txt**。

```
<Sysname> display vlan 1 > vlan.txt
```

查看 **vlan.txt** 的内容，验证 **display >** 命令的执行效果。

```
<Sysname> more vlan.txt
```

```
VLAN ID: 1
```

```
VLAN type: Static
```

```
Route interface: Not configured
```

```
Description: VLAN 0001
```

```
Name: VLAN 0001
```

```
Tagged ports: None
```

```
Untagged ports: None
```

将 **display vlan 999** 的显示信息以追加方式保存到指定文件 **vlan.txt**。

```
<Sysname> display vlan 999 >> vlan.txt
```

查看 **vlan.txt** 的内容，验证 **display >>** 命令的执行效果。

```
<Sysname> more vlan.txt
```

```
VLAN ID: 1
VLAN type: Static
Route interface: Not configured
Description: VLAN 0001
Name: VLAN 0001
Tagged ports:   None
Untagged ports: None
```

```
VLAN ID: 999
VLAN type: Static
Route interface: Configured
IP address: 192.168.2.1
Subnet mask: 255.255.255.0
Description: For LAN Access
Name: VLAN 0999
Tagged ports:   None
Untagged ports: None
```

1.8.5 各种便捷查看方式的综合应用

1. 功能简介

执行**display**命令时，通过选择参数，可以同时实现“[1.8.2 查看带行号的显示信息](#)”、“[1.8.3 使用正则表达式过滤显示信息](#)”和“[1.8.4 将显示信息保存到指定文件](#)”。

2. 配置步骤

请在用户视图下执行本命令，以综合使用各种方式便捷地查看显示信息。

```
display command [ | [ by-linenum ] { begin | exclude | include }
regular-expression ] [ > filename | >> filename ]
```

3. 配置举例

下面将通过举例示意如何将各种便捷查看方式综合应用。

按行号将当前配置保存到文件 **test.txt**。

```
<Sysname> display current-configuration | by-linenum > test.txt
```

将 **SNMP** 的相关配置以追加方式保存到文件 **test.txt**。

```
<Sysname> display current-configuration | include snmp >> test.txt
```

查看当前配置，从包含“**user-group**”字符串的行开始到最后一行配置信息，并同时显示行号。（行号后为“**:**”表示该行包含“**user-group**”字符串，行号后为“**-**”表示该行不包含“**user-group**”字符串。）

```
<Sysname> display current-configuration | by-linenum begin user-group
114:  user-group system
115-  #
116-  return
```

目 录

1 RBAC	1-1
1.1 RBAC简介	1-1
1.1.1 角色权限分配	1-1
1.1.2 为用户授权角色	1-3
1.2 FIPS相关说明	1-4
1.3 RBAC配置任务简介	1-4
1.4 创建用户角色	1-5
1.5 配置用户角色规则	1-5
1.6 配置特性组	1-7
1.7 配置资源控制策略	1-7
1.7.1 功能简介	1-7
1.7.2 配置限制和指导	1-7
1.7.3 配置接口资源控制策略	1-7
1.7.4 配置VLAN资源控制策略	1-8
1.8 为用户授权角色	1-8
1.8.1 配置限制和指导	1-8
1.8.2 使能缺省用户角色授权功能	1-8
1.8.3 为远程AAA认证用户授权角色	1-9
1.8.4 为本地AAA认证用户授权角色	1-9
1.8.5 为非AAA认证用户授权角色	1-10
1.9 配置用户角色切换	1-10
1.9.1 功能简介	1-10
1.9.2 配置限制和指导	1-11
1.9.3 配置用户角色切换的认证方式	1-12
1.9.4 配置用户角色切换的缺省目的用户角色	1-12
1.9.5 配置用户角色切换的密码	1-12
1.9.6 配置用户角色切换认证时使用用户登录的用户名认证	1-13
1.9.7 切换用户角色	1-13
1.10 RBAC显示和维护	1-13
1.11 RBAC典型配置举例	1-14
1.11.1 Telnet用户的本地用户角色授权配置举例	1-14
1.11.2 Telnet用户的RADIUS用户角色授权配置举例	1-16
1.11.3 Telnet用户的HWTACACS用户角色切换认证配置举例	1-18

1.11.4 Telnet 用户的RADIUS用户角色切换认证配置举例	1-23
1.12 RBAC常见故障处理.....	1-26
1.12.1 被授权的用户角色与本地用户实际拥有的权限不符.....	1-26
1.12.2 使用远程认证服务器进行身份认证的用户登录设备失败.....	1-27

1 RBAC

1.1 RBAC简介

RBAC (Role Based Access Control, 基于角色的访问控制) 通过建立“权限<->角色”的关联实现将权限赋予给角色, 并通过建立“角色<->用户”的关联实现为用户指定角色, 从而使用户获得相应角色所具有的权限。RBAC 的基本思想就是给用户指定角色, 这些角色中定义了允许用户操作哪些系统功能以及资源对象。RBAC 采用权限与用户分离的思想, 提高用户权限分配的灵活性, 减小用户授权管理的复杂度, 降低管理开销。

1.1.1 角色权限分配

为一个用户角色赋予权限的具体实现包括以下两个方面:

- 定义用户角色规则: 实现对系统功能的操作权限的控制。例如, 定义用户角色规则允许用户配置 **A** 功能, 或禁止用户配置 **B** 功能。
- 定义资源控制策略: 实现对系统资源的操作权限的控制。例如, 定义资源控制策略允许用户操作 **VLAN 10**。

资源控制策略需要与用户角色规则相配合才能生效。在用户执行命令的过程中, 系统对该命令涉及的系统资源使用权限进行动态检测, 因此只有用户同时拥有执行该命令的权限和使用该资源的权限时, 才能执行该命令。例如, 若管理员为某用户角色定义了一条规则允许用户执行创建 **VLAN** 的命令 **vlan**, 且同时定义了一条 **VLAN** 策略允许用户操作 **VLAN 10**, 则当用户被授权此用户角色并试图创建 **VLAN 10** 时, 操作会被允许, 但试图创建其它 **VLAN** 时, 操作会被禁止。若管理员并没有为该用户角色定义规则允许用户执行创建 **VLAN** 命令, 则用户即便拥有该 **VLAN** 资源的操作权限, 也无法执行相关的命令。

1. 用户角色规则

用户角色规则定义了允许/禁止用户操作某些功能的权限。一个用户角色中可以包含多条用户角色规则, 每条规则定义了是允许还是禁止用户对某命令、特性、特性组、**Web** 菜单、**XML** 元素或者 **OID** 进行操作。

- 基于命令的规则: 用来控制一条命令或者与指定命令关键字相匹配的一类命令是否允许被执行。
- 基于特性的规则: 用来控制特性包含的命令是否允许被执行。
- 基于特性组的规则: 用来同时对多个特性包含的命令进行控制。
- 基于 **Web** 菜单的规则: 用来控制指定的 **Web** 菜单选项是否允许被操作。
- 基于 **XML** 元素的规则: 用来控制指定的 **XML** 元素是否允许被执行。
- 基于 **OID** 的规则: 用来控制指定的 **OID** 是否允许被 **SNMP** 访问。

RBAC 对命令、特性、特性组、**Web** 菜单、**XML** 元素或者 **OID** 进行的操作, 又包括三种类型:

- 读类型: 用于显示系统配置信息和维护信息。如显示命令 **display**、显示文件信息的命令 **dir** 为读类型的命令。

- 写类型：用于对系统进行配置。如开启信息中心功能的命令 **info-center enable**、配置调试信息开关的命令 **debugging** 为写类型的命令。
- 执行类型：用于执行特定的功能。如 **ping** 命令、与 FTP 服务器建立连接的命令 **ftp** 为执行类型的命令。

一个用户角色中可以定义多条规则，各规则以创建时指定的编号为唯一标识，被授权该角色的用户可以执行的命令为这些规则中定义的可执行命令的并集。若这些规则定义的权限内容有冲突，则规则编号大的有效。例如，规则 1 允许执行命令 A，规则 2 允许执行命令 B，规则 3 禁止执行命令 A，则最终规则 2 和规则 3 生效，即禁止执行命令 A，允许执行命令 B。

2. 资源控制策略

资源控制策略规定了用户对系统资源的操作权限。在用户角色中可定义如下类型的资源控制策略：

- 接口策略：定义用户允许操作的接口，包括创建并进入接口视图、删除接口。
- VLAN 策略：定义用户允许操作的 VLAN，包括创建并进入 VLAN 视图、删除 VLAN。

在 **display** 命令中指定接口/VLAN 参数并不属于应用接口/VLAN。

3. 缺省用户角色

系统预定义了多种用户角色，用户角色名和对应的权限如 [表 1-1](#) 所示。这些用户角色缺省均具有操作所有系统资源的权限，但具有不同的系统功能操作权限。如果系统预定义的用户角色无法满足权限管理需求，管理员还可以自定义用户角色来对用户权限做进一步控制。

在所有系统预定义的用户角色当中，仅 **network-admin** 或者 **level-15** 角色的用户具有执行创建/修改/删除本地用户和本地用户组的权限。其它角色的用户，即使被授权对本地用户和本地用户组的操作权限，也仅仅具有修改自身密码的权限，没有除此之外的对本地用户和本地用户组的任何操作权限。用户以任意角色登录设备，在某视图下输入 **<?>** 会显示该视图下系统定义的缺省别名帮助信息，但用户对帮助信息中的命令行别名未必具有实际操作权限，命令行别名的实际操作权限以原命令行的操作权限为准。有关命令行别名的详细介绍请参见“基础配置指导”中的“CLI”。

用户以任意角色登录设备，均具有执行 **system-view**、**quit** 和 **exit** 命令的权限。

系统预定义的用户角色中，仅 **level-0~level-14** 可以通过自定义规则和资源控制策略调整自身的权限，但这种修改对于 **display history-command all** 命令不生效，即不能通过添加对应的规则来更改它的缺省执行权限。

表1-1 系统预定义的用户角色名和对应的权限

用户角色名	权限
network-admin	可操作系统所有功能和资源（除安全日志文件管理相关命令 display security-logfile summary 、 info-center security-logfile directory 、 security-logfile save 之外）

用户角色名	权限
network-operator	<ul style="list-style-type: none"> 可执行系统所有功能和资源的相关 display 命令（除 display history-command all、display security-logfile summary 等命令，具体请通过 display role 命令查看） 如果用户采用本地认证方式登录系统并被授予该角色，则可以修改自己的密码 可执行进入 XML 视图的命令 可允许用户操作所有读类型的 Web 菜单选项 可允许用户操作所有读类型的 XML 元素 可允许用户操作所有读类型的 OID
level-n (n = 0~15)	<ul style="list-style-type: none"> level-0: 可执行命令 ping、tracert、ssh2、telnet 和 super，且管理员可以为其配置权限 level-1: 具有 level-0 用户角色的权限，并且可执行系统所有功能和资源的相关 display 命令（除 display history-command all 之外），以及管理员可以为其配置权限 level-2~level-8 和 level-10~level-14: 无缺省权限，需要管理员为其配置权限 level-9: 可操作系统中绝大多数的功能和所有的资源，且管理员可以为其配置权限，但不能操作 display history-command all 命令、RBAC 的命令（Debug 命令除外）、文件管理、设备管理以及本地用户特性。对于本地用户，若用户登录系统并被授予该角色，可以修改自己的密码 level-15: 具有与 network-admin 角色相同的权限
security-audit	<p>安全日志管理员，仅具有安全日志文件的读、写、执行权限，具体如下：</p> <ul style="list-style-type: none"> 可执行安全日志文件管理相关的命令（display security-logfile summary、info-center security-logfile directory、security-logfile save）。安全日志文件管理相关命令的介绍，请参见“网络管理与监控”中的“信息中心” 可执行安全日志文件操作相关的命令，例如 more 显示安全日志文件内容；dir、mkdir 操作安全日志文件目录等，具体命令的介绍请参见“基础配置命令参考”中的“文件系统管理” <p>以上权限，仅安全日志管理员角色独有，其它任何角色均不具备 该角色不能被授权给从当前用户线登录系统的用户</p>

1.1.2 为用户授权角色

通过为用户授权角色实现角色与用户的关联。将有效的用户角色成功授权给用户后，登录设备的用户才能以各角色所具有的权限来配置、管理或者监控设备。根据用户登录设备时采用的不同认证方式，可以将为用户授权角色分为 AAA（Authentication、Authorization、Accounting，认证、授权、计费）方式和非 AAA 方式。

- AAA 方式: 用户登录时使用的认证方式为 **scheme**，用户登录设备后所拥有的用户角色由 AAA 功能进行授权。
 - 若用户通过了本地授权，则由设备为其授权用户角色，授权的用户角色是在本地用户中设置的。

- 若用户通过了远程授权，则由远程 AAA 服务器为其授权用户角色，授权的用户角色是在远程 AAA 服务器（RADIUS 或 HWTACACS 服务器）上设置的。
- 非 AAA 方式：用户登录时使用的认证方式为 **none** 或者 **password**，用户登录后所拥有的用户角色是用户线下配置的用户角色。SSH 用户通过 **publickey** 或 **password-publickey** 认证登录服务器，登录后将被授予同名的设备管理类本地用户视图下配置的授权用户角色。

以上两种方式均支持对一个用户同时授权多个用户角色。拥有多个角色的用户可获得这些角色中被允许执行的功能以及被允许操作的资源的集合。例如，某用户拥有角色 A，它禁止用户执行 **qos apply policy** 命令，且仅允许操作接口 2。同时，该用户拥有角色 B，它允许用户执行 **qos apply policy** 命令，且允许用户操作所有接口。则，这种情况下该用户将能够在所有接口下执行 **qos apply policy** 命令，以及可以操作所有的接口资源。

AAA 相关内容的介绍请参见“安全配置指导”中的“AAA”。用户线相关内容的介绍请参见“基础配置指导”中的“登录设备”。

1.2 FIPS相关说明

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”。

1.3 RBAC配置任务简介

RBAC 配置任务如下：

- (1) [创建用户角色](#)
- (2) [配置用户角色规则](#)
- (3) （可选）[配置特性组](#)
- (4) [配置资源控制策略](#)
 - [配置接口资源控制策略](#)
 - [配置VLAN资源控制策略](#)
- (5) [为用户授权角色](#)
 - [使能缺省用户角色授权功能](#)
 - [为远程AAA认证用户授权角色](#)
 - [为本地AAA认证用户授权角色](#)
 - [为非AAA认证用户授权角色](#)
- (6) [配置用户角色切换](#)
 - a. [配置用户角色切换的认证方式](#)
 - b. [配置用户角色切换的缺省目的用户角色](#)
 - c. [配置用户角色切换的密码](#)
 - d. [（可选）配置用户角色切换认证时使用用户登录的用户名认证](#)
 - e. [切换用户角色](#)

1.4 创建用户角色

1. 功能简介

如果系统预定义角色无法满足用户的权限管理需求，可以自定义用户角色来对用户权限做更精细和灵活的控制。除系统预定义的用户角色外，系统中最多允许同时创建 64 个用户角色。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 创建用户角色，并进入用户角色视图。

```
role name role-name
```

缺省情况下，系统预定义的用户角色为 **network-admin**、**network-operator**、**level-n**（n 为 0～15 的整数）、**security-audit**。其中，仅用户角色 **level-0**～**level-14** 可以自定义规则、资源控制策略以及配置描述信息。

- (3) （可选）配置用户角色描述信息。

```
description text
```

缺省情况下，未定义用户角色描述信息。

1.5 配置用户角色规则

1. 功能简介

一个用户角色中可以包含多条用户角色规则，每条规则定义了是允许或禁止用户对某命令、特性、特性组、Web 菜单、XML 元素或者 OID 进行操作。

- 基于非 OID 的规则匹配
 - 一个用户角色中可以定义多条规则，各规则以创建时指定的编号为唯一标识，被授权该角色的用户可以执行的命令为这些规则中定义的可执行命令的并集。若这些规则定义的权限内容有冲突，则规则编号大的有效。例如，角色中存在“rule 1 permit command ping”，“rule 2 permit command tracert”和“rule 3 deny command ping”，其中 rule 1 和 rule 3 冲突，规则编号大的 rule 3 生效，匹配的结果为用户禁止执行 ping 命令，允许执行 tracert 命令。
 - 同时存在系统预定义规则和自定义规则的用户角色时，若预定义规则定义的权限内容与自定义规则定义的权限内容有冲突，则以自定义规则为准。
- 基于 OID 的规则匹配
 - 与用户访问的 OID 形成最长匹配的规则生效。例如用户访问的 OID 为 1.3.6.1.4.1.25506.141.3.0.1，角色中存在“rule 1 permit read write oid 1.3.6”，“rule 2 deny read write oid 1.3.6.1.4.1”和“rule 3 permit read write oid 1.3.6.1.4”，其中 rule 2 与用户访问的 OID 形成最长匹配，则认为 rule 2 与 OID 匹配，匹配的结果为用户的此访问请求被拒绝。
 - 对于定义的 OID 长度相同的规则，规则编号大的生效。例如用户访问的 OID 为 1.3.6.1.4.1.25506.141.3.0.1，角色中存在“rule 1 permit read write oid 1.3.6”，“rule 2 deny

read write oid 1.3.6.1.4.1”和“rule 3 permit read write oid 1.3.6.1.4.1”，其中 rule 2 和 rule 3 与访问的 OID 形成最长匹配，则 rule 3 生效，匹配的结果为用户的访问请求被允许。

2. 配置限制和指导

- 只有具有 network-admin 或者 level-15 用户角色的用户登录设备后才具有如下命令的操作权限，其它系统预定义角色和用户自定义角色不能执行相应的命令。
 - **display history-command all** 命令。
 - 以 **display role**、**reboot**、**startup saved-configuration** 开头的所有命令。
 - 系统视图下以 **role**、**undo role**、**super**、**undo super**、**password-recovery**、**undo password-recovery** 开头的所有命令。
 - 系统视图下创建 SNMP 团体、用户或组的命令：**snmp-agent community**、**snmp-agent usm-user** 和 **snmp-agent group**。
 - 用户线视图下以 **user-role**、**undo user-role**、**authentication-mode**、**undo authentication-mode**、**set authentication password**、**undo set authentication password** 开头的所有命令。
 - Schedule 视图下以 **user-role**、**undo user-role** 开头的所有命令。
 - CLI 监控策略视图下以 **user-role**、**undo user-role** 开头的所有命令。
- 每个用户角色中最多可以配置 256 条规则，系统中的用户角色规则总数不能超过 1024。
- 修改后的规则对于当前已经在线的用户不生效，对于之后使用该角色登录设备的用户生效。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入用户角色视图。

```
role name role-name
```

- (3) 配置用户规则。请至少选择其中一项进行配置。

- 配置基于命令的规则。

```
rule number { deny | permit } command command-string
```

- 配置基于特性的规则。

```
rule number { deny | permit } { execute | read | write } * feature  
[ feature-name ]
```

- 配置基于特性组的规则。

```
rule number { deny | permit } { execute | read | write } * feature-group  
feature-group-name
```

只有特性组创建后，基于特性组的规则才能生效。

- 配置基于 Web 菜单的规则。

```
rule number { deny | permit } { execute | read | write } * web-menu  
[ web-string ]
```

- 配置基于 XML 元素的规则。

```
rule number { deny | permit } { execute | read | write } * xml-element  
[ xml-string ]
```

- 配置基于 OID 的规则。

```
rule number { deny | permit } { execute | read | write } * oid oid-string
```

1.6 配置特性组

1. 功能简介

特性组是一个或者多个特性的集合。配置特性组便于管理员为有相同权限需求的多个特性定义统一的用户角色规则。除系统预定义的特性组之外，最多允许创建 64 个特性组，且各特性组之间包含的特性允许重叠。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 创建特性组，并进入特性组视图。

```
role feature-group name feature-group-name
```

缺省情况下，存在两个系统预定义特性组，名称为 L2 和 L3，且不能被修改和删除。

- L2：包含所有二层协议相关功能的命令。
- L3：包含所有三层协议相关功能的命令。

- (3) 向特性组中添加一个特性。

```
feature feature-name
```

缺省情况下，自定义特性组中不包含任何特性。

1.7 配置资源控制策略

1.7.1 功能简介

资源控制策略分为接口策略、VLAN 策略。所有用户角色均具有缺省的资源控制策略，允许用户具有操作任何系统资源的权限。若要限制或区分用户对这些资源的使用权限，则应该配置资源控制策略并在指定类型的策略中配置允许操作的资源列表。

1.7.2 配置限制和指导

修改后的资源控制策略对于当前已经在线的用户不生效，对于之后使用该角色登录设备的用户生效。

1.7.3 配置接口资源控制策略

- (1) 进入系统视图。

```
system-view
```

- (2) 进入用户角色视图。

```
role name role-name
```

- (3) 进入接口策略视图。

```
interface policy deny
```

缺省情况下，用户角色具有操作任何接口的权限。

进入接口策略视图后，如果不配置允许操作的接口列表，则用户角色将没有操作任何接口的权限。

- (4) （可选）配置允许操作的接口列表。

```
permit interface interface-list
```

缺省情况下，未定义允许操作的接口列表，用户角色没有操作任何接口的权限。

可以多次执行此命令向接口列表中添加允许操作的接口。

1.7.4 配置VLAN资源控制策略

- (1) 进入系统视图。

```
system-view
```

- (2) 进入用户角色视图。

```
role name role-name
```

- (3) 进入 VLAN 策略视图。

```
vlan policy deny
```

缺省情况下，用户具有操作任何 VLAN 的权限。

进入 VLAN 策略视图后，如果不配置允许操作的 VLAN 列表，则用户将没有操作任何 VLAN 的权限。

- (4) （可选）配置允许操作的 VLAN 列表。

```
permit vlan vlan-id-list
```

缺省情况下，未定义允许操作的 VLAN 列表，用户没有操作任何 VLAN 的权限。

可以多次执行此命令向 VLAN 列表中添加允许操作的 VLAN。

1.8 为用户授权角色

1.8.1 配置限制和指导

为保证对用户授权角色成功，设备上必须存在对应的被授权的用户角色。若要授权的用户角色有多个，则只要被授权的用户角色中的一个或多个在设备上存在，相应的用户角色即可授权成功；若设备上不存在任何一个被授权的用户角色，则用户角色授权将会失败。

1.8.2 使能缺省用户角色授权功能

1. 功能简介

对于通过 AAA 认证登录设备的用户，由服务器（远程认证服务器或本地认证服务器）为其授权用户角色。如果用户没有被授权任何用户角色，将无法成功登录设备，需要使能缺省用户角色授权功能。为此，设备提供了一个缺省用户角色授权功能。使能该功能后，用户在没有被服务器授权任何角色的情况下，将具有一个缺省的用户角色，该缺省用户角色可以通过参数配置为系统中已存在的任意用户角色。

2. 配置步骤

- (1) 进入系统视图。

system-view

- (2) 使能缺省用户角色授权功能。

role default-role enable [*role-name*]

缺省情况下，缺省用户角色授权功能处于关闭状态。

若未通过 **authorization-attribute** 命令配置本地用户或用户组的授权属性，则必须使能缺省用户角色授权功能。关于命令 **authorization-attribute** 的详细介绍请参见“安全配置命令参考”的“AAA”。

1.8.3 为远程AAA认证用户授权角色

对于通过 AAA 远程认证登录设备的用户，由 AAA 服务器的配置决定为其授权的用户角色。有关 AAA 以及远程 AAA 认证相关配置的详细介绍请参见“安全配置指导”中的“AAA”。

RADIUS 服务器上的授权角色配置与服务器的具体情况有关，请参考服务器的配置指导进行；HWTACACS 服务器上的授权角色配置必须满足格式：**roles="name1 name2 namen"**，其中 name1、name2、namen 为要授权下发给用户的用户角色，可为多个，并使用空格分隔。

需要注意的是，若 AAA 服务器同时为用户授权了包括安全日志管理员在内的多个用户角色，则仅安全日志管理员角色生效。

1.8.4 为本地AAA认证用户授权角色

1. 功能简介

对于通过本地 AAA 认证登录设备的用户，由本地用户配置决定为其授权的用户角色。有关 AAA 以及本地用户相关配置的详细介绍请参见“安全配置指导”中的“AAA”。

2. 配置限制和指导

- 由于本地用户缺省就拥有一个用户角色，如果要赋予本地用户新的用户角色，请确认是否需要保留这个缺省的用户角色，若不需要，请删除。
- 系统中的最后一个安全日志管理员角色的本地用户不可被删除。
- 安全日志管理员与其它用户角色互斥，为一个本地用户授权安全日志管理员角色时，经过界面的交互式确认后，系统会自动删除当前用户的所有其它用户角色。
- 如果已经为当前本地用户授权了安全日志管理员角色，再授权其它的用户角色时，经过界面的交互确认后，系统会自动删除当前用户的安全日志管理员角色。
- 可通过多次执行该配置，为本地用户授权多个用户角色，最多可授权 64 个。

3. 配置步骤

- (1) 进入系统视图。

system-view

- (2) 创建本地用户，并进入本地用户视图。

local-user *user-name* **class** { **manage** | **network** }

- (3) 为本地用户授权用户角色。

authorization-attribute **user-role** *role-name*

缺省情况下，由用户角色为 **network-admin** 或 **level-15** 的用户创建的本地用户将被授权用户角色 **network-operator**。

1.8.5 为非AAA认证用户授权角色

1. 功能简介

对于不使用 AAA 认证登录设备的非 SSH 用户，由用户线配置决定为其授权的用户角色。有关用户线相关配置的详细介绍请参见“基础配置指导”中的“登录设备”。

通过 **publickey** 或 **password-publickey** 认证登录设备的 SSH 用户，由同名的设备管理类本地用户配置决定为其授权的用户角色。SSH 用户相关的介绍请参见“安全配置指导”中的“SSH”。

2. 配置限制和指导

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。

不能为从当前用户线登录系统的用户授权安全日志管理员的用户角色。

3. 配置步骤

(1) 进入系统视图。

```
system-view
```

(2) 进入用户线或用户线类视图。

○ 进入用户线视图。

```
line { first-num1 [ last-num1 ] | { aux | vty } first-num2 [ last-num2 ] }
```

○ 进入用户线类视图。

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

关于用户线和用户线视图下各属性生效情况和优先级的详细介绍，请参见“基础配置指导”中的“配置通过 CLI 登录设备”。

(3) 为从当前用户线登录系统的用户配置授权的用户角色。

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

缺省情况下，使用 **AUX** 用户线登录系统的用户将被授权用户角色 **network-admin**；通过其它用户线登录系统的用户将被授权用户角色 **network-operator**。

1.9 配置用户角色切换

1.9.1 功能简介

切换用户角色是指在不退出当前登录、不断开当前连接的前提下修改用户的用户角色，改变用户所拥有的命令行权限。切换后的用户角色只对当前登录生效，用户重新登录后，又会恢复到原有角色。

- 为了防止对设备的误操作，通常情况下建议管理员使用较低权限的用户角色登录设备、查看设备运行参数，当需要对设备进行维护时，再临时切换到较高权限的用户角色。
- 当管理员需要暂时离开设备或者将设备暂时交给其它人代为管理时，为了安全起见，可以临时切换到较低权限的用户角色，来限制其他人员的操作。
- 为了保证操作的安全性，通常用户进行用户角色切换时，均需要输入用户角色切换密码。切换到不同的用户角色时，需要输入相应切换密码。如果服务器没有响应或者没有配置用户角

色切换密码，则切换操作失败，若还有备份认证方案，则转而进行备份认证。设备支持如 [表 1-2](#) 所示的四种用户角色切换认证方式。

表1-2 用户角色的切换认证方式

认证方式	涵义	说明
local	本地密码认证	<p>设备验证用户输入的用户角色切换密码</p> <p>使用该方式时，需要在设备上使用 super password 命令设置用户角色切换密码</p> <p>对于 Console 口登录的用户，在设备仅采用本地密码切换认证方式且未配置切换密码的情况下，设备不关心用户是否输入切换密码以及输入切换密码的内容，可允许用户成功切换用户角色</p>
scheme	通过HWTACACS或RADIUS进行远程AAA认证	<p>设备将用户角色切换使用的用户名和密码发送给 HWTACACS/RADIUS 服务器进行远程验证</p> <p>使用该方式时，需要进行以下相关配置：</p> <ul style="list-style-type: none"> 在设备上配置 HWTACACS/RADIUS 方案，并在 ISP 域中引用已创建的 HWTACACS/RADIUS 方案，详细介绍请参见“安全配置指导”中的“AAA” 在 HWTACACS/RADIUS 服务器上创建相应的用户并配置密码
local scheme	先本地密码认证，后远程AAA认证	<p>先进行本地密码认证，若设备上未设置本地用户角色切换密码，使用 VTY 用户线登录的用户则转为远程 AAA 认证，使用 AUX 用户线登录的用户则可以成功切换用户角色</p>
scheme local	先远程AAA认证，后本地密码认证	<p>先进行远程 AAA 认证，远程 HWTACACS/RADIUS 服务器无响应或设备上的 AAA 远程认证配置无效时，转为本地密码认证</p>

1.9.2 配置限制和指导

- 在进行切换操作前，请先保证配置了正确的用户角色切换密码。
- 当使用 HWTACACS 方案进行用户角色切换认证时，若未配置用户角色切换认证时使用用户登录的用户名认证，则系统使用用户输入的用户角色切换用户名进行角色切换认证，HWTACACS 服务器上也必须存在相应的用户。
 - 当用户要切换到 **level-*n*** 的用户角色时，要求 HWTACACS 服务器上存在能提供切换到 **level-*n*** 角色的用户。在 HWTACACS 服务器上，支持切换到用户角色 **level-*n*** 的用户也能够支持切换到 **level-0** 到 **level-*n*** 之间任意的用户角色。
 - 当用户要切换到非 **level-*n*** 的用户角色时，要求 HWTACACS 服务器上存在至少能提供切换到 **level-0** 角色的用户，且该用户配置了取值为 **allowed-roles="role"** 的自定义属性（其中 **role** 为要切换的目的用户角色名称）。
- 当使用 RADIUS 方案进行用户角色切换认证时，系统使用 “\$enab*n*\$” 形式的用户名进行用户角色切换认证，其中 *n* 为用户希望切换到的用户角色 **level-*n*** 中的 *n*，RADIUS 服务器上也必须存在该形式用户名的用户。与 HWTACACS 不同的是，用户进行角色切换时可输入任意用户名，该名称在认证过程中无实际意义。
 - 当用户要切换到 **level-*n*** 的用户角色时，要求 RADIUS 服务器上存在用户名为 “\$enab*n*\$” 的用户。例如，用户希望切换到用户角色 **level-3**，输入任意用户名，系统忽略用户输入的用户名，使用 “\$enab3\$” 形式的用户名进行用户角色切换认证。

- 当用户要切换到非 **level-n** 的用户角色时，要求 RADIUS 服务器上存在用户名为 “\$enab0\$” 的用户，且该用户配置了取值为 **allowed-roles=“role”** 的自定义属性（其中 **role** 为要切换的目的用户角色名称）。
- 用户进行用户角色切换认证时，系统发送给 RADIUS 服务器的认证请求报文中的用户名中不会携带域名，系统采用的切换认证方案使用缺省域。
- 用户进行用户角色切换认证时，系统发送给 HWTACACS 服务器的认证请求报文中的用户名是否携带域名由配置决定（**user-name-format**），系统采用的切换认证方案由用户输入的用户名中指定的域名决定，若该用户名中未携带域名，则使用缺省域。
- 当用户从用户角色 **a** 切换到用户角色 **b** 后，若输入 **quit** 命令，将退出当前登录的用户线。

1.9.3 配置用户角色切换的认证方式

- (1) 进入系统视图。
system-view
- (2) 配置用户角色切换时的认证方式。
super authentication-mode { local | scheme } *
缺省情况下，采用 **local** 认证方式。

1.9.4 配置用户角色切换的缺省目的用户角色

- (1) 进入系统视图。
system-view
- (2) 配置用户角色切换的缺省目的用户角色。
super default role role-name
缺省情况下，用户角色切换的缺省目的角色为 **network-admin**。

1.9.5 配置用户角色切换的密码

1. 功能简介

如果用户角色的切换认证方式采用 **local** 认证方式，则需要配置用户角色切换的密码。如果采用 **scheme** 认证方式则无需此配置。

2. 配置步骤

- (1) 进入系统视图。
system-view
- (2) 配置用户角色切换的密码。
(非 FIPS 模式)
super password [role role-name] [{ hash | simple } string]
(FIPS 模式)
super password [role role-name]
缺省情况下，未设置切换用户角色的密码。
若不指定用户角色，则设置的是切换到当前缺省目的用户角色的密码。

1.9.6 配置用户角色切换认证时使用用户登录的用户名认证

1. 功能简介

在设备采用远程 AAA 认证方案进行用户角色切换认证，且用户采用用户名和密码方式登录设备的情况下，用户切换用户角色时，设备会自动获取用户登录使用的用户名作为角色切换认证的用户名，不再需要用户输入用户名。

2. 配置限制和指导

开启本功能后，若设备采用远程 AAA 认证方案进行用户角色切换认证，但用户未采用用户名和密码方式登录设备，则用户角色切换失败。

若设备未采用远程 AAA 认证方案进行用户角色切换认证，则本功能配置无法生效。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 配置用户角色切换认证时使用用户登录的用户名认证。

```
super use-login-username
```

缺省情况下，用户角色切换认证时系统提示用户输入用户名进行认证。

1.9.7 切换用户角色

1. 配置限制和指导

用户最多可以连续进行三次切换认证，如果三次认证都失败则本轮切换失败。

如果用户登录认证和用户角色切换认证使用相同的域，为保证用户能够成功切换非 **level** 角色，建议两者采用相同的 AAA 方案，即均为本地认证或均为远程认证。

2. 配置准备

若要执行切换用户角色的操作，必须保证当前用户具有执行本命令的权限。

3. 配置步骤

请在用户视图下执行本命令，切换用户角色。

```
super [ role-name ]
```

若不指定用户角色，则切换到当前缺省目的用户角色。缺省的目的用户角色由 **super default role** 命令指定。

1.10 RBAC显示和维护

完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后 RBAC 的运行情况，通过查看显示信息验证配置的效果。

表1-3 RBAC 显示和维护

操作	命令
显示用户角色信息	display role [name <i>role-name</i>]
显示特性信息	display role feature [name <i>feature-name</i> verbose]

操作	命令
显示特性组信息	<code>display role feature-group [name feature-group-name] [verbose]</code>

1.11 RBAC典型配置举例

1.11.1 Telnet用户的本地用户角色授权配置举例

1. 组网需求

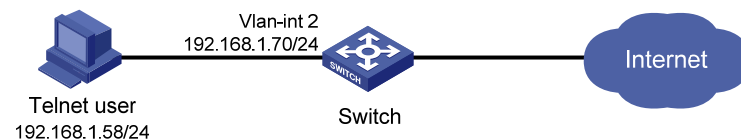
如 图 1-1 所示，Telnet 用户主机与 Switch 相连，需要实现 Switch 对 Telnet 用户进行本地认证并授权用户角色。Telnet 用户的登录用户名为 user1@bbb，认证通过后被授权的用户角色为 role1。

role1 具有如下用户权限：

- 允许用户执行所有特性中读类型的命令；
- 允许用户执行创建 VLAN 以及进入 VLAN 视图后的相关命令，并只具有操作 VLAN 10～VLAN 20 的权限。

2. 组网图

图1-1 Telnet 用户本地认证/授权配置组网图



3. 配置步骤

配置 VLAN 接口 2 的 IP 地址，Telnet 用户将通过该地址连接 Switch。

```

<Switch> system-view
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] ip address 192.168.1.70 255.255.255.0
[Switch-Vlan-interface2] quit
  
```

开启 Switch 的 Telnet 服务器功能。

```
[Switch] telnet server enable
```

配置 Telnet 用户登录采用 AAA 认证方式。

```

[Switch] line vty 0 63
[Switch-line-vty0-63] authentication-mode scheme
[Switch-line-vty0-63] quit
  
```

配置 ISP 域 bbb 的 AAA 方法为本地认证和本地授权。

```

[Switch] domain bbb
[Switch-isp-bbb] authentication login local
[Switch-isp-bbb] authorization login local
[Switch-isp-bbb] quit
  
```

创建用户角色 role1。

```
[Switch] role name role1
```

配置用户角色规则 1，允许用户执行所有特性中读类型的命令。

```
[Switch-role-role1] rule 1 permit read feature
```

配置用户角色规则 2，允许用户执行创建 VLAN 以及进入 VLAN 视图后的相关命令。

```
[Switch-role-role1] rule 2 permit command system-view ; vlan *
```

进入 VLAN 策略视图，允许用户具有操作 VLAN 10~VLAN 20 的权限。

```
[Switch-role-role1] vlan policy deny
```

```
[Switch-role-role1-vlanpolicy] permit vlan 10 to 20
```

```
[Switch-role-role1-vlanpolicy] quit
```

```
[Switch-role-role1] quit
```

创建设备管理类本地用户 user1。

```
[Switch] local-user user1 class manage
```

配置用户的密码是明文的 aabbcc。

```
[Switch-luser-manage-user1] password simple aabbcc
```

指定用户的服务类型是 Telnet。

```
[Switch-luser-manage-user1] service-type telnet
```

指定用户 user1 的授权角色为 role1。

```
[Switch-luser-manage-user1] authorization-attribute user-role role1
```

为保证用户仅使用授权的用户角色 role1，删除用户 user1 具有的缺省用户角色 network-operator。

```
[Switch-luser-manage-user1] undo authorization-attribute user-role network-operator
```

```
[Switch-luser-manage-user1] quit
```

4. 验证配置

用户向 Switch 发起 Telnet 连接，在 Telnet 客户端按照提示输入用户名 user1@bbb 及正确的密码后，可成功登录 Switch，并被授予用户角色 role1，具有相应的命令行执行权限。

可通过如下步骤验证用户的权限：

- 可操作 VLAN 10~VLAN 20。（以创建 VLAN 10 为例）

```
<Switch> system-view
[Switch] vlan 10
[Switch-vlan10] quit
```
- 不能操作其它 VLAN。（以创建 VLAN 30 为例）

```
[Switch] vlan 30
Permission denied.
```
- 可执行所有特性中读类型的命令。（以 **display clock** 为例）

```
[Switch] display clock
09:31:56.258 UTC Sat 01/01/2018
[Switch] quit
```
- 不能执行特性中写类型和执行类型的命令。

```
<Switch> debugging role all
Permission denied.
<Switch> ping 192.168.1.58
Permission denied.
```

1.11.2 Telnet用户的RADIUS用户角色授权配置举例

1. 组网需求

如 图 1-2 所示, Telnet用户主机与Switch相连, Switch与一台RADIUS服务器相连, 要实现RADIUS服务器对登录Switch的Telnet用户进行认证和授权。

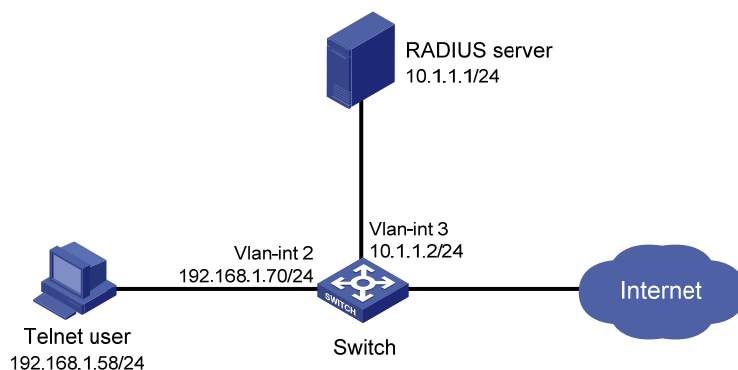
- 由一台 FreeRadius 服务器 (IP 地址为 10.1.1.1/24) 担当认证/授权 RADIUS 服务器的职责;
- Switch 与 RADIUS 服务器交互报文时使用的共享密钥为 expert, 认证端口号为 1812;
- Switch 向 RADIUS 服务器发送的用户名携带域名;
- Telnet 用户登录 Switch 时使用 RADIUS 服务器上配置的用户名 hello@bbb 以及密码进行认证, 认证通过后被授权的用户角色为 role2。

role2 具有如下用户权限:

- 允许用户执行 ISP 视图下的所有命令;
- 允许用户执行 ARP 和 RADIUS 特性中读和写类型的命令;
- 禁止用户执行 ACL 特性中读类型的命令;
- 允许用户执行创建 VLAN 以及进入 VLAN 视图后的相关命令, 并只具有操作 VLAN 1~VLAN 20 的权限;
- 允许用户执行进入接口视图以及接口视图下的相关命令, 并具有操作接口 GigabitEthernet1/0/1~GigabitEthernet1/0/4 的权限。

2. 组网图

图1-2 Telnet 用户 RADIUS 认证/授权配置组网图



3. 配置步骤

(1) Switch 上的配置

配置接口 VLAN 接口 2 的 IP 地址, Telnet 用户将通过该地址连接 Switch。

```
<Switch> system-view
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] ip address 192.168.1.70 255.255.255.0
[Switch-Vlan-interface2] quit
```

配置接口 VLAN 接口 3 的 IP 地址, Switch 将通过该地址与服务器通信。

```
[Switch] interface vlan-interface 3
[Switch-Vlan-interface3] ip address 10.1.1.2 255.255.255.0
[Switch-Vlan-interface3] quit
```

```

# 开启 Switch 的 Telnet 服务器功能。
[Switch] telnet server enable

# 配置 Telnet 用户登录采用 AAA 认证方式。
[Switch] line vty 0 63
[Switch-line-vty0-63] authentication-mode scheme
[Switch-line-vty0-63] quit

# 创建 RADIUS 方案 rad。
[Switch] radius scheme rad

# 配置主认证/授权服务器的 IP 地址为 10.1.1.1，认证端口号为 1812。
[Switch-radius-rad] primary authentication 10.1.1.1 1812

# 配置与认证/授权服务器交互报文时的共享密钥为明文 expert。
[Switch-radius-rad] key authentication simple expert
[Switch-radius-rad] quit

# 配置 ISP 域 bbb 的 AAA 方法。由于 RADIUS 服务器的授权信息是随认证应答报文发给 RADIUS 客户端的，所以必须保证认证和授权方法相同。
[Switch] domain bbb
[Switch-isp-bbb] authentication login radius-scheme rad
[Switch-isp-bbb] authorization login radius-scheme rad
[Switch-isp-bbb] accounting login none
[Switch-isp-bbb] quit

# 创建特性组 fgroup1。
[Switch] role feature-group name fgroup1

# 配置特性组 fgroup1 中包含特性 ARP 和 RADIUS。
[Switch-featuregrp-fgroup1] feature arp
[Switch-featuregrp-fgroup1] feature radius
[Switch-featuregrp-fgroup1] quit

# 创建用户角色 role2。
[Switch] role name role2

# 配置用户角色规则 1，允许用户执行 ISP 视图下的所有命令。
[Switch-role-role2] rule 1 permit command system-view ; domain *

# 配置用户角色规则 2，允许用户执行特性组 fgroup1 中所有特性的读和写类型的命令。
[Switch-role-role2] rule 2 permit read write feature-group fgroup1

# 配置用户角色规则 3，禁止用户执行 ACL 特性中读类型的命令。
[Switch-role-role2] rule 3 deny read feature acl

# 配置用户角色规则 4，允许用户执行创建 VLAN 以及进入 VLAN 视图后的相关命令。
[Switch-role-role2] rule 4 permit command system-view ; vlan *

# 配置用户角色规则 5，允许用户执行进入接口视图以及接口视图下的相关命令。
[Switch-role-role2] rule 5 permit command system-view ; interface *

# 进入 VLAN 策略视图，允许用户具有操作 VLAN 1～VLAN 20 的权限。
[Switch-role-role2] vlan policy deny
[Switch-role-role2-vlanpolicy] permit vlan 1 to 20
[Switch-role-role2-vlanpolicy] quit

# 进入接口策略视图，允许用户具有操作接口 GigabitEthernet1/0/1～GigabitEthernet1/0/4 的权限。

```



```
[Switch-role-role2] interface policy deny
[Switch-role-role2-ifpolicy] permit interface gigabitethernet 1/0/1 to gigabitethernet
1/0/4
[Switch-role-role2-ifpolicy] quit
[Switch-role-role2] quit
```

(2) RADIUS 服务器的配置

需要在 **FreeRadius** 服务器的字典文件中增加如下配置文本之一：

```
Cisco-AVPair = "shell:roles=\"role2\""
```

```
Cisco-AVPair = "shell:roles*\"role2\""
```

关于 **FreeRadius** 的其它配置请参见服务器的相关手册，本文不进行详细介绍。

4. 验证配置

用户向 **Switch** 发起 **Telnet** 连接，在 **Telnet** 客户端按照提示输入用户名 **hello@bbb** 及正确的密码后，可成功登录 **Switch**，并被授予用户角色 **role2**，具有相应的命令行执行权限。

可通过如下命令验证用户的权限：

- 可执行 **ISP** 视图下所有的命令。

```
<Switch> system-view
[Switch] domain abc
[Switch-isp-abc] authentication login radius-scheme abc
[Switch-isp-abc] quit
```

- 可执行 **RADIUS** 特性中读和写类型的命令。（**ARP** 特性同，此处不再举例）

```
[Switch] radius scheme rad
[Switch-radius-rad] primary authentication 2.2.2.2
[Switch-radius-rad] display radius scheme rad
```

RADIUS 方案的显示信息此处略。

- 可操作 **VLAN 1~VLAN 20**。（以创建 **VLAN 10**、**VLAN 30** 为例）

```
[Switch] vlan 10
[Switch-vlan10] quit
[Switch] vlan 30
Permission denied.
```

- 可操作接口 **GigabitEthernet1/0/1~GigabitEthernet1/0/4**。（以接口 **GigabitEthernet1/0/2**、**GigabitEthernet1/0/5** 为例）

```
[Switch] vlan 10
# 将接口 GigabitEthernet1/0/2 加入到 VLAN 10。
[Switch-vlan10] port gigabitethernet 1/0/2
# 将接口 GigabitEthernet1/0/5 加入到 VLAN 10。
[Switch-vlan10] port gigabitethernet 1/0/5
Permission denied.
```

1.11.3 Telnet用户的HWTACACS用户角色切换认证配置举例

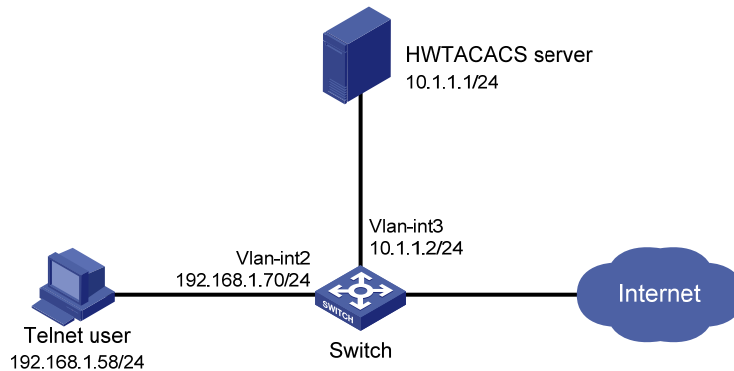
1. 组网需求

如 [图 1-3](#) 所示，**Telnet** 用户主机与 **Switch** 直接相连，**Switch** 与一台 **HWTACACS** 服务器相连，需要配置 **Switch** 实现对登录 **Switch** 的 **Telnet** 用户进行用户角色切换认证。具体要求如下：

Telnet 用户登录 Switch 时进行 HWTACACS 认证, 登录后被授予用户角色 level-0, 当进行 level-0~level3 之间的任意用户角色切换或切换到 network-admin 用户角色时, 首先使用 HWTACACS 认证, 若 AAA 配置无效或者 HWTACACS 服务器没有响应则转为 local 认证。

2. 组网图

图1-3 Telnet 用户远端 HWTACACS 用户角色切换认证配置组网图



3. 配置思路

在交换机上的配置思路如下：

- (1) 配置 Telnet 用户登录采用 AAA 认证方式(**scheme**), 并且使用 AAA 中的 HWTACACS 认证。
 - 创建 ISP 域 bbb, 配置 Telnet 用户登录时认证方法为 HWTACACS 方案 hwtac 和授权方法为 HWTACACS 方案 hwtac。
 - 在 HWTACACS server 上需要添加 Telnet 用户登录密码及登录后的用户角色。
- (2) Telnet 用户进行用户角色切换时, 首先使用 HWTACACS 认证, 若 AAA 配置无效或者 HWTACACS 服务器没有响应则转为本地认证。
 - 配置用户角色切换认证方式为 **scheme local**。
 - 配置 HWTACACS 方案 hwtac, 指定 HWTACACS 服务器 IP 地址及与其进行交互的相关参数 (HWTACACS 协议报文交互时使用的共享密钥, Switch 发送给 HWTACACS 服务器的用户名不带域名)。在 ISP 域 bbb 下配置用户角色切换认证方法为 hwtac。
 - 配置采用本地认证方式时的用户角色切换密码。

在 HWTACACS server 上需要添加用于用户角色切换认证的用户名和密码。

4. 配置步骤

(1) 配置 Switch

配置 VLAN 接口 2 的 IP 地址, Telnet 客户端将通过该地址连接 Switch。

```
<Switch> system-view
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] ip address 192.168.1.70 255.255.255.0
[Switch-Vlan-interface2] quit
```

配置 VLAN 接口 3 的 IP 地址, Switch 将通过该地址与服务器通信。

```
[Switch] interface vlan-interface 3
[Switch-Vlan-interface3] ip address 10.1.1.2 255.255.255.0
[Switch-Vlan-interface3] quit
```

```

# 开启 Switch 的 Telnet 服务器功能。
[Switch] telnet server enable
# 配置 Telnet 用户登录采用 AAA 认证方式。
[Switch] line vty 0 15
[Switch-line-vty0-15] authentication-mode scheme
[Switch-line-vty0-15] quit
# 配置进行用户角色切换时的认证方式为 scheme local。（首先使用 HWTACACS 认证，
若 AAA 配置无效或者 HWTACACS 服务器没有响应则转为本地认证）
[Switch] super authentication-mode scheme local
# 创建 HWTACACS 方案 hwtac。
[Switch] hwtacacs scheme hwtac
# 配置主认证服务器的 IP 地址为 10.1.1.1，认证端口号为 49。
[Switch-hwtacacs-hwtac] primary authentication 10.1.1.1 49
# 配置主授权服务器的 IP 地址为 10.1.1.1，认证端口号为 49。
[Switch-hwtacacs-hwtac] primary authorization 10.1.1.1 49
# 配置与认证服务器交互报文时的共享密钥为 expert。
[Switch-hwtacacs-hwtac] key authentication simple expert
# 配置与授权服务器交互报文时的共享密钥为 expert。
[Switch-hwtacacs-hwtac] key authorization simple expert
# 配置向 HWTACACS 服务器发送的用户名不携带域名。
[Switch-hwtacacs-hwtac] user-name-format without-domain
[Switch-hwtacacs-hwtac] quit
# 创建 ISP 域 bbb。
[Switch] domain bbb
# 配置 Telnet 用户登录认证方法为 hwtac。
[Switch-isp-bbb] authentication login hwtacacs-scheme hwtac
# 配置 Telnet 用户登录授权方法为 hwtac。
[Switch-isp-bbb] authorization login hwtacacs-scheme hwtac
# 配置 Telnet 用户登录计费方法为 none。
[Switch-isp-bbb] accounting login none
# 配置用户角色切换认证方法为 hwtac。
[Switch-isp-bbb] authentication super hwtacacs-scheme hwtac
[Switch-isp-bbb] quit
# 配置用户角色切换认证方式为本地认证时，切换到用户角色 level-3 时使用的密码为 654321。
[Switch] super password role level-3 simple 654321
# 配置切换到用户角色 network-admin 时使用的密码为 654321。
[Switch] super password role network-admin simple 654321
[Switch] quit

```

(2) 配置 HWTACACS server



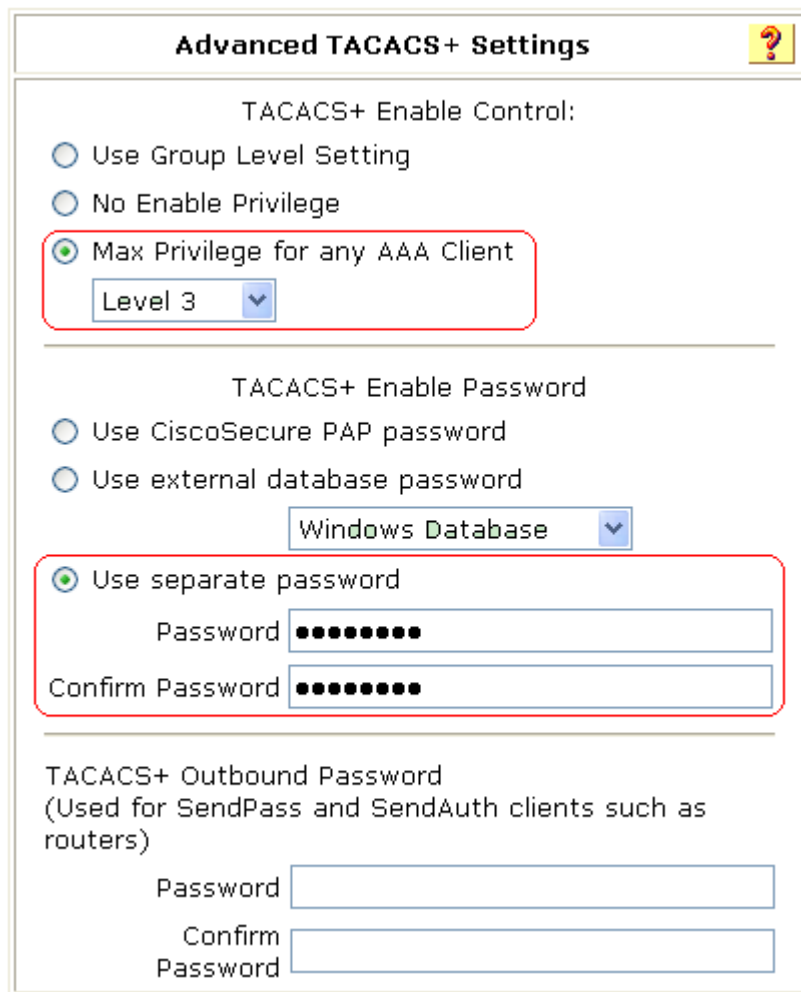
说明

下面以 ACSv4.0 为例，说明该例中 HWTACACS server 的基本配置。

在 HWTACACS server 上添加用户 test，对该用户的高级属性进行设置。

- 设置 Enable Password 为 enabpass;
- 设置 Max Privilege 为 Level 3，表示用户角色在 level-0 到 level-3 之间任意切换时均使用密码 enabpass 进行认证。如果目的切换角色仅仅为 network-admin，则 Max Privilege 可以设置为任意 Level。

图1-4 设置 Telnet 用户的高级属性



The image shows a screenshot of the 'Advanced TACACS+ Settings' dialog box. It has a title bar with a question mark icon. The dialog is divided into three main sections. The first section, 'TACACS+ Enable Control:', has three radio buttons: 'Use Group Level Setting', 'No Enable Privilege', and 'Max Privilege for any AAA Client'. The third option is selected and highlighted with a red box. Below it is a dropdown menu showing 'Level 3'. The second section, 'TACACS+ Enable Password', has two radio buttons: 'Use CiscoSecure PAP password' and 'Use external database password'. Below the second option is a dropdown menu showing 'Windows Database'. The third option, 'Use separate password', is selected and highlighted with a red box. Below it are two text input fields: 'Password' and 'Confirm Password', both containing eight black dots. The third section, 'TACACS+ Outbound Password (Used for SendPass and SendAuth clients such as routers)', has two text input fields: 'Password' and 'Confirm Password', both empty.

- 设置 Shell(exex)的 Custom attributes 属性字符串为 allowed-roles="network-admin"，多个角色可用空格间隔。

图1-5 设置 Telnet 用户的 HWTACACS 属性

The screenshot shows a configuration window for HWTACACS attributes. The 'Custom attributes' section is highlighted with a red box, showing the attribute 'allowed-roles=network-admin'. Other options include 'Shell (exec)', 'Access control list', 'Auto command', 'Callback line', 'Callback rotary', 'Idle time', 'No callback verify', 'No escape', 'No hangup', 'Privilege level', and 'Timeout'. Each option has a checkbox and a corresponding input field or status indicator.

5. 验证配置

(1) Telnet 用户建立与 Switch 的连接

在 Telnet 客户端按照提示输入用户名 `test@bbb` 及密码 `aabbcc`，即可成功登录 Switch，且只能访问指定权限的命令。

```
<Switch> telnet 192.168.1.70
Trying 192.168.1.70 ...
Press CTRL+K to abort
Connected to 192.168.1.70 ...
*****
* Copyright (c) 2004-2018 New H3C Technologies Co., Ltd. All rights reserved.*
* Without the owner's prior written consent,                               *
* no decompiling or reverse-engineering shall be allowed.                  *
*****

login: test@bbb
Password:
<Switch>?
User view commands:
ping          Ping function
quit          Exit from current command view
ssh2          Establish a secure shell client connection
super         Switch to a user role
system-view   Enter the System View
telnet        Establish a telnet connection
```

```
tracert      Tracert function
<Switch>
```

(2) 切换用户角色

在当前的用户线下执行切换到用户角色 **level-3** 的命令，按照提示输入 HWTACACS 用户角色切换认证密码 **enabpass**，若认证成功即可将当前 Telnet 用户的角色切换到 **level-3**。

```
<Switch> super level-3
Username: test@bbb
Password: <——此处需输入 HWTACACS 用户角色切换认证密码
User privilege role is level-3, and only those commands that authorized to the role can be used.
```

若 ACS 服务器无响应，按照提示输入本地用户角色切换认证密码 **654321**，若认证成功即可将当前 Telnet 用户的角色切换到 **level-3**。

```
<Switch> super level-3
Username: test@bbb
Password: <——此处需输入 HWTACACS 用户角色切换认证密码
Invalid configuration or no response from the authentication server.
Change authentication mode to local.
Password: <——此处需输入本地用户角色切换认证密码
User privilege role is level-3, and only those commands that authorized to the role can be used.
```

切换到用户角色 **level-0**、**level-1**、**level2**、**network-admin** 的过程同上。

1.11.4 Telnet 用户的RADIUS用户角色切换认证配置举例

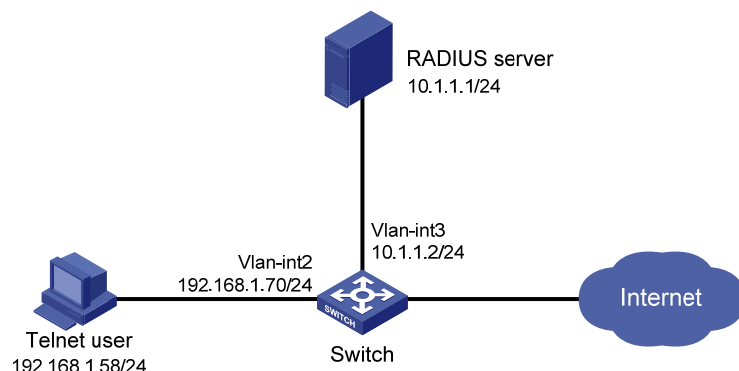
1. 组网需求

如 [图 1-6](#) 所示，Telnet 用户主机与 Switch 直接相连，Switch 与一台 RADIUS 服务器相连，需要配置 Switch 实现对登录 Switch 的 Telnet 用户进行用户级别切换认证。具体要求如下：

Telnet 用户登录 Switch 时进行 RADIUS 认证，登录后被授予用户角色 **level-0**，当切换到非 **level-*n***（本例切换到角色 **network-admin**）的用户角色时，首先使用 RADIUS 认证，若 AAA 配置无效或者 RADIUS 服务器没有响应则转为 **local** 认证。

2. 组网图

图1-6 Telnet 用户远端 RADIUS 用户角色切换认证配置组网图



3. 配置思路

在 Switch 上的配置思路如下：

- (1) 配置 Telnet 用户登录采用 AAA 认证方式 (**scheme**)，并且使用 AAA 中的 RADIUS 认证。
 - 创建 ISP 域 bbb，配置 Telnet 用户登录时认证方法为 RADIUS 方案 radius 和授权方法为 RADIUS 方案 radius。
 - 在 RADIUS server 上需要添加 Telnet 用户登录密码及登录后的用户角色。
 - (2) Telnet 用户进行用户角色切换时，首先使用 RADIUS 认证，若 AAA 配置无效或者 RADIUS 服务器没有响应则转为本地认证。
 - 配置用户角色切换认证方式为 **scheme local**。
 - 配置 RADIUS 方案 radius，指定 RADIUS 服务器 IP 地址及与其进行交互的相关参数（RADIUS 协议报文交互时使用的共享密钥，Switch 发送给 RADIUS 服务器的用户名不带域名）。在 ISP 域 bbb 下配置用户角色切换认证方法为 RADIUS 方案 radius。
 - 配置采用本地认证方式时的用户角色切换密码。
- 在 RADIUS server 上需要添加用于用户角色切换认证的用户名 “\$enab0\$” 和密码。

4. 配置步骤

- (1) 配置 Switch

配置 VLAN 接口 2 的 IP 地址，Telnet 客户端将通过该地址连接 Switch。

```
<Switch> system-view
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] ip address 192.168.1.70 255.255.255.0
[Switch-Vlan-interface2] quit
```

配置 VLAN 接口 3 的 IP 地址，Switch 将通过该地址与服务器通信。

```
[Switch] interface vlan-interface 3
[Switch-Vlan-interface3] ip address 10.1.1.2 255.255.255.0
[Switch-Vlan-interface3] quit
```

开启 Switch 的 Telnet 服务器功能。

```
[Switch] telnet server enable
```

配置 Telnet 用户登录采用 AAA 认证方式。

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

配置进行用户角色切换时的认证方式为 **scheme local**。（首先使用 RADIUS 认证，若 AAA 配置无效或者 RADIUS 服务器没有响应则转为本地认证）

```
[Switch] super authentication-mode scheme local
```

创建 RADIUS 方案 radius。

```
[Switch] radius scheme radius
```

配置主认证服务器的 IP 地址为 10.1.1.1，与认证服务器交互报文时的共享密钥为 expert。

```
[Switch-radius-radius] primary authentication 10.1.1.1 key simple expert
```

配置向 RADIUS 服务器发送的用户名不携带域名。

```
[Switch-radius-radius] user-name-format without-domain
[Switch-radius-radius] quit
```

创建 ISP 域 bbb。

```

[Switch] domain bbb
# 配置 Telnet 用户登录认证方法为 radius。
[Switch-isp-bbb] authentication login radius-scheme radius
# 配置 Telnet 用户登录授权方法为 radius。
[Switch-isp-bbb] authorization login radius-scheme radius
# 配置 Telnet 用户登录计费方法为 none。
[Switch-isp-bbb] accounting login none
# 配置用户角色切换认证方法为 radius。
[Switch-isp-bbb] authentication super radius-scheme radius
[Switch-isp-bbb] quit
# 配置用户角色切换认证方式为本地认证时，切换到用户角色 network-admin 时使用的密码为
abcdef654321。
[Switch] super password role network-admin simple abcdef654321
[Switch] quit

```

(2) 配置 RADIUS server

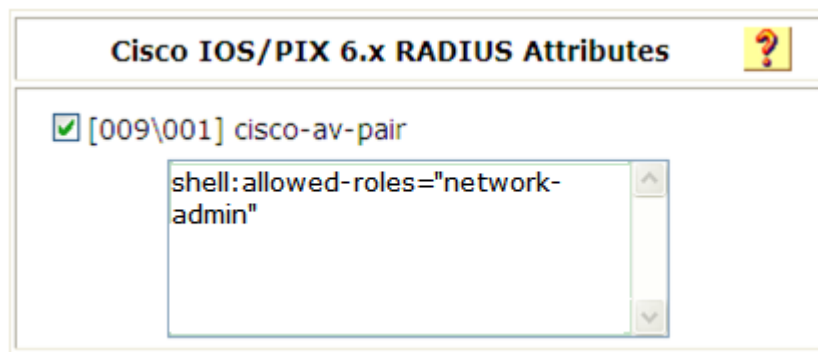


说明

下面以 ACSv4.2 为例，说明该例中 RADIUS server 的基本配置。

在 RADIUS server 上添加用户 \$enab0\$, 设置密码为 123456。并对该用户的 RADIUS 属性中的 cisco-av-pair 属性字符串进行设置。

图1-7 设置 Telnet 用户的 RADIUS 属性



5. 验证配置

(1) Telnet 用户建立与 Switch 的连接

在 Telnet 客户端按照提示输入用户名 test@bbb 及密码 aabbcc，即可成功登录 Switch，且只能访问指定权限的命令。

```

<Switch> telnet 192.168.1.70
Trying 192.168.1.70 ...
Press CTRL+K to abort
Connected to 192.168.1.70...
*****
* Copyright (c) 2004-2018 New H3C Technologies Co., Ltd. All rights reserved.*

```



```

* Without the owner's prior written consent,
* no decompiling or reverse-engineering shall be allowed.
*****

```

```

login: test@bbb
Password:
<Switch>?
User view commands:
    ping          Ping function
    quit          Exit from current command view
    ssh2          Establish a secure shell client connection
    super         Switch to a user role
    system-view   Enter the System View
    telnet        Establish a telnet connection
    tracert       Tracert function
<Switch>

```

(2) 切换用户角色

在当前的用户线下执行切换到用户角色 **network-admin** 的命令，按照提示输入 **RADIUS** 用户角色切换认证密码 **123456**，若认证成功即可将当前 **Telnet** 用户的角色切换到 **network-admin**。

```

<Switch> super network-admin
Username: test@bbb
Password: <——此处需输入 RADIUS 用户角色切换认证密码
User privilege role is network-admin, and only those commands that authorized to the
role can be used.

```

若 **ACS** 服务器无响应，按照提示输入本地用户角色切换认证密码 **abcdef654321**，若认证成功即可将当前 **Telnet** 用户的角色切换到 **network-admin**。

```

<Switch> super network-admin
Username: test@bbb
Password: <——此处需输入 RADIUS 用户角色切换认证密码
Invalid configuration or no response from the authentication server.
Change authentication mode to local.
Password: <——此处需输入本地用户角色切换认证密码
User privilege role is network-admin, and only those commands that authorized to the
role can be used.

```

1.12 RBAC常见故障处理

1.12.1 被授权的用户角色与本地用户实际拥有的权限不符

1. 故障现象

用户通过本地认证并被授权指定的用户角色后，发现登录设备后实际具有的权限与被授权的用户角色权限不符。

2. 故障分析

可能是该本地用户被授权了其它用户角色，例如该本地用户还具有缺省的用户角色。

3. 处理过程

通过 **display local-user** 命令查看该用户实际拥有的用户权限，并删除授予用户的多余用户角色。

1.12.2 使用远程认证服务器进行身份认证的用户登录设备失败

1. 故障现象

在 AAA 配置正确及设备与服务器通信无故障的情况下，使用 RADIUS 服务器进行远程身份认证的用户登录设备失败。

2. 故障分析

RBAC 要求登录设备的用户必须至少拥有一个用户角色，如果用户没有被服务器授权任何用户角色，则登录失败。

3. 处理过程

通过执行 **role default-role enable** 命令允许用户使用系统预定义的缺省用户角色登录设备，或根据需要在服务器上为该用户添加要授权的用户角色。

目 录

1 登录设备方式介绍.....	1-1
2 通过Console口首次登录设备.....	2-1
3 配置通过CLI登录设备.....	3-1
3.1 通过CLI登录设备简介.....	3-1
3.1.1 用户线简介.....	3-1
3.1.2 认证方式简介.....	3-1
3.1.3 用户角色简介.....	3-2
3.2 FIPS相关说明.....	3-2
3.3 CLI登录配置限制和指导.....	3-2
3.4 配置通过Console口登录设备.....	3-3
3.4.1 功能简介.....	3-3
3.4.2 配置限制和指导.....	3-3
3.4.3 通过Console口登录设备配置任务简介.....	3-3
3.4.4 配置通过Console口登录设备的认证方式.....	3-3
3.4.5 配置Console口登录方式的公共属性.....	3-5
3.5 配置通过Telnet登录设备.....	3-7
3.5.1 功能简介.....	3-7
3.5.2 配置限制和指导.....	3-7
3.5.3 配置设备作为Telnet服务器配置.....	3-8
3.5.4 配置设备作为Telnet客户端登录其他设备.....	3-11
3.6 配置通过SSH登录设备.....	3-12
3.6.1 功能简介.....	3-12
3.6.2 配置设备作为SSH服务器.....	3-12
3.6.3 配置设备作为SSH客户端登录其他设备.....	3-14
3.7 通过CLI登录显示和维护.....	3-15
4 配置通过Web登录设备.....	4-1
4.1 通过Web登录设备简介.....	4-1
4.2 FIPS相关说明.....	4-1
4.3 Web登录配置限制和指导.....	4-1
4.4 Web登录配置任务简介.....	4-1
4.5 Web登录配置准备.....	4-2
4.6 配置通过HTTP方式登录设备.....	4-2

4.7 配置通过HTTPS方式登录设备	4-2
4.8 配置用于Web登录的本地用户	4-4
4.9 管理Web登录用户连接	4-4
4.10 开启Web操作日志输出功能	4-5
4.11 通过Web登录设备显示和维护	4-5
4.12 通过Web登录设备典型配置举例	4-5
4.12.1 使用HTTP方式登录设备典型配置举例	4-5
4.12.2 使用HTTPS方式登录设备典型配置举例	4-6
5 配置通过SNMP登录设备	5-1
6 配置通过RESTful登录设备	6-1
6.1 通过RESTful登录设备简介	6-1
6.2 FIPS相关说明	6-1
6.3 配置通过基于HTTP的RESTful方式登录设备	6-1
6.4 配置通过基于HTTPS的RESTful方式登录设备	6-1
7 对登录用户的控制	7-1
7.1 登录用户控制简介	7-1
7.2 FIPS相关说明	7-1
7.3 配置对Telnet/SSH用户的控制	7-1
7.3.1 配置对Telnet用户的控制	7-1
7.3.2 配置对SSH用户的控制	7-1
7.3.3 对Telnet用户的控制典型配置举例	7-2
7.4 配置对Web用户的控制	7-3
7.4.1 配置通过源IP对Web用户进行控制	7-3
7.4.2 对Web用户的控制典型配置举例	7-3
7.5 配置对NMS的控制	7-4
7.5.1 功能简介	7-4
7.5.2 对NMS的控制典型配置举例	7-4
7.6 配置命令行授权功能	7-4
7.6.1 功能简介	7-4
7.6.2 配置限制和指导	7-5
7.6.3 配置步骤	7-5
7.6.4 命令行授权典型配置举例	7-6
7.7 配置命令行计费功能	7-7
7.7.1 功能简介	7-7
7.7.2 配置限制和指导	7-7
7.7.3 配置步骤	7-7

7.7.4 命令行计费典型配置举例	7-8
-------------------------	-----

1 登录设备方式介绍

设备支持以下登录方式：

- 通过 **CLI** 登录设备。登录成功后，可以直接输入命令行，来配置和管理设备。CLI 方式下又根据使用的登录接口以及登录协议不同，分为：通过 **Console** 口、**Telnet**、**SSH** 登录方式。
- 通过 **Web** 登录设备。登录成功后，用户可以使用 **Web** 界面直观地配置和管理网络设备。
- 通过 **SNMP** 登录设备。登录成功后，**NMS** 可以通过 **Set** 和 **Get** 等操作来配置和管理设备。
- 通过 **RESTful** 登录设备。登录成功后，用户可以使用 **RESTful API** 来配置和管理设备。

用户首次登录设备时，只能通过 **Console** 口登录。只有通过 **Console** 口登录到设备，进行相应的配置后，才能通过其他方式登录。



说明

- 此处设备登录方式设置均假设设备启动后不进入自动配置程序。
 - 设备运行于 **FIPS** 模式时，不支持 **Telnet** 登录、基于 **HTTP** 的 **Web** 登录以及基于 **HTTP** 的 **RESTful** 登录。有关 **FIPS** 模式的详细介绍请参见“安全配置指导”中的“**FIPS**”。
-

2 通过Console口首次登录设备

1. 功能简介

通过 Console 口进行本地登录是登录设备的最基本的方式,也是配置通过其他方式登录设备的基础。

2. 配置准备

在通过 Console 口搭建本地配置环境时,需要通过超级终端或 PuTTY 等终端仿真程序与设备建立连接。用户可以运行这些程序来连接网络设备、Telnet 或 SSH 站点。这些程序的详细介绍和使用方法请参见该程序的使用指导。

3. 配置步骤

通过 Console 口登录设备时,请按照以下步骤进行操作:

(1) 将 PC 断电。

因为 PC 机串口不支持热插拔,请不要在 PC 带电的情况下,将串口线插入或者拔出 PC 机。

(2) 请使用产品随机附带的配置口电缆连接 PC 机和设备。请先将配置口电缆的 DB-9 (孔) 插头插入 PC 机的 9 芯 (针) 串口中,再将 RJ-45 插头端插入设备的 Console 口中。



提示

- 连接时请认准接口上的标识,以免误插入其他接口。
- 在拆下配置口电缆时,请先拔出 RJ-45 端,再拔下 DB-9 端。

图2-1 将设备与 PC 通过配置口电缆进行连接



(3) 给 PC 上电。

(4) 打开终端仿真程序,按如下要求设置终端参数:

- 波特率: 9600
- 数据位: 8
- 停止位: 1
- 奇偶校验: 无
- 流量控制: 无

(5) 设备上电。

在设备自检结束后,用户可通过键入回车进入命令交互界面。出现命令行提示符后即可键入命令来配置设备或查看设备运行状态,需要帮助可以随时键入?。

3 配置通过CLI登录设备

3.1 通过CLI登录设备简介

CLI 登录用户的访问行为需要由用户线管理、限制，即网络管理员可以给每个用户线配置一系列参数，比如用户登录时是否需要认证、用户登录后的角色等。当用户通过 CLI 登录到设备的时候，系统会给用户分配一个用户线，登录用户将受到该用户线下配置参数的约束。

3.1.1 用户线简介

1. 用户线类型

设备提供如下类型的用户线：

- **AUX 用户线**：用来管理和监控通过 **Console** 口登录的用户。
- **VTY (Virtual Type Terminal, 虚拟类型终端) 用户线**：用来管理和监控通过 **Telnet** 或 **SSH** 登录的用户。

2. 用户线编号

用户线的编号有绝对编号方式和相对编号方式。

- **绝对编号方式**
使用绝对编号方式，可以唯一的指定一个用户线。绝对编号从0开始自动编号，每次增长1，先给所有 **AUX** 用户线，然后是 **VTY** 用户线。使用 **display line**（不带参数）可查看到设备当前支持的用户线以及它们的绝对编号。
- **相对编号方式**
相对编号是每种类型用户线的内部编号，表现形式为“用户线类型 编号”。用户线的编号从0开始以1为单位递增。

3. 用户线分配

用户登录时，系统会根据用户的登录方式，自动给用户分配一个当前空闲的、编号最小的某类型的用户线，整个登录过程将受该用户线视图下配置的约束。用户与用户线并没有固定的对应关系：

- 同一用户登录的方式不同，分配的用户线不同。比如用户 **A** 使用 **Console** 口登录设备时，将受到 **AUX** 用户线视图下配置的约束；当使用 **Telnet** 登录设备时，将受到 **VTY** 用户线视图下配置的约束。
- 同一用户登录的时间不同，分配的用户线可能不同。比如用户本次使用 **Telnet** 登录设备，设备为其分配的用户线是 **VTY 1**。当该用户下次再 **Telnet** 登录时，设备可能已经把 **VTY 1** 分配给其他 **Telnet** 用户了，只能为该用户分配其他的用户线。

如果没有空闲的、相应类型的用户线可分配，则用户不能登录设备。

3.1.2 认证方式简介

在用户线下配置认证方式，可以要求当用户使用指定用户线登录时是否需要认证，以提高设备的安全性。设备支持配置如下认证方式：

- 认证方式为 **none**：表示下次使用该用户线登录时不需要进行用户名和密码认证，任何人都可以登录到设备上，这种情况可能会带来安全隐患。**FIPS** 模式下不支持该认证方式。
 - 认证方式为 **password**：表示下次使用该用户线登录时，需要输入密码。只有密码正确，用户才能登录到设备上。配置认证方式为 **password** 后，请妥善保管密码。**FIPS** 模式下不支持该认证方式。
 - 认证方式为 **scheme**：表示下次使用该用户线登录设备时需要进行用户名和密码认证，用户名或密码错误，均会导致登录失败。配置认证方式为 **scheme** 后，请妥善保管用户名及密码。
- 认证方式不同，配置不同，具体配置如 [表 3-1](#) 所示。

表3-1 不同认证方式下配置任务简介

认证方式	认证所需配置
none	设置登录用户的认证方式为不认证
password	设置登录用户的认证方式为password认证 设置密码认证的密码
scheme	设置登录用户的认证方式为scheme认证 在ISP域视图下为login用户配置认证方法

3.1.3 用户角色简介

用户角色中定义了允许用户配置的系统功能以及资源对象，即用户登录后执行的命令。关于用户角色的详细描述以及配置请参见“基础配置指导”中的“RBAC”。

- 对于 **none** 和 **password** 认证方式，登录用户的角色由用户线下的用户角色配置决定。
- 对于 **scheme** 认证方式，且用户通过 **SSH** 的 **publickey** 或 **password-publickey** 方式登录设备时，登录用户将被授予同名的设备管理类本地用户视图下配置的授权用户角色。
- 对于 **scheme** 认证方式，非 **SSH** 登录以及用户通过 **SSH** 的 **password** 方式登录设备时，登录用户使用 **AAA** 认证用户的角色配置。尤其对于远程 **AAA** 认证用户，如果 **AAA** 服务器没有下发用户角色且缺省用户角色授权功能处于关闭状态时，用户将不能登录设备。

3.2 FIPS相关说明

- 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**”。
- 设备运行于 **FIPS** 模式时，不支持用户通过 **Telnet** 登录设备。

3.3 CLI登录配置限制和指导

通过 **CLI** 登录设备时，有以下限制和指导：

- 用户线视图下的配置优先于用户线类视图下的配置。
- 当用户线或用户线类视图下的属性配置为缺省值时，将优先采用配置为非缺省值的视图下的配置。
- 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。

3.4 配置通过Console口登录设备

3.4.1 功能简介

通过Console口进行本地登录是登录设备的基本方式之一，用户可以使用本地链路登录设备，便于系统维护。如 [图 3-1](#) 所示。具体登录步骤，请参见 [通过Console口首次登录设备](#)。

图3-1 通过 Console 口登录设备示意图



缺省情况下，通过 Console 口登录时认证方式为 `none`，可直接登录。登录成功之后用户角色为 `network-admin`。

首次登录后，建议修改认证方式以及其他参数来增强设备的安全性。

3.4.2 配置限制和指导

改变 Console 口登录的认证方式后，新认证方式对新登录的用户生效。

FIPS 模式下，不支持无需认证、密码认证，仅支持 AAA 认证（`scheme`）。

3.4.3 通过Console口登录设备配置任务简介

通过 Console 口登录设备配置任务如下：

- (1) [配置通过Console口登录设备的认证方式](#)
 - [配置通过Console口登录设备时无需认证（`none`）](#)
 - [配置通过Console口登录设备时采用密码认证（`password`）](#)
 - [配置通过Console口登录设备时采用AAA认证（`scheme`）](#)
- (2) （可选）[配置Console口登录方式的公共属性](#)

3.4.4 配置通过Console口登录设备的认证方式

1. 配置通过Console口登录设备时无需认证（`none`）

- (1) 进入系统视图。
system-view
- (2) 进入 AUX 用户线或 AUX 用户线类视图。
 - 进入 AUX 用户线视图。
line aux first-number [last-number]
 - 进入 AUX 用户线类视图。
line class aux
- (3) 设置登录用户的认证方式为不认证。

authentication-mode none

缺省情况下，用户通过 Console 口登录，认证方式如下：

- 对于 S5000V3-EI 系列交换机和 S5000E-X 系列交换机：
 - 设备采用出厂配置启动时，用户通过 Console 口登录，认证方式为 **scheme**。
 - 设备采用空配置启动时，用户通过 Console 口登录，认证方式为 **none**。
- 对于其它系列交换机，用户通过 Console 口登录，认证方式为 **none**。

关于空配置启动和缺省配置启动的详细介绍，请参见“基础配置指导”中的“配置文件管理”。

- (4) 配置从当前用户线登录设备的用户角色。

user-role *role-name*

缺省情况下，通过 Console 口登录设备的用户角色为 **network-admin**。

2. 配置通过Console口登录设备时采用密码认证（password）

- (1) 进入系统视图。

system-view

- (2) 进入 AUX 用户线或 AUX 用户线类视图。

- 进入 AUX 用户线视图。

line aux *first-number* [*last-number*]

- 进入 AUX 用户线类视图。

line class aux

- (3) 设置登录用户的认证方式为密码认证。

authentication-mode password

缺省情况下，用户通过 Console 口登录，认证方式如下：

- 对于 S5000V3-EI 系列交换机和 S5000E-X 系列交换机：
 - 设备采用出厂配置启动时，用户通过 Console 口登录，认证方式为 **scheme**。
 - 设备采用空配置启动时，用户通过 Console 口登录，认证方式为 **none**。
- 对于其它系列交换机，用户通过 Console 口登录，认证方式为 **none**。

关于空配置启动和缺省配置启动的详细介绍，请参见“基础配置指导”中的“配置文件管理”。

- (4) 设置认证密码。

set authentication password { **hash** | **simple** } *password*

缺省情况下，未设置认证密码。

- (5) 配置从当前用户线登录设备的用户角色。

user-role *role-name*

缺省情况下，通过 Console 口登录设备的用户角色为 **network-admin**。

3. 配置通过Console口登录设备时采用AAA认证（scheme）

- (1) 进入系统视图。

system-view

- (2) 进入 AUX 用户线或 AUX 用户线类视图。

- 进入 AUX 用户线视图。

```
line aux first-number [ last-number ]
```

- 进入 AUX 用户线类视图。

```
line class aux
```

(3) 设置登录用户的认证方式为通过 AAA 认证。

（非 FIPS 模式）

```
authentication-mode scheme
```

缺省情况下，用户通过 Console 口登录，认证方式如下：

- 对于 S5000V3-EI 系列交换机和 S5000E-X 系列交换机：
 - 设备采用出厂配置启动时，用户通过 Console 口登录，认证方式为 **scheme**。
 - 设备采用空配置启动时，用户通过 Console 口登录，认证方式为 **none**。
- 对于其它系列交换机，用户通过 Console 口登录，认证方式为 **none**。

关于空配置启动和缺省配置启动的详细介绍，请参见“基础配置指导”中的“配置文件管理”。

（FIPS 模式）

```
authentication-mode scheme
```

缺省情况下，用户登录设备的认证方式为 **scheme**。

(4) 在 ISP 域视图下为 login 用户配置认证方法。

如果选择本地认证，请配置本地用户及相关属性；如果选择远程认证，请配置 RADIUS、HWTACACS 或 LDAP 方案。相关配置的详细介绍请参见“安全配置指导”中的“AAA”。

3.4.5 配置Console口登录方式的公共属性

1. 配置限制和指导

改变 Console 口属性后会立即生效，所以通过 Console 口登录来配置 Console 口属性可能在配置过程中发生连接中断，建议通过其他登录方式来配置 Console 口属性。

若用户需要通过 Console 口再次登录设备，需要改变 PC 机上运行的终端仿真程序的相应配置，使之与设备上配置的 Console 口属性保持一致。否则，连接失败。

2. 配置步骤

(1) 进入系统视图。

```
system-view
```

(2) 进入 AUX 用户线或 AUX 用户线类视图。

- 进入 AUX 用户线视图。

```
line aux first-number [ last-number ]
```

- 进入 AUX 用户线类视图。

```
line class aux
```

(3) 配置设备与访问终端之间的通信参数。

- 配置设备与访问终端之间的传输速率。

```
speed speed-value
```

缺省情况下，用户线的传输速率为 9600bit/s。

用户线类视图下不支持该命令。

- 配置校验方式。

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

缺省情况下，设备校验位的校验方式为 **none**，即不进行校验。

用户线类视图下不支持该命令。

- 配置流量控制方式。

flow-control { **none** | **software** }

缺省情况下，没有配置流量控制方式。

用户线类视图下不支持该命令。

- 配置数据位。

databits { **7** | **8** }

缺省情况下，用户线的数据位为 8 位。

用户线类视图下不支持该命令。

类型	支持的数据位
传送字符的编码类型为标准ASCII码	7
传送字符的编码类型为扩展ASCII码	8

- 配置停止位。

stopbits { **1** | **1.5** | **2** }

缺省情况下，用户线的停止位为 1 比特。

停止位用来表示单个包的结束。停止位的位数越多，传输效率越低。用户线类视图下不支持该命令。

(4) 配置用户线的终端属性。

- 在用户线上启动终端服务。

shell

缺省情况下，所有用户线的终端服务功能处于开启状态。

AUX 用户线视图下不允许关闭 **shell** 终端服务。

- 配置终端的显示类型。

terminal type { **ansi** | **vt100** }

缺省情况下，终端显示类型为 ANSI。

建议设备的终端类型与客户端的终端类型都配置为 VT100，或者均配置为 ANSI 的同时保证当前编辑的命令行的总字符数不超过 80。否则客户端的终端屏幕不能正常显示。

- 配置终端屏幕一屏显示的行数。

screen-length *screen-length*

缺省情况下，终端屏幕一屏显示的行数为 24 行。

screen-length 0 表示关闭分屏显示功能。

- 设置历史命令缓冲区大小。

history-command max-size *value*

缺省情况下，每个用户的历史缓冲区的大小为 10，即可存放 10 条历史命令。

- 设置用户线的空闲超时时间。

idle-timeout *minutes* [*seconds*]

缺省情况下，所有的用户线的超时时间为 10 分钟，如果直到超时时间到达，某用户线一直没有用户进行操作，则该用户线将自动断开。

超时时间为 0 表示永远不会超时。

- (5) 设置终端线路的自动执行的命令。

auto-execute command *command*

缺省情况下，终端线路未设置自动执行命令。

用户登录到终端线路后，设备会自动依次执行 *command*，然后退出当前连接。

AUX 用户线/AUX 用户线类视图下不支持该命令。

- (6) 配置快捷键。

- 配置启动终端会话的快捷键。

activation-key *character*

缺省情况下，按<Enter>键启动终端会话。

- 配置中止当前运行任务的快捷键。

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

缺省情况下，键入<Ctrl+C>中止当前运行的任务。

- 配置对当前用户线进行锁定并重新认证的快捷键。

lock-key *key-string*

缺省情况下，不存在对当前用户线进行锁定并重新认证的快捷键。

3.5 配置通过Telnet登录设备

3.5.1 功能简介

设备可以作为Telnet服务器，以使用户能够Telnet登录到设备进行远程管理和监控。具体配置请参见“[3.5.3 配置设备作为Telnet服务器配置](#)”。

设备也可以作为Telnet客户端，Telnet到其他设备，对别的设备进行管理和监控。具体配置请参见“[3.5.4 配置设备作为Telnet客户端登录其他设备](#)”。

3.5.2 配置限制和指导

设备运行于 FIPS 模式时，不支持 Telnet 登录。有关 FIPS 模式的详细介绍请参见“安全配置指导”中的“FIPS”。

改变 Telnet 登录的认证方式后，新认证方式对新登录的用户生效。

3.5.3 配置设备作为Telnet服务器配置

1. 通过Telnet登录设备配置任务简介

设备作为 Telnet 服务器配置任务如下：

- (1) [开启Telnet服务](#)
- (2) 配置设备作为 Telnet 服务器时的认证方式
 - [配置Telnet登录设备时无需认证（none）](#)
 - [配置Telnet登录设备时采用密码认证（password）](#)
 - [配置Telnet登录设备时采用AAA认证（scheme）](#)
- (3) （可选）[配置Telnet服务器发送报文的公共属性](#)
- (4) （可选）[配置VTY用户线的公共属性](#)

2. 开启Telnet服务

- (1) 进入系统视图。
system-view
- (2) 开启设备的 Telnet 服务。
telnet server enable
缺省情况下，Telnet 服务处于关闭状态。

3. 配置Telnet登录设备时无需认证（none）

- (1) 进入系统视图。
system-view
- (2) 进入 VTY 用户线或 VTY 用户线类视图。
 - 进入 VTY 用户线视图。
line vty *first-number* [*last-number*]
 - 进入 VTY 用户线类视图。
line class vty
- (3) 设置登录用户的认证方式为不认证。
authentication-mode none
缺省情况下，Telnet 用户的认证方式为 **password**。
用户线视图下，**authentication-mode** 和 **protocol inbound** 存在关联绑定关系，当两条命令中的任意一条配置了非缺省值，那么另外一条取用户线下的值。
- (4) 配置从当前用户线登录设备的用户角色。
user-role *role-name*
缺省情况下，通过 Telnet 登录设备的用户角色为 **network-operator**。

4. 配置Telnet登录设备时采用密码认证（password）

- (1) 进入系统视图。
system-view
- (2) 进入 VTY 用户线或 VTY 用户线类视图。
 - 进入 VTY 用户线视图。

```
line vty first-number [ last-number ]
```

- 进入 VTY 用户线类视图。

```
line class vty
```

- (3) 设置登录用户的认证方式为密码认证。

```
authentication-mode password
```

缺省情况下，Telnet 用户的认证方式为 **password**。

用户线视图下，**authentication-mode** 和 **protocol inbound** 存在关联绑定关系，当两条命令中的任意一条配置了非缺省值，那么另外一条取用户线下的值。

- (4) 设置密码认证的密码。

```
set authentication password { hash | simple } password
```

缺省情况下，未设置密码认证的密码。

- (5) （可选）配置从当前用户线登录设备的用户角色。

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

缺省情况下，通过 Telnet 登录设备的用户角色为 **network-operator**。

5. 配置Telnet登录设备时采用AAA认证（scheme）

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 VTY 用户线或 VTY 用户线类视图。

- 进入 VTY 用户线视图。

```
line vty first-number [ last-number ]
```

- 进入 VTY 用户线类视图。

```
line class vty
```

- (3) 设置登录用户的认证方式为通过 AAA 认证。

```
authentication-mode scheme
```

缺省情况下，Telnet 用户的认证方式为 **password**。

用户线视图下，**authentication-mode** 和 **protocol inbound** 存在关联绑定关系，当两条命令中的任意一条配置了非缺省值，那么另外一条取用户线下的值。

- (4) 在 ISP 域视图下为 login 用户配置认证方法。

如果选择本地认证，请配置本地用户及相关属性；如果选择远程认证，请配置 RADIUS、HWTACACS 或 LDAP 方案。相关配置的详细介绍请参见“安全配置指导”中的“AAA”。

6. 配置Telnet服务器发送报文的公共属性

- (1) 进入系统视图。

```
system-view
```

- (2) 配置 Telnet 服务器发送报文的 DSCP 优先级。

（IPv4 网络）

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

（IPv6 网络）

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


缺省情况下，Telnet 服务器发送 Telnet 报文的 DSCP 优先级为 48。

- (3) 配置 Telnet 协议的端口号。

(IPv4 网络)

```
telnet server port port-number
```

(IPv6 网络)

```
telnet server ipv6 port port-number
```

缺省情况下，Telnet 协议的端口号为 23。

- (4) 配置 Telnet 登录同时在线的最大用户连接数。

```
aaa session-limit telnet max-sessions
```

缺省情况下，Telnet 方式登录同时在线的最大用户连接数为 32。

配置本命令后，已经在线的用户连接不会受到影响，只对新的用户连接生效。如果当前在线的用户连接数已经达到最大值，则新的连接请求会被拒绝，登录会失败。

关于该命令的详细描述，请参见“安全命令参考”中的“AAA”。

7. 配置VTY用户线的公共属性

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 VTY 用户线或 VTY 用户线类视图。

- 进入 VTY 用户线视图。

```
line vty first-number [ last-number ]
```

- 进入 VTY 用户线类视图。

```
line class vty
```

- (3) 设置 VTY 终端属性。

- 设置在终端线路上启动终端服务。

```
shell
```

缺省情况下，所有用户线的终端服务功能处于开启状态。

- 配置终端的显示类型。

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

缺省情况下，终端显示类型为 ANSI。

- 设置终端屏幕一屏显示的行数。

```
screen-length screen-length
```

缺省情况下，终端屏幕一屏显示的行数为 24 行。

取值为 0 表示关闭分屏显示功能。

- 设置设备历史命令缓冲区大小。

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

缺省情况下，每个用户的历史缓冲区大小为 10，即可存放 10 条历史命令。

- 设置 VTY 用户线的空闲超时时间。

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

缺省情况下，所有的用户线的超时时间为 10 分钟。如果 10 分钟内某用户线没有用户进行操作，则该用户线将自动断开。

取值为 0 表示永远不会超时。

(4) 配置 VTY 用户线支持的协议。

```
protocol inbound { all | ssh | telnet }
```

缺省情况下，设备同时支持 Telnet 和 SSH 协议。

该配置将在用户下次使用该用户线登录时生效。

用户线视图下，**authentication-mode** 和 **protocol inbound** 存在关联绑定关系，当两条命令中的任意一条配置了非缺省值，那么另外一条取用户线下的值。

(5) 设置从用户线登录后自动执行的命令。

```
auto-execute command command
```

缺省情况下，未配置自动执行命令。



注意

在配置 **auto-execute command** 命令并退出登录之前，要确保可以通过其他 VTY、AUX 用户登录并更改配置，以便出现问题后，能删除该配置。

配置自动执行命令后，用户在登录时，系统会自动执行已经配置好的命令，执行完命令后，自动断开用户连接。如果这条命令引发了一个任务，系统会等这个任务执行完毕后再断开连接。

(6) 配置快捷键。

- 配置中止当前运行任务的快捷键。

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

缺省情况下，键入 <Ctrl+C> 中止当前运行的任务。

- 配置对当前用户线进行锁定并重新认证的快捷键。

```
lock-key key-string
```

缺省情况下，不存在对当前用户线进行锁定并重新认证的快捷键。

3.5.4 配置设备作为Telnet客户端登录其他设备

1. 功能简介

用户已经成功登录到了设备上，并希望将当前设备作为Telnet客户端登录到Telnet服务器上进行操作，如 [图 3-2](#) 所示。

图3-2 通过设备登录到其他设备



2. 配置准备

先配置设备 IP 地址并获取 Telnet 服务器的 IP 地址。如果设备与 Telnet 服务器相连的端口不在同一子网内，请保证两台设备间路由可达。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) （可选）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。

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

缺省情况下，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。

- (3) 退回用户视图。

```
quit
```

- (4) 设备作为 Telnet 客户端登录到 Telnet 服务器。

（IPv4 网络）

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

（IPv6 网络）

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

3.6 配置通过SSH登录设备

3.6.1 功能简介

用户通过一个不能保证安全的网络环境远程登录到设备时，SSH（Secure Shell，安全外壳）可以利用加密和强大的认证功能提供安全保障，保护设备不受诸如 IP 地址欺诈、明文密码截取等攻击。

- 设备可以作为SSH服务器，以使用户能够使用SSH协议登录到设备进行远程管理和监控。具体配置请参见“[3.6.2 配置设备作为SSH服务器](#)”。
- 设备也可以作为SSH客户端，使用SSH协议登录到别的设备，对别的设备进行管理和监控。具体配置请参见“[3.6.3 配置设备作为SSH客户端登录其他设备](#)”。

3.6.2 配置设备作为SSH服务器

以下配置步骤只介绍采用 **password** 方式认证 SSH 客户端的配置方法，**publickey** 方式的配置方法及 SSH 的详细介绍，请参见“安全配置指导”中的“SSH”。

- (1) 进入系统视图。

```
system-view
```

- (2) 生成本地密钥对。

（非 FIPS 模式）

```
public-key local create { dsa | ecdsa [ secp192r1 | secp256r1 | secp384r1  
| secp521r1 ] | rsa } [ name key-name ]
```

（FIPS 模式）

```
public-key local create { dsa | ecdsa [ secp256r1 | secp384r1 | secp521r1 ]  
| rsa } [ name key-name ]
```

- (3) 开启 SSH 服务器功能。

```
ssh server enable
```

缺省情况下，SSH 服务器功能处于关闭状态。

- (4) （可选）建立 SSH 用户，并指定 SSH 用户的认证方式。

```
ssh user username service-type stelnet authentication-type password
```

- (5) 进入 VTY 用户线或 VTY 用户线类视图。

- 进入 VTY 用户线视图。

```
line vty first-number [ last-number ]
```

- 进入 VTY 用户线类视图。

```
line class vty
```

- (6) 配 VTY 用户线的认证方式为 scheme 方式。

（非 FIPS 模式）

```
authentication-mode scheme
```

缺省情况下，VTY 用户线的认证方式为 password 方式。

用户线视图下，**authentication-mode** 和 **protocol inbound** 存在关联绑定关系，当两条命令中的任意一条配置了非缺省值，那么另外一条取用户线下的值。

（FIPS 模式）

```
authentication-mode scheme
```

缺省情况下，VTY 用户线的认证方式为 scheme 方式。

用户线视图下，**authentication-mode** 和 **protocol inbound** 存在关联绑定关系，当两条命令中的任意一条配置了非缺省值，那么另外一条取用户线下的值。

- (7) （可选）配置 VTY 用户线支持的 SSH 协议。

（非 FIPS 模式）

```
protocol inbound { all | ssh | telnet }
```

缺省情况下，设备同时支持 Telnet 和 SSH 协议。

本配置将在用户下次使用该用户线登录时生效。

用户线视图下，**authentication-mode** 和 **protocol inbound** 存在关联绑定关系，当两条命令中的任意一条配置了非缺省值，那么另外一条取用户线下的值。

（FIPS 模式）

```
protocol inbound ssh
```

缺省情况下，设备支持 SSH 协议。

本配置将在用户下次使用该用户线登录时生效。

用户线视图下，**authentication-mode** 和 **protocol inbound** 存在关联绑定关系，当两条命令中的任意一条配置了非缺省值，那么另外一条取用户线下的值。

- (8) (可选) 配置 SSH 方式登录设备时，同时在线的最大用户连接数。

```
aaa session-limit ssh max-sessions
```

缺省情况下，SSH 方式登录同时在线的最大用户连接数为 32。

配置本命令后，已经在线的用户连接不会受到影响，只对新的用户连接生效。如果当前在线的用户连接数已经达到最大值，则新的连接请求会被拒绝，登录会失败。

关于该命令的详细描述，请参见“安全命令参考”中的“AAA”。

- (9) (可选) 退回系统视图并配置 VTY 用户线的公共属性。

- a. 退回系统视图。

```
quit
```

- b. 配置 VTY 用户线的公共属性。

详细配置请参见“[3.5.3 7. 配置VTY用户线的公共属性](#)”。

3.6.3 配置设备作为SSH客户端登录其他设备

1. 功能简介

用户已经成功登录到了设备上，并希望将当前设备作为SSH客户端登录到其他设备上进行操作，如图 3-3 所示。

图3-3 通过设备登录到其他设备



2. 配置准备

先配置设备 IP 地址并获取 SSH 服务器的 IP 地址。如果设备与 SSH 服务器相连的端口不在同一子网内，请配置路由使得两台设备间路由可达。

3. 配置步骤

请在用户视图下执行本命令，配置设备作为 SSH 客户端登录到 SSH 服务器。

(IPv4 网络)

```
ssh2 server
```

(IPv6 网络)

```
ssh2 ipv6 server
```



说明

为配合 SSH 服务器，设备作为 SSH 客户端时还可进一步进行其他配置，具体配置请参见“安全配置指导”中的“SSH”。

3.7 通过CLI登录显示和维护

表3-2 CLI 显示和维护

操作	命令	说明
显示用户线的相关信息	display line [<i>num1</i> { aux vty } <i>num2</i>] [summary]	在任意视图下执行
显示设备作为Telnet客户端的相关配置信息	display telnet client	在任意视图下执行
显示当前正在使用的用户线以及用户的相关信息	display users	在任意视图下执行
显示设备支持的所有用户线以及用户的相关信息	display users all	在任意视图下执行
释放指定的用户线	free line { <i>num1</i> { aux vty } <i>num2</i> }	在用户视图下执行 系统支持多个用户同时对设备进行配置，当管理员在维护设备时，其他在线用户的配置影响到管理员的操作，或者管理员正在进行一些重要配置不想被其他用户干扰时，可以使用以下命令强制断开该用户的连接 不能使用该命令释放用户当前自己使用的连接
锁定当前用户线并设置解锁密码，防止未授权的用户操作该线	lock	在用户视图下执行 缺省情况下，系统不会自动锁定当前用户线 FIPS模式下，不支持此命令
锁定当前用户线并对其进行重新认证	lock reauthentication	在任意视图下执行 缺省情况下，系统不会自动锁定当前用户线并对其进行重新认证 请使用设备登录密码解除锁定并重新登录设备
向指定的用户线发送消息	send { all <i>num1</i> { aux vty } <i>num2</i> }	在用户视图下执行

4 配置通过Web登录设备

4.1 通过Web登录设备简介

为了方便用户对网络设备进行配置和维护，设备提供 Web 功能。用户可以通过 PC 登录到设备上，使用 Web 界面直观地配置和维护设备。

设备支持两种 Web 登录方式：

- HTTP 登录方式：HTTP（Hypertext Transfer Protocol，超文本传输协议）用来在 Internet 上传递 Web 页面信息。HTTP 位于 TCP/IP 协议栈的应用层，传输层采用面向连接的 TCP。设备同时支持 HTTP 协议 1.0 和 1.1 版本。
- HTTPS 登录方式：HTTPS（Hypertext Transfer Protocol Secure，超文本传输协议的安全版本）是支持 SSL（Secure Sockets Layer，安全套接字层）协议的 HTTP 协议。HTTPS 通过 SSL 协议，能对客户端与设备之间交互的数据进行加密，能为设备制定基于证书属性的访问控制策略，提高了数据传输的安全性和完整性，保证合法客户端可以安全地访问设备，禁止非法的客户端访问设备，从而实现了设备的安全管理。

4.2 FIPS相关说明

- 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”。
- 设备运行于 FIPS 模式时，不支持用户通过 HTTP 方式的 Web 登录。

4.3 Web登录配置限制和指导

如果设备只开启了 HTTP 服务，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。

4.4 Web登录配置任务简介

Web 登录配置任务如下：

- (1) 配置通过 Web 登录设备
请选择其中一项进行配置：
 - [配置通过HTTP方式登录设备](#)
 - [配置通过HTTPS方式登录设备](#)
- (2) [配置用于Web登录的本地用户](#)
- (3) [管理Web登录用户连接](#)
- (4) [开启Web操作日志输出功能](#)

4.5 Web登录配置准备

在通过 Web 登录设备前，需要配置设备的 IP 地址，确保设备与 Web 登录用户间路由可达。

4.6 配置通过HTTP方式登录设备

- (1) （可选）请在用户视图下执行本命令，配置用户访问 Web 的固定校验码。

```
web captcha verification-code
```

缺省情况下，用户只能使用 Web 页面显示的校验码访问 Web。

- (2) 进入系统视图。

```
system-view
```

- (3) 开启 HTTP 服务。

```
ip http enable
```

对于 S5000V3-EI 系列交换机和 S5000E-X 系列交换机：

- 设备采用出厂配置启动时，HTTP 服务处于开启状态。
- 设备采用空配置启动时，HTTP 服务处于关闭状态。

对于其他系列交换机，缺省情况下，HTTP 服务器处于关闭状态。

关于空配置启动和缺省配置启动的详细介绍，请参见“基础配置指导”中的“配置文件管理”。

- (4) （可选）配置 HTTP 服务的端口号。

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

缺省情况下，HTTP 服务的端口号为 80。

4.7 配置通过HTTPS方式登录设备

1. 功能简介

HTTPS 登录方式分为以下两种：

- 简便登录方式：采用这种方式时，设备上只需开启 HTTPS 服务，用户即可通过 HTTPS 登录设备。此时，设备使用的证书为自签名证书，使用的 SSL 参数为各个参数的缺省值。这种方式简化了配置，但是存在安全隐患。（自签名证书指的是服务器自己生成的证书，无需从 CA 获取）
- 安全登录方式：采用这种方式时，设备上不仅要开启 HTTPS 服务，还需要配置 SSL 服务器端策略、PKI 域等。这种方式配置复杂，但是具有更高的安全性。

SSL 的相关描述和配置请参见“安全配置指导”中的“SSL”。PKI 的相关描述和配置请参见“安全配置指导”中的“PKI”。

2. 配置限制和指导

- 更改 HTTPS 服务与 SSL 服务器端的关联策略，需要先关闭 HTTP 和 HTTPS 服务，再重新配置 HTTPS 服务与 SSL 服务器端策略关联，最后重新开启 HTTP 服务和 HTTPS 服务，新的策略即可生效。

- 如需恢复 HTTPS 使用自签名证书的情况，必须先关闭 HTTP 和 HTTPS 服务，再执行 **undo ip https ssl-server-policy**，最后重新开启 HTTP 服务和 HTTPS 服务即可。
- 开启 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。此时，需要多次执行 **ip https enable** 命令，HTTPS 服务才能正常启动。
- 如果配置 HTTPS 服务与证书属性访问控制策略关联，则必须同时在与 HTTPS 服务关联的 SSL 服务器端策略中配置 **client-verify enable** 命令，且证书属性访问控制策略中必须至少包括一条 **permit** 规则，否则任何 HTTPS 客户端都无法登录设备。

3. 配置通过HTTPS方式登录设备

- (1) （可选）请在用户视图下执行本命令，配置用户访问 Web 的固定校验码。

```
web captcha verification-code
```

缺省情况下，用户只能使用 Web 页面显示的校验码访问 Web。

- (2) 进入系统视图。

```
system-view
```

- (3) （可选）配置 HTTPS 服务与其他策略的关联。

- 配置 HTTPS 服务与 SSL 服务器端策略关联。

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

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

- 配置 HTTPS 服务与证书属性访问控制策略关联。

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

缺省情况下，HTTPS 服务未与证书属性访问控制策略关联。

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。证书属性访问控制策略的详细介绍请参见“安全配置指导”中的“PKI”。

- (4) 开启 HTTPS 服务。

```
ip https enable
```

对于 S5000V3-EI 系列交换机和 S5000E-X 系列交换机：

- 设备采用出厂配置启动时，HTTPS 服务处于开启状态。
- 设备采用空配置启动时，HTTPS 服务处于关闭状态。

对于其他系列交换机，缺省情况下，HTTPS 服务处于关闭状态。

关于空配置启动和缺省配置启动的详细介绍，请参见“基础配置指导”中的“配置文件管理”。

- (5) （可选）配置 HTTPS 服务的端口。

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

缺省情况下，HTTPS 服务的端口号为 443。

- (6) （可选）配置使用 HTTPS 登录设备时的认证方式。

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

缺省情况下，用户使用 HTTPS 登录设备时采用的认证模式为 **manual**。

4.8 配置用于Web登录的本地用户

- (1) 进入系统视图。

system-view

- (2) 创建本地用户用于 Web 登录，并进入本地用户视图。

local-user *user-name* [**class** *manage*]

- (3) （可选）设置本地用户的密码。

（非 FIPS 模式）

password [{ **hash** | **simple** } *password*]

缺省情况下，不存在本地用户密码，即本地用户认证时无需输入密码，只要用户名有效且其他属性验证通过即可认证成功。

（FIPS 模式）

password

缺省情况下，不存在本地用户密码，但本地用户认证时不能成功。

- (4) 配置 Web 登录用户的属性。

- 配置 Web 登录的用户角色。

authorization-attribute **user-role** *user-role*

缺省情况下，Web 登录的用户角色为 *network-operator*。

- 配置 Web 登录用户的服务类型。

service-type { **http** | **https** }

缺省情况下，未配置用户的服务类型。

4.9 管理Web登录用户连接

1. 配置Web登录用户连接的超时时间

- (1) 进入系统视图。

system-view

- (2) 配置 Web 登录用户连接的超时时间。

web idle-timeout *minutes*

缺省情况下，Web 闲置超时时间为 10 分钟。

2. 配置同时在线的最大Web用户连接数

- (1) 进入系统视图。

system-view

- (2) 配置同时在线的最大 Web 用户连接数。

aaa session-limit { **http** | **https** } *max-sessions*

缺省的同时在线的最大 Web 用户连接数为 32。

配置本命令后，已经在线的用户连接不会受到影响，只对新的用户连接生效。如果当前在线的用户连接数已经达到最大值，则新的连接请求会被拒绝，登录会失败。关于该命令的详细描述，请参见“安全命令参考”中的“AAA”。

3. 强制在线Web用户下线

请在用户视图下执行本命令，强制在线 Web 用户下线。

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

4.10 开启Web操作日志输出功能

(1) 进入系统视图。

```
system-view
```

(2) 开启 Web 操作日志输出功能。

```
webui log enable
```

缺省情况下，Web 操作日志输出功能处于关闭状态。

4.11 通过Web登录设备显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示 Web 用户的信息、HTTP 的状态信息和 HTTPS 的状态信息，通过查看显示信息验证配置的效果。

表4-1 Web 用户显示

操作	命令
显示HTTP的状态信息	display ip http
显示HTTPS的状态信息	display ip https
显示Web的页面菜单树	display web menu [chinese]
显示Web用户的相关信息	display web users

4.12 通过Web登录设备典型配置举例

4.12.1 使用HTTP方式登录设备典型配置举例

1. 组网需求

PC 与设备通过 IP 网络相连且路由可达，PC 和设备 Vlan-interface1 的 IP 地址分别为 192.168.101.99/24 和 192.168.100.99/24。

2. 组网图

图4-1 配置 HTTP 方式登录组网图



3. 配置步骤

(1) 配置 Device

配置 Web 用户名为 admin，认证密码为 admin，服务类型为 http，用户角色为 network-admin。

```
[Sysname] local-user admin
[Sysname-luser-manage-admin] service-type http
[Sysname-luser-manage-admin] authorization-attribute user-role network-admin
[Sysname-luser-manage-admin] password simple admin
[Sysname-luser-manage-admin] quit
```

配置开启 HTTP 服务。

```
[Sysname] ip http enable
```

(2) 配置 PC

在 PC 的浏览器地址栏内输入设备的 IP 地址并回车，浏览器将显示 Web 登录页面。

在“Web 用户登录”对话框中输入用户名、密码及验证码，点击<登录>按钮后即可登录，显示 Web 初始页面。成功登录后，用户可以在配置区对设备进行相关配置。

4.12.2 使用HTTPS方式登录设备典型配置举例

1. 组网需求

用户可以通过 Web 页面访问和控制设备。为了防止非法用户访问和控制设备，提高设备管理的安全性，设备要求用户以 HTTPS 的方式登录 Web 页面，利用 SSL 协议实现用户身份验证，并保证传输的数据不被窃听和篡改。

为了满足上述需求，需要进行如下配置：

- 配置 Device 作为 HTTPS 服务器，并为 Device 申请证书。
- 为 HTTPS 客户端 Host 申请证书，以便 Device 验证其身份。

其中，负责为 Device 和 Host 颁发证书的 CA(Certificate Authority, 证书颁发机构)名称为 new-ca。

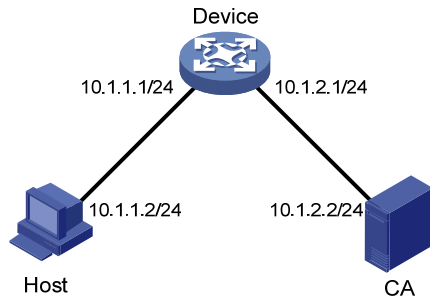


说明

- 本配置举例中，采用 Windows Server 作为 CA。在 CA 上需要安装 SCEP (Simple Certificate Enrollment Protocol, 简单证书注册协议) 插件。
- 进行下面的配置之前，需要确保 Device、Host、CA 之间路由可达。

2. 组网图

图4-2 HTTPS 配置组网图



3. 配置步骤

(1) 配置 HTTPS 服务器 Device

配置 PKI 实体 en，指定实体的通用名为 http-server1、FQDN 为 ssl.security.com。

```
<Device> system-view
[Device] pki entity en
[Device-pki-entity-en] common-name http-server1
[Device-pki-entity-en] fqdn ssl.security.com
[Device-pki-entity-en] quit
```

配置 PKI 域 1，指定信任的 CA 名称为 new-ca、注册服务器的 URL 为 http://10.1.2.2/certsrv/mscep/mscep.dll、证书申请的注册受理机构为 RA、实体名称为 en。

```
[Device] pki domain 1
[Device-pki-domain-1] ca identifier new-ca
[Device-pki-domain-1] certificate request url http://10.1.2.2/certsrv/mscep/mscep.dll
[Device-pki-domain-1] certificate request from ra
[Device-pki-domain-1] certificate request entity en
```

指定证书申请使用的 RSA 密钥对名称为 “hostkey”，用途为 “通用”，密钥对长度为 1024 比特。

```
[Device-pki-domain-1] public-key rsa general name hostkey length 1024
[Device-pki-domain-1] quit
```

生成本地的 RSA 密钥对。

```
[Device] public-key local create rsa
```

获取 CA 的证书。

```
[Device] pki retrieve-certificate domain 1 ca
```

为 Device 申请证书。

```
[Device] pki request-certificate domain 1
```

创建 SSL 服务器端策略 myssl，指定该策略使用 PKI 域 1，并配置服务器端需要验证客户端身份。

```
[Device] ssl server-policy myssl
[Device-ssl-server-policy-myssl] pki-domain 1
[Device-ssl-server-policy-myssl] client-verify enable
[Device-ssl-server-policy-myssl] quit
```

创建证书属性组 **mygroup1**，并配置证书属性规则，该规则规定证书颁发者的 DN（Distinguished Name，识别名）中包含 **new-ca**。

```
[Device] pki certificate attribute-group mygroup1
[Device-pki-cert-attribute-group-mygroup1] attribute 1 issuer-name dn ctn new-ca
[Device-pki-cert-attribute-group-mygroup1] quit
```

创建证书访问控制策略 **myacp**，并建立控制规则，该规则规定只有由 **new-ca** 颁发的证书可以通过证书访问控制策略的检测。

```
[Device] pki certificate access-control-policy myacp
[Device-pki-cert-acp-myacp] rule 1 permit mygroup1
[Device-pki-cert-acp-myacp] quit
```

配置 HTTPS 服务与 SSL 服务器端策略 **myssl** 关联。

```
[Device] ip https ssl-server-policy myssl
```

配置 HTTPS 服务与证书属性访问控制策略 **myacp** 关联，确保只有从 **new-ca** 获取证书的 HTTPS 客户端可以访问 HTTPS 服务器。

```
[Device] ip https certificate access-control-policy myacp
```

开启 HTTPS 服务。

```
[Device] ip https enable
```

创建本地用户 **usera**，密码为 **123**，服务类型为 **https**，用户角色为 **network-admin**。

```
[Device] local-user usera
[Device-luser-usera] password simple 123
[Device-luser-usera] service-type https
[Device-luser-usera] authorization-attribute user-role network-admin
```

(2) 配置 HTTPS 客户端 Host

在 Host 上打开 IE 浏览器，输入网址 **http://10.1.2.2/certsrv**，根据提示为 Host 申请证书。

(3) 验证配置结果

在 Host 上打开 IE 浏览器，输入网址 **https://10.1.1.1**，选择 **new-ca** 为 Host 颁发的证书，即可打开 Device 的 Web 登录页面。在登录页面，输入用户名 **usera**，密码 **123**，则可进入 Device 的 Web 配置页面，实现对 Device 的访问和控制。



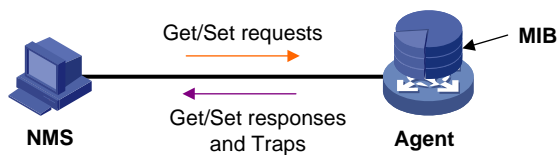
说明

- HTTPS 服务器的 URL 地址以 “https://” 开始，HTTP 服务器的 URL 地址以 “http://” 开始。
 - PKI 配置命令的详细介绍请参见“安全命令参考”中的“PKI”；
 - **public-key local create rsa** 命令的详细介绍请参见“安全命令参考”中的“公钥管理”；
 - SSL 配置命令的详细介绍请参见“安全命令参考”中的“SSL”。
-

5 配置通过SNMP登录设备

使用SNMP协议，用户可通过NMS（Network Management System，网络管理系统）登录到设备上，通过Set和Get等操作对设备进行管理、配置，如 [图 5-1](#) 所示。

图5-1 通过 SNMP 登录设备组网图



通过 SNMP 登录设备的详细介绍，请参见“网络管理和监控配置指导”中的“SNMP”。

6 配置通过RESTful登录设备

6.1 通过RESTful登录设备简介

为了方便用户对网络设备进行配置和维护，设备提供了 RESTful API（Representational State Transfer Application Programming Interface）。用户遵循 API 参数和返回值约定，使用 python、ruby 或 java 等语言进行编程，发送 HTTP 或 HTTPS 报文到设备进行认证，认证成功后，可以通过在 HTTP 或 HTTPS 报文中指定 RESTful API 操作来配置和维护设备，这些操作包括 Get、Put、Post、Delete 等等。

设备支持 HTTP 和 HTTPS 两种方式在 Internet 上传递 RESTful 请求信息。

6.2 FIPS相关说明

- 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”。
- 设备运行于 FIPS 模式时，不支持用户通过 HTTP 方式的 RESTful 登录。

6.3 配置通过基于HTTP的RESTful方式登录设备

- (1) 进入系统视图。

```
system-view
```

- (2) 开启基于 HTTP 的 RESTful 功能。

```
restful http enable
```

缺省情况下，基于 HTTP 的 RESTful 功能处于关闭状态。

- (3) 创建本地用户用于 RESTful 登录，并进入本地用户视图。

```
local-user user-name [ class manage ]
```

- (4) 设置本地用户的密码。

```
password [ { hash | simple } password ]
```

- (5) （可选）配置 RESTful 用户的角色。

```
authorization-attribute user-role user-role
```

缺省情况下，RESTful 用户的角色为 network-operator。

- (6) 配置 RESTful 用户的服务类型为 HTTP。

```
service-type http
```

缺省情况下，未配置用户的服务类型。

6.4 配置通过基于HTTPS的RESTful方式登录设备

- (1) 进入系统视图。

```
system-view
```


- (2) 开启基于 HTTPS 的 RESTful 功能。

restful https enable

缺省情况下，基于 HTTPS 的 RESTful 功能处于关闭状态。

- (3) 创建本地用户用于 RESTful 登录，并进入本地用户视图。

local-user *user-name* [**class** **manage**]

- (4) 设置本地用户的密码。

（非 FIPS 模式）

password [{ **hash** | **simple** } *password*]

（FIPS 模式）

password

- (5) （可选）配置 RESTful 用户的角色。

authorization-attribute user-role *user-role*

缺省情况下，RESTful 用户的角色为 *network-operator*。

- (6) 配置 RESTful 用户的服务类型为 HTTPS。

service-type https

缺省情况下，未配置用户的服务类型。

7 对登录用户的控制

7.1 登录用户控制简介

通过引用 ACL（Access Control List，访问控制列表），可以对访问设备的登录用户进行控制：

- 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，以免非法用户访问设备。

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

用户登录后，可以通过 AAA 功能来对用户使用的命令行进行授权和计费。

7.2 FIPS 相关说明

- 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”。
- 设备运行于 FIPS 模式时，不支持用户通过 Telnet 登录和 HTTP 方式的 Web 登录。

7.3 配置对 Telnet/SSH 用户的控制

7.3.1 配置对 Telnet 用户的控制

- (1) 进入系统视图。

```
system-view
```

- (2) 配置对 Telnet 用户的访问控制。

（IPv4 网络）

```
telnet server acl { advanced-acl-number | basic-acl-number | mac  
mac-acl-number }
```

（IPv6 网络）

```
telnet server ipv6 acl { ipv6 { advanced-acl-number | basic-acl-number }  
| mac mac-acl-number }
```

缺省情况下，未对 Telnet 用户进行 ACL 限制。

- (3) （可选）开启匹配 ACL deny 规则后打印日志信息功能。

```
telnet server acl-deny-log enable
```

缺省情况下，匹配 ACL deny 规则后打印日志信息功能处于关闭状态。

7.3.2 配置对 SSH 用户的控制

- (1) 进入系统视图。

```
system-view
```

- (2) 配置对 SSH 用户的访问控制。

(IPv4 网络)

```
ssh server acl { advanced-acl-number | basic-acl-number | mac  
mac-acl-number }
```

(IPv6 网络)

```
ssh server ipv6 acl { ipv6 { advanced-acl-number | basic-acl-number }  
| mac mac-acl-number }
```

缺省情况下，未 SSH 用户进行 ACL 限制。

- (3) (可选) 开启匹配 ACL deny 规则后打印日志信息功能。

```
ssh server acl-deny-log enable
```

关于 `ssh server acl`、`ssh server ipv6 acl` 和 `ssh server acl-deny-log enable` 命令的详细介绍请参见“安全命令参考”中的“SSH”。

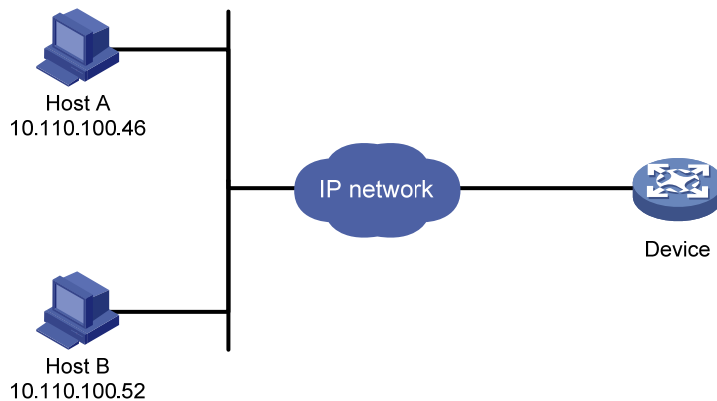
7.3.3 对Telnet用户的控制典型配置举例

1. 组网需求

通过源 IP 对 Telnet 进行控制，仅允许来自 10.110.100.52 和 10.110.100.46 的 Telnet 用户访问设备。

2. 组网图

图7-1 使用 ACL 对 Telnet 用户进行控制



3. 配置步骤

定义 ACL。

```
<Sysname> system-view  
[Sysname] acl basic 2000 match-order config  
[Sysname-acl-ipv4-basic-2000] rule 1 permit source 10.110.100.52 0  
[Sysname-acl-ipv4-basic-2000] rule 2 permit source 10.110.100.46 0  
[Sysname-acl-ipv4-basic-2000] quit
```

引用 ACL，允许源地址为 10.110.100.52 和 10.110.100.46 的 Telnet 用户访问设备。

```
[Sysname] telnet server acl 2000
```

7.4 配置对Web用户的控制

7.4.1 配置通过源IP对Web用户进行控制

- (1) 进入系统视图。

system-view

- (2) 引用访问控制列表对 Web 用户进行控制。请选择其中一项进行配置。

- 对 HTTP 登录用户进行控制：

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

- 对 HTTPS 登录用户进行控制：

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

缺省情况下，Web 用户没有引用访问控制列表。

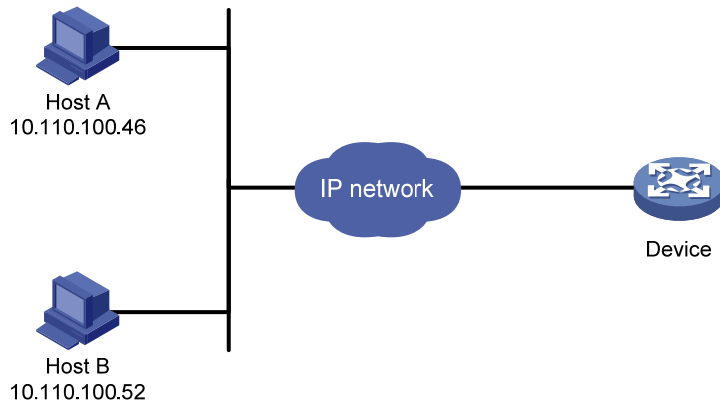
7.4.2 对Web用户的控制典型配置举例

1. 组网需求

通过源 IP 对 Web 用户进行控制，仅允许来自 10.110.100.52 的 Web 用户访问设备。

2. 组网图

图7-2 对 Device 的 HTTP 用户进行 ACL 控制



3. 配置步骤

定义基本访问控制列表。

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

```
[Sysname] acl basic 2030 match-order config
```

```
[Sysname-acl-ipv4-basic-2030] rule 1 permit source 10.110.100.52 0
```

引用访问控制列表，仅允许来自 10.110.100.52 的 Web 用户访问设备。

```
[Sysname] ip http acl 2030
```

7.5 配置对NMS的控制

7.5.1 功能简介

对 NMS 的访问进行控制的详细介绍请参见“网络管理和监控配置指导”中的“SNMP”。

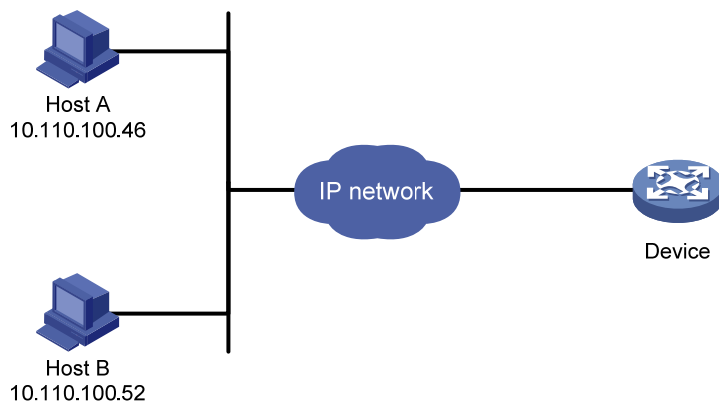
7.5.2 对NMS的控制典型配置举例

1. 组网需求

通过源 IP 对 NMS 进行控制，仅允许来自 10.110.100.52 和 10.110.100.46 的 NMS 访问设备。

2. 组网图

图7-3 使用 ACL 对 NMS 进行控制



3. 配置步骤

定义基本 ACL。

```
<Sysname> system-view
[Sysname] acl basic 2000 match-order config
[Sysname-acl-ipv4-basic-2000] rule 1 permit source 10.110.100.52 0
[Sysname-acl-ipv4-basic-2000] rule 2 permit source 10.110.100.46 0
[Sysname-acl-ipv4-basic-2000] quit
```

引用 ACL，仅允许来自 10.110.100.52 和 10.110.100.46 的 NMS 访问设备。

```
[Sysname] snmp-agent community read aaa acl 2000
[Sysname] snmp-agent group v2c groupa acl 2000
[Sysname] snmp-agent usm-user v2c usera groupa acl 2000
```

7.6 配置命令行授权功能

7.6.1 功能简介

缺省情况下，用户登录设备后可以使用的命令行由用户拥有的用户角色决定。当用户线采用 AAA 认证方式并配置命令行授权功能后，用户可使用的命令行将受到用户角色和 AAA 授权的双重限制。用户每执行一条命令都会进行授权检查，只有授权成功的命令才被允许执行。

7.6.2 配置限制和指导

要使配置的命令行授权功能生效，还需要在 ISP 域视图下配置命令行授权方法。命令行授权方法可以和 login 用户的授权方法相同，也可以不同。相关详细介绍请参见“安全配置指导”中的“AAA”。

7.6.3 配置步骤

- (1) 进入系统视图。

system-view

- (2) 进入用户线/用户线类视图。请选择其中一项进行配置。

- 进入用户线视图。

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

- 进入用户线类视图。

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

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。用户线类视图下的配置修改会在用户下次登录后生效。

- (3) 设置登录用户的认证方式为通过 AAA 认证。

（非 FIPS 模式）

authentication-mode scheme

缺省情况下，用户通过 VTY 用户线登录，认证方式为 **password**。

缺省情况下，用户通过 Console 口登录，认证方式如下：

- 对于 S5000V3-EI 系列交换机和 S5000E-X 系列交换机：
 - 设备采用出厂配置启动时，用户通过 Console 口登录，认证方式为 **scheme**。
 - 设备采用空配置启动时，用户通过 Console 口登录，认证方式为 **none**。
- 对于其它系列交换机，用户通过 Console 口登录，认证方式为 **none**。

关于空配置启动和缺省配置启动的详细介绍，请参见“基础配置指导”中的“配置文件管理”。

用户线视图下，**authentication-mode** 和 **protocol inbound** 存在关联绑定关系，当两条命令中的任意一条配置了非缺省值，那么另外一条取用户线下的值。

（FIPS 模式）

authentication-mode scheme

缺省情况下，用户登录设备的认证方式为 **scheme**。

用户线视图下，**authentication-mode** 和 **protocol inbound** 存在关联绑定关系，当两条命令中的任意一条配置了非缺省值，那么另外一条取用户线下的值。

- (4) 开启命令行授权功能。

command authorization

缺省情况下，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授权。

如果用户类视图下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，并且在该类型用户线视图下将无法关闭命令行授权功能。

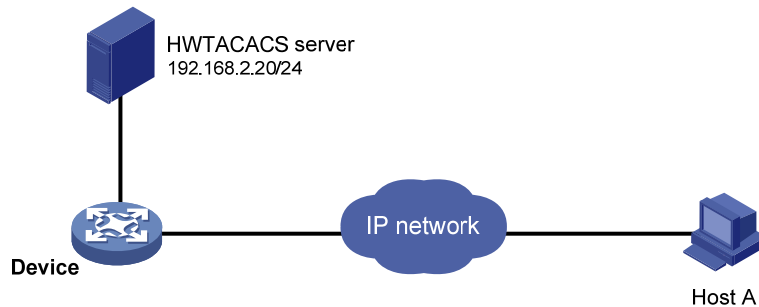
7.6.4 命令行授权典型配置举例

1. 组网需求

为了保证 **Device** 的安全，需要对登录用户执行命令的权限进行限制：用户 **Host A** 登录设备后，输入的命令必须先获得 **HWTACACS** 服务器的授权，才能执行。否则，不能执行该命令。如果 **HWTACACS** 服务器故障导致授权失败，则采用本地授权。

2. 组网图

图7-4 命令行授权配置组网图



3. 配置步骤

在设备上配置 IP 地址，以保证 **Device** 和 **Host A**、**Device** 和 **HWTACACS server** 之间互相路由可达。（配置步骤略）

开启设备的 **Telnet** 服务器功能，以使用户访问。

```
<Device> system-view
[Device] telnet server enable
```

配置用户登录设备时，需要输入用户名和密码进行 **AAA** 认证，可以使用的命令由认证结果决定。

```
[Device] line vty 0 4
[Device-line-vty0-4] authentication-mode scheme
```

开启命令行授权功能，限制用户只能使用授权成功的命令。

```
[Device-line-vty0-4] command authorization
[Device-line-vty0-4] quit
```

配置 **HWTACACS** 方案：授权服务器的 IP 地址:TCP 端口号为 **192.168.2.20:49**（该端口号必须和 **HWTACACS** 服务器上的设置一致），报文的加密密码是 **expert**，登录时不需要输入域名，使用缺省域。

```
[Device] hwtacacs scheme tac
[Device-hwtacacs-tac] primary authentication 192.168.2.20 49
[Device-hwtacacs-tac] primary authorization 192.168.2.20 49
[Device-hwtacacs-tac] key authentication simple expert
[Device-hwtacacs-tac] key authorization simple expert
[Device-hwtacacs-tac] user-name-format without-domain
[Device-hwtacacs-tac] quit
```

配置缺省域的命令行授权 **AAA** 方案，使用 **HWTACACS** 方案。

```
[Device] domain system
[Device-isp-system] authentication login hwtacacs-scheme tac local
```

```
[Device-isp-system] authorization command hwtacacs-scheme tac local
[Device-isp-system] quit
```

配置本地认证所需参数：创建本地用户 **monitor**，密码为明文的 **123**，可使用的服务类型为 **telnet**，用户角色为 **level-1**。

```
[Device] local-user monitor
[Device-luser-manage-monitor] password simple 123
[Device-luser-manage-monitor] service-type telnet
[Device-luser-manage-monitor] authorization-attribute user-role level-1
```

7.7 配置命令行计费功能

7.7.1 功能简介

当用户线采用 AAA 认证方式并配置命令行计费功能后，系统会将用户执行过的命令记录到 HWTACACS 服务器上，以便集中监视用户对设备的操作。命令行计费功能生效后，如果没有配命令行授权功能，则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。

7.7.2 配置限制和指导

要使配置的命令行计费功能生效，还需要在 ISP 域视图下配置命令行计费方法。命令行计费方法、命令行授权方法、login 用户的授权方法可以相同，也可以不同。相关详细介绍请参见“安全配置指导”中的“AAA”。

7.7.3 配置步骤

- (1) 进入系统视图。

system-view

- (2) 进入用户线/用户线类视图。请选择其中一项进行配置。

- 进入用户线视图。

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

- 进入用户线类视图。

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

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。用户线类视图下的配置修改将在用户下次登录后生效。

- (3) 设置登录用户的认证方式为通过 AAA 认证。

（非 FIPS 模式）

authentication-mode scheme

缺省情况下，用户通过 VTY 用户线登录，认证方式为 **password**。

缺省情况下，用户通过 Console 口登录，认证方式如下：

- 对于 S5000V3-EI 系列交换机和 S5000E-X 系列交换机：
 - 设备采用出厂配置启动时，用户通过 Console 口登录，认证方式为 **scheme**。

- 设备采用空配置启动时，用户通过 **Console** 口登录，认证方式为 **none**。
- 对于其它系列交换机，用户通过 **Console** 口登录，认证方式为 **none**。

关于空配置启动和缺省配置启动的详细介绍，请参见“基础配置指导”中的“配置文件管理”。

用户线视图下，**authentication-mode** 和 **protocol inbound** 存在关联绑定关系，当两条命令中的任意一条配置了非缺省值，那么另外一条取用户线下的值。

（FIPS 模式）

authentication-mode scheme

缺省情况下，用户登录设备的认证方式为 **scheme**。

用户线视图下，**authentication-mode** 和 **protocol inbound** 存在关联绑定关系，当两条命令中的任意一条配置了非缺省值，那么另外一条取用户线下的值。

(4) 开启命令行计费功能。

command accounting

缺省情况下，命令行计费功能处于关闭状态。

如果用户类视图下开启了命令行计费功能，则该类型用户线视图都开启命令行计费功能，并且在该类型用户线视图下将无法关闭命令行计费功能。

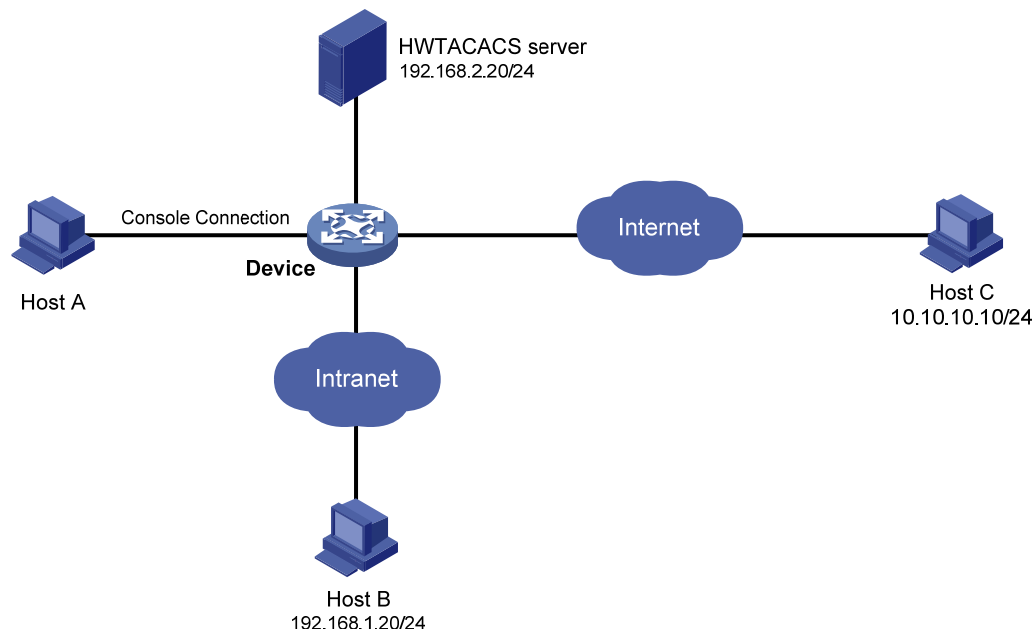
7.7.4 命令行计费典型配置举例

1. 组网需求

为便于集中控制、监控用户对设备的操作，需要将登录用户执行的命令发送到 HWTACACS 服务器进行记录。

2. 组网图

图7-5 命令行计费配置组网图



3. 配置步骤

开启设备的 Telnet 服务器功能，以使用户访问。

```
<Device> system-view
[Device] telnet server enable
```

配置使用 Console 口登录设备的用户执行的命令需要发送到 HWTACACS 服务器进行记录。

```
[Device] line aux 0
[Device-line-aux0] command accounting
[Device-line-aux0] quit
```

配置使用 Telnet 或者 SSH 登录的用户执行的命令需要发送到 HWTACACS 服务器进行记录。

```
[Device] line vty 0 63
[Device-line-vty0-63] command accounting
[Device-line-vty0-63] quit
```

配置 HWTACACS 方案：计费服务器的 IP 地址:TCP 端口号为 192.168.2.20:49，报文的加密密码是 expert，登录时不需要输入域名，使用缺省域。

```
[Device] hwtacacs scheme tac
[Device-hwtacacs-tac] primary accounting 192.168.2.20 49
[Device-hwtacacs-tac] key accounting simple expert
[Device-hwtacacs-tac] user-name-format without-domain
[Device-hwtacacs-tac] quit
```

配置缺省域的命令行计费 AAA 方案，使用 HWTACACS 方案。

```
[Device] domain system
[Device-isp-system] accounting command hwtacacs-scheme tac
[Device-isp-system] quit
```

目 录

1 FTP	1-1
1.1 FTP简介	1-1
1.1.1 FTP文件传输模式	1-1
1.1.2 FTP工作方式	1-1
1.2 FIPS相关说明	1-1
1.3 配置FTP服务器	1-1
1.3.1 FTP服务器配置任务简介	1-1
1.3.2 启动FTP服务器功能	1-2
1.3.3 配置FTP服务器的认证和授权	1-2
1.3.4 配置FTP服务器访问限制	1-2
1.3.5 配置FTP服务器连接管理参数	1-3
1.3.6 配置FTP服务器引用SSL	1-3
1.3.7 配置FTP服务器发送报文的DSCP优先级	1-3
1.3.8 释放已建立的FTP连接	1-4
1.3.9 FTP服务器显示和维护	1-4
1.3.10 FTP服务器典型配置举例	1-4
1.4 配置FTP客户端	1-6
1.4.1 FTP客户端配置任务简介	1-6
1.4.2 建立FTP连接	1-6
1.4.3 显示帮助信息	1-7
1.4.4 查看FTP服务器上的目录/文件	1-8
1.4.5 操作FTP服务器上的目录	1-8
1.4.6 操作FTP客户端本地的工作目录	1-8
1.4.7 操作FTP服务器上的文件	1-8
1.4.8 更改登录用户	1-9
1.4.9 FTP连接的维护与调试	1-10
1.4.10 断开FTP连接	1-10
1.4.11 FTP客户端显示和维护	1-11
1.4.12 FTP客户端典型配置举例	1-11
2 TFTP	2-1
2.1 TFTP简介	2-1
2.2 FIPS相关说明	2-1

2.3 TFTP配置限制和指导	2-1
2.4 配置IPv4 TFTP客户端	2-1
2.5 配置IPv6 TFTP客户端	2-2

1 FTP

1.1 FTP简介

FTP（File Transfer Protocol，文件传输协议）用于在 FTP 服务器和 FTP 客户端之间传输文件，是 IP 网络上传输文件的通用协议。

FTP 协议使用 TCP 端口 20 和 21 进行传输。端口 20 用于传输数据，端口 21 用于传输控制消息。设备既可以作为 FTP 服务器，也可以作为 FTP 客户端。

1.1.1 FTP文件传输模式

FTP 有两种文件传输模式：

- 二进制模式，用于传输非文本文件（比如后缀名为.app、.bin 和.btm 的文件）；
- ASCII 码模式，用于传输文本格式的文件（比如后缀名为.txt、.bat 和.cfg 的文件）。

当设备作为 FTP 客户端时，用户可通过命令行指定使用的传输模式，缺省为二进制模式；当设备作为 FTP 服务器时，使用的传输模式由 FTP 客户端决定。

1.1.2 FTP工作方式

FTP 有两种工作方式：

- 主动方式（PORT）：建立数据连接时由 FTP 服务器发起连接请求，当 FTP 客户端处于防火墙后时不适用（如 FTP 客户端处于私网内）。
- 被动方式（PASV）：建立数据连接时由 FTP 客户端发起连接请求，当 FTP 服务器限制客户端连接其高位端口（一般情况下大于 1024）时不适用。

是否使用被动方式由 FTP 客户端程序决定，不同 FTP 客户端软件对 FTP 工作方式的支持情况可能不同，请在使用时以软件的实际情况为准。

1.2 FIPS相关说明

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”。

1.3 配置FTP服务器

1.3.1 FTP服务器配置任务简介

FTP 服务器配置任务如下：

- (1) [启动FTP服务器功能](#)
- (2) [配置FTP服务器的认证和授权](#)
- (3) （可选）[配置FTP服务器访问限制](#)
- (4) （可选）[配置FTP服务器连接管理参数](#)

- (5) (可选) [配置FTP服务器引用SSL](#)
- (6) (可选) [配置FTP服务器发送报文的DSCP优先级](#)
- (7) (可选) [释放已建立的FTP连接](#)

1.3.2 启动FTP服务器功能

- (1) 进入系统视图。

system-view

- (2) 启动 FTP 服务器功能。

ftp server enable

缺省情况下，FTP 服务器功能处于关闭状态。

1.3.3 配置FTP服务器的认证和授权

只有认证通过并授权成功的用户，才能通过 FTP 访问设备上的指定路径。

设备对 FTP 客户端的认证，有以下两种方式：

- 本地认证：设备作为认证服务器，在本设备上验证 FTP 客户端的用户名和密码是否合法。
- 远程认证：远程认证是指设备将用户输入的用户名/密码发送给远端的认证服务器，由认证服务器来验证用户名/密码是否匹配。

设备对 FTP 客户端的授权，有以下两种方式：

- 本地授权：设备给 FTP 客户端授权，指定 FTP 客户端可以使用设备上的某个路径。
- 远程授权：远程服务器给 FTP 客户端授权，指定 FTP 客户端可以使用设备上的某个路径。

关于认证和授权的详细配置请参见“安全配置指导”中的“AAA”。

1.3.4 配置FTP服务器访问限制

1. 功能简介

通过将 FTP 服务与 ACL 关联，可以过滤掉来自某些 FTP 客户端的 FTP 请求报文，只允许符合 ACL 过滤规则的 FTP 客户端访问设备。

2. 配置限制和指导

该配置只过滤新建立的 FTP 连接，不会对已建立的 FTP 连接和操作造成影响。如果多次使用该命令配置 FTP 服务与 ACL 关联，FTP 服务将只与最后一次配置的 ACL 关联。

3. 配置步骤

- (1) 进入系统视图。

system-view

- (2) 配置 FTP 服务器访问限制。

**ftp server acl { advanced-acl-number | basic-acl-number | ipv6
{ advanced-acl-number | basic-acl-number } }**

缺省情况下，FTP 服务器的访问不受 ACL 限制。

- (3) 开启匹配 ACL deny 规则后打印日志信息功能。

ftp server acl-deny-log enable

缺省情况下，匹配 ACL deny 规则后打印日志信息功能处于关闭状态。

1.3.5 配置FTP服务器连接管理参数

- (1) 进入系统视图。

```
system-view
```

- (2) 配置 FTP 服务器的连接空闲时间。

```
ftp timeout minutes
```

缺省情况下，连接空闲时间为 30 分钟。

如果在设置的连接空闲时间到期时，FTP 服务器和客户端一直没有信息交互，则断开它们之间的连接。

- (3) 配置使用 FTP 方式同时登录设备的在线的最大用户连接数。

```
aaa session-limit ftp max-sessions
```

缺省的最大用户连接数为 32。

配置本命令后，已经在线的用户连接不会受到影响，只对新的用户连接生效。如果当前在线的用户连接数已经达到最大值，则新的连接请求会被拒绝，登录会失败。

关于该命令的详细描述请参见“安全 命令参考”中的“AAA”。

1.3.6 配置FTP服务器引用SSL

1. 功能简介

当支持 FTP 安全扩展协议的两台设备建立 FTP 连接时，通过将 FTP 服务与 SSL 服务器端策略关联，可以建立一条安全的 SSL 连接来传输数据，保证 FTP 传输的安全性。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 配置 FTP 服务器引用 SSL。

```
ftp server ssl-server-policy policy-name
```

缺省情况下，FTP 服务器未引用 SSL 服务器端策略。

1.3.7 配置FTP服务器发送报文的DSCP优先级

- (1) 进入系统视图。

```
system-view
```

- (2) 配置 FTP 服务器发送的 FTP 报文的 DSCP 优先级。

(IPv4 网络)

```
ftp server dscp dscp-value
```

(IPv6 网络)

```
ftp server ipv6 dscp dscp-value
```

缺省情况下，FTP 服务器发送的 FTP 报文的 DSCP 优先级为 0。

1.3.8 释放已建立的FTP连接

请在用户视图下执行本命令，释放已建立的 FTP 连接。请选择其中一项进行配置。

- 强制释放与指定用户之间的 FTP 连接。
`free ftp user username`
- 强制释放与指定 IP 地址的主机之间的 FTP 连接。
`free ftp user-ip [ipv6] ip-address [port port]`

1.3.9 FTP服务器显示和维护

完成上述配置后，在任意视图下执行 **display** 命令可以显示 FTP 服务器的配置和运行情况，通过查看显示信息验证配置的效果。

表1-1 FTP 服务器显示和维护

操作	命令
查看当前FTP服务器的配置和运行情况	<code>display ftp-server</code>
查看当前FTP登录用户的详细情况	<code>display ftp-user</code>

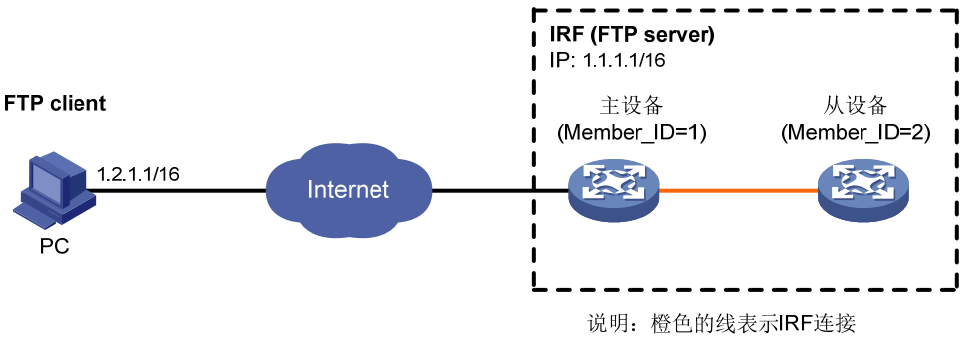
1.3.10 FTP服务器典型配置举例

1. 组网需求

- 主设备和从设备共同组成 IRF。主设备的成员编号为 1，从设备的成员编号为 2。
- IRF 作为 FTP 服务器，PC 作为 FTP 客户端。
- 将存储在 PC 上的文件 temp.bin 上传到 FTP 服务器，并使用 FTP 功能备份 IRF 的配置文件。
- FTP 客户端登录 FTP 服务器的用户名为 abc，密码为 123456。

2. 组网图

图1-1 FTP 服务器典型配置组网图



3. 配置步骤



说明

如果主设备和从设备剩余的内存空间不够，请使用 **delete /unreserved file-url** 命令删除部分暂时不用的文件后再执行以下操作。

配置前请确保Device和PC之间路由可达，IP地址如 [图 1-1](#) 所示，具体配置步骤略。

(1) IRF（FTP server）上的配置

在 IRF 上添加一个本地用户 **abc**，并设置其认证密码为 **123456**，访问时使用的用户角色为 **network-admin**，授权访问目录为 **Flash** 的根目录，**abc** 可以使用的服务类型为 **FTP**。

```
<Sysname> system-view
[Sysname] local-user abc class manage
[Sysname-luser-abc] password simple 123456
[Sysname-luser-abc] authorization-attribute user-role network-admin work-directory
flash: /
```



说明

如果要直接访问从设备 **Flash** 的根目录，需要将 “authorization-attribute work-directory flash:/” 配置中的 “flash:/” 替换成 “slot2#flash:/”。

```
[Sysname-luser-abc] service-type ftp
[Sysname-luser-abc] quit
# 启动 IRF 的 FTP 服务功能。
[Sysname] ftp server enable
[Sysname] quit
```

(2) PC（FTP client）的配置

以用户名 **abc**、密码 **123456** 登录 **FTP** 服务器。

```
c:\> ftp 1.1.1.1
Connected to 1.1.1.1.
220 FTP service ready.
User(1.1.1.1:(none)):abc
331 Password required for abc.
Password:
230 User logged in.
```

将传输模式设置为 **ascii**，并将 IRF 的配置文件 **config.cfg** 下载到 **PC** 本地进行备份。

```
ftp> ascii
200 TYPE is now ASCII
ftp> get config.cfg back-config.cfg
```

将传输模式设置为 **binary**，并上传文件 **temp.bin** 到主设备存储介质的根目录下。

```
ftp> binary
200 TYPE is now 8-bit binary
ftp> put temp.bin
```

退出 **FTP**。

ftp> bye

1.4 配置FTP客户端

1.4.1 FTP客户端配置任务简介

FTP 客户端配置任务如下：

- (1) [建立FTP连接](#)
- (2) （可选）[显示帮助信息](#)
- (3) （可选）[查看FTP服务器上的目录/文件](#)
- (4) （可选）[操作FTP服务器上的目录](#)
- (5) （可选）[操作FTP服务器上的文件](#)
- (6) （可选）[更改登录用户](#)
- (7) （可选）[FTP连接的维护与调试](#)
- (8) （可选）[断开FTP连接](#)

1.4.2 建立FTP连接

1. 建立FTP连接配置任务简介

建立 FTP 连接配置任务如下：

- (1) （可选）[配置FTP客户端发送的FTP报文的源地址](#)
- (2) [登录FTP服务器](#)
- (3) [配置FTP文件传输方式](#)

2. 配置限制和指导

- 使用 **ftp client source** 命令指定了源地址后，又在 **ftp** 命令中指定了源地址，则采用 **ftp** 命令中指定的源地址进行通信。
- 使用 **ftp client ipv6 source** 命令指定了源地址后，又在 **ftp ipv6** 命令中指定了源地址，则采用 **ftp ipv6** 命令中指定的源地址进行通信。

3. 配置FTP客户端发送的FTP报文的源地址

- (1) 进入系统视图。

system-view

- (2) 配置 FTP 客户端发送的 FTP 报文的源地址。

（IPv4 网络）

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

缺省情况下，未配置源地址，使用路由出接口的主 IP 地址作为设备发送 FTP 报文的源 IP 地址。

（IPv6 网络）

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

缺省情况下，未配置源地址，设备自动选择 IPv6 FTP 报文的源 IPv6 地址，具体选择原则请参见 RFC 3484。

4. 登录FTP服务器

- 从用户视图登录 FTP 服务器。

(IPv4 网络)

```
ftp [ ftp-server [ service-port ] [ dscp dscp-value | source { interface  
interface-type interface-number | ip source-ip-address } | -d ] * ]
```

(IPv6 网络)

```
ftp ipv6 [ ftp-server [ service-port ] [ dscp dscp-value | source  
{ interface interface-type interface-number | ipv6 source-ipv6-address }  
| -d ] * [ -i interface-type interface-number ] ]
```

- 从 FTP 客户端视图登录 FTP 服务器。
 - a. 请在用户视图下执行本命令，进入 FTP 客户端视图。

```
ftp [ ipv6 ]
```

- b. 登录 FTP 服务器。

```
open server-address [ service-port ]
```

5. 配置FTP文件传输方式

- 请在用户视图下执行本命令，进入 FTP 客户端视图。

```
ftp
```

- 设置 FTP 文件传输的模式。
 - 配置 FTP 文件传输的模式为 ASCII 模式。

```
ascii
```

- 配置 FTP 文件传输的模式为二进制模式。

```
binary
```

缺省情况下，文件传输模式为二进制模式。

- 切换数据的传输方式。

```
passive
```

缺省情况下，数据传输的方式为被动方式。

1.4.3 显示帮助信息

- 请在用户视图下执行本命令，进入 FTP 客户端视图。

```
ftp
```

- 显示命令或命令的帮助信息。

- 方式一

```
help [ command-name ]
```

- 方式二

```
? [ command-name ]
```

1.4.4 查看FTP服务器上的目录/文件

- (1) 请在用户视图下执行本命令，进入 FTP 客户端视图。

ftp

- (2) 查看 FTP 服务器上的目录/文件。

- 方式一

dir [remotefile [localfile]]

- 方式二

ls [remotefile [localfile]]

1.4.5 操作FTP服务器上的目录

1. 配置准备

使用 **dir** 或者 **ls** 命令查看 FTP 服务器上的目录/文件的详细信息。

2. 配置步骤

- (1) 请在用户视图下执行本命令，进入 FTP 客户端视图。

ftp

- (2) 操作 FTP 服务器上的目录

- 显示当前用户正在访问的 FTP 服务器上的路径。

pwd

- 切换 FTP 服务器上的工作路径。

cd { directory | .. | / }

- 退出 FTP 服务器的当前目录，返回 FTP 服务器的上一级目录。

cdup

- 在 FTP 服务器上创建目录。

mkdir directory

- 删除 FTP 服务器上指定的目录。

rmdir directory

1.4.6 操作FTP客户端本地的工作目录

- (1) 请在用户视图下执行本命令，进入 FTP 客户端视图。

ftp

- (2) 显示或切换 FTP 客户端本地的工作路径。

lcd [directory | /]

上传的文件为该路径下的文件时，缺省情况下文件下载后也将保存到该路径。

1.4.7 操作FTP服务器上的文件

1. 配置准备

使用 **dir** 或者 **ls** 命令了解 FTP 服务器上的目录结构以及文件所处的位置。

2. 配置步骤

- (1) 请在用户视图下执行本命令，进入 FTP 客户端视图。

ftp

- (2) 操作 FTP 服务器上的文件

- 删除 FTP 服务器上的文件。

delete *remotefile*

用户必须具有删除的权限才能执行该操作。

- 重命名文件。

rename [*oldfilename* [*newfilename*]]

- 上传本地文件到 FTP 服务器。

put *localfile* [*remotefile*]

- 下载 FTP 服务器上的文件。

get *remotefile* [*localfile*]

- 在原文件的内容后面添加新文件的内容。

append *localfile* [*remotefile*]

- 指定重传点。

restart *marker*

配合 **put**、**get**、**append** 等命令使用。

- 更新本地文件。

newer *remotefile*

- 从本地文件的尾部开始获取文件的剩余内容。

reget *remotefile* [*localfile*]

1.4.8 更改登录用户

1. 功能简介

当设备作为 FTP 客户端，与 FTP 服务器连接建立成功后，可以通过该功能实现不同权限用户之间的切换。用户成功切换后，不会影响当前的 FTP 连接（即 FTP 控制连接、数据连接以及连接状态都不变）。

2. 配置限制和指导

如果在用户切换时，输入的用户名/密码错误，则会断开当前连接，用户必须重新登录才能继续访问 FTP 服务器。

3. 配置步骤

- (1) 请在用户视图下执行本命令，进入 FTP 客户端视图。

ftp

- (2) 在现有 FTP 连接上重新发起 FTP 认证。

user *username* [*password*]

1.4.9 FTP连接的维护与调试

1. 功能简介

当设备作为 FTP 客户端，与 FTP 服务器连接建立成功后，通过以下命令，可以帮助用户定位和诊断 FTP 连接出现的问题。

2. 配置步骤

- (1) 请在用户视图下执行本命令，进入 FTP 客户端视图。

ftp

- (2) 维护与调试 FTP 连接

- 显示 FTP 服务器支持的 FTP 相关协议命令字。

rhelp

- 显示 FTP 服务器支持的 FTP 相关协议命令字的帮助信息。

rhelp protocol-command

- 显示 FTP 服务器的状态。

rstatus

- 显示 FTP 服务器上指定目录或文件的详细信息。

rstatus remotefile

- 显示当前 FTP 连接的状态。

status

- 显示 FTP 服务器的系统信息。

system

- 切换 FTP 功能的协议信息开关。

verbose

缺省情况下，FTP 协议信息开关处于开启状态。

- 打开 FTP 调试信息开关。

debug

缺省情况下，FTP 客户端调试信息开关处于关闭状态。

- 清除缓存的命令应答。

reset

1.4.10 断开FTP连接

- (1) 请在用户视图下执行本命令，进入 FTP 客户端视图。

ftp

- (2) 断开与 FTP 服务器的连接。请选择其中一项进行配置。

- 断开与 FTP 服务器的连接，并留在 FTP 客户端视图。请选择其中一项进行配置。

disconnect

close

- 断开与 FTP 服务器的连接，并退回到用户视图。请选择其中一项进行配置。

bye
quit

1.4.11 FTP客户端显示和维护

在完成上述配置后，可在任意视图下执行 **display** 命令，通过查看显示信息验证配置的效果。

表1-2 FTP 客户端显示和维护

操作	命令
显示设备作为FTP客户端时的源地址配置	display ftp client source

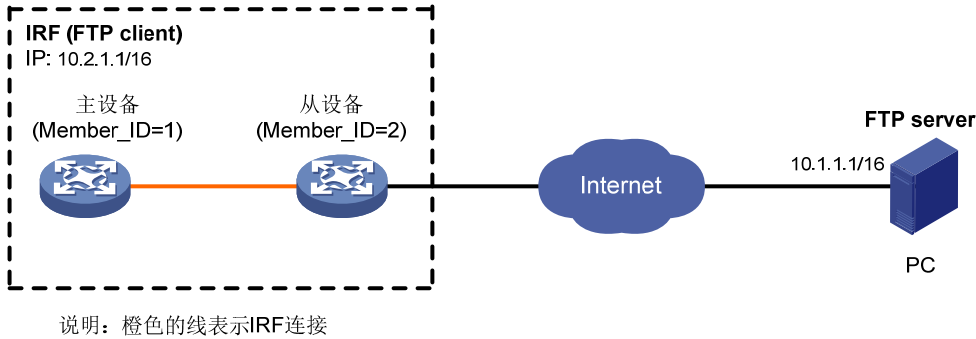
1.4.12 FTP客户端典型配置举例

1. 组网需求

- 主设备和从设备两台成员设备组成 IRF。主设备的成员编号为 1，从设备的成员编号为 2。
- IRF 作为 FTP 客户端，PC 作为 FTP 服务器。
- IRF 从 PC 上下载新的文件 temp.bin，并将配置文件上传到 PC 进行备份。
- PC 上已设置设备登录 FTP 服务器的用户名为 abc，密码为 123456。

2. 组网图

图1-2 FTP 客户端典型配置组网图



3. 配置步骤



说明

如果主设备和从设备剩余的内存空间不够，请使用 **delete /unreserved file-url** 命令删除部分暂时不用的文件后再执行以下操作。

配置前请确保IRF和PC之间路由可达，IP地址如 [图 1-2](#) 所示，具体配置步骤略。

以用户名 abc、密码 123456 登录 FTP 服务器。

```
<Sysname> ftp 10.1.1.1  
Press CTRL+C to abort.
```

```

Connected to 10.1.1.1 (10.1.1.1).
220 WFTPD 2.0 service (by Texas Imperial Software) ready for new user
User (10.1.1.1:(none)): abc
331 Give me your password, please
Password:
230 Logged in successfully
Remote system type is MSDOS.
ftp>
# 将传输模式设置为 binary，以便传输文件。
ftp> binary
200 TYPE is now 8-bit binary
# 将文件 temp.bin 从 FTP 服务器下载到 IRF。
• 将文件 temp.bin 从 FTP 服务器下载到主设备存储介质的根目录下。
  ftp> get temp.bin
  local: temp.bin remote: temp.bin
  150 Connecting to port 47457
  226 File successfully transferred
  23951480 bytes received in 95.399 seconds (251.0 kbyte/s)
• 将文件 temp.bin 从 FTP 服务器下载到从设备存储介质的根目录下。
  ftp> get temp.bin slot2#flash:/temp.bin
# 将 IRF 的配置文件 config.cfg 上传到 FTP 服务器进行备份。
ftp> ascii
200 TYPE is now ASCII
ftp> put config.cfg back-config.cfg
local: config.cfg remote: back-config.cfg
150 Connecting to port 47461
226 File successfully transferred
3494 bytes sent in 5.646 seconds (618.00 kbyte/s)
ftp> bye
221-Goodbye. You uploaded 2 and downloaded 2 kbytes.
221 Logout.
<Sysname>

```


2 TFTP

2.1 TFTP简介

TFTP (Trivial File Transfer Protocol, 简单文件传输协议) 用于在 TFTP 服务器和 TFTP 客户端之间传输文件。它基于 UDP 协议, 使用 UDP 端口建立连接、收/发数据报文。与基于 TCP 的 FTP 协议比较, TFTP 不需要认证, 没有复杂的报文交互, 部署简单, 适用于客户端和服务端均很可靠的网络环境。

2.2 FIPS相关说明

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”。

2.3 TFTP配置限制和指导

当设备作为 TFTP 客户端时, 可以把设备的文件上传到 TFTP 服务器, 还可以从 TFTP 服务器下载文件到设备。如果下载时设备上已经存在一个和目标文件名同名的文件, 则系统会先将设备上已有的文件删除, 再保存远端文件。如果下载失败 (如网络断开等原因), 则原文件已被删除, 无法恢复。因此, 当下载启动文件或配置文件等重要文件时, 建议使用一个当前目录下不存在的文件名作为目标文件名。

目前, 设备只能作为 TFTP 客户端, 不支持作为 TFTP 服务器。

2.4 配置IPv4 TFTP客户端

- (1) 进入系统视图。

```
system-view
```

- (2) (可选) 使用 ACL 限制设备可访问哪些 TFTP 服务器。

```
tftp-server acl acl-number
```

缺省情况下, 未使用 ACL 对设备可访问的 TFTP 服务器进行限制。

- (3) 配置 TFTP 客户端的源地址。

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

缺省情况下, 未配置源地址, 使用路由出接口的主 IP 地址作为设备发送 TFTP 报文的源 IP 地址。

- (4) 退回用户视图。

```
quit
```

- (5) 在 IPv4 网络, 用 TFTP 上传/下载文件。

```
tftp tftp-server { get | put | sget } source-filename
[ destination-filename ] [ dscp dscp-value | source { interface
interface-type interface-number | ip source-ip-address } ] *
```

使用 **tftp client source** 命令指定了源地址后，又在 **tftp** 命令中指定了源地址，则采用 **tftp** 命令中指定的源地址进行通信。

2.5 配置IPv6 TFTP客户端

- (1) 进入系统视图。

```
system-view
```

- (2) （可选）在 IPv6 网络，使用 ACL 限制设备可访问哪些 TFTP 服务器。

```
tftp-server ipv6 acl ipv6-acl-number
```

缺省情况下，未使用 ACL 对设备可访问的 TFTP 服务器进行限制。

- (3) 在 IPv6 网络，配置 TFTP 客户端的源地址。

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

缺省情况下，未配置源地址，设备自动选择 IPv6 TFTP 报文的源 IPv6 地址，具体选择原则请参见 RFC 3484。

- (4) 退回用户视图。

```
quit
```

- (5) 在 IPv6 网络，用 TFTP 上传/下载文件。

```
tftp ipv6 tftp-server [ -i interface-type interface-number ] { get | put |
sget } source-filename [ destination-filename ] [ dscp dscp-value |
source { interface interface-type interface-number | ipv6
source-ipv6-address } ] *
```

使用 **tftp client ipv6 source** 命令指定了源地址后，又在 **tftp ipv6** 命令中指定了源地址，则采用 **tftp ipv6** 命令中指定的源地址进行通信。

目 录

1 文件系统管理	1-1
1.1 文件系统管理简介	1-1
1.1.1 存储介质和文件系统	1-1
1.1.2 目录	1-1
1.1.3 文件	1-2
1.1.4 文件夹和文件指定方法	1-2
1.2 FIPS相关说明	1-3
1.3 文件系统配置限制和指导	1-3
1.4 存储介质和文件系统操作	1-3
1.4.1 格式化文件系统	1-3
1.4.2 恢复文件系统的空间	1-3
1.5 文件和文件夹操作	1-3
1.5.1 设置操作文件和文件夹时是否提示	1-3
1.5.2 显示文件和文件夹信息	1-4
1.5.3 显示文本文件内容	1-4
1.5.4 显示当前工作路径	1-4
1.5.5 修改当前工作路径	1-4
1.5.6 创建文件夹	1-4
1.5.7 重命名文件和文件夹	1-4
1.5.8 复制文件	1-5
1.5.9 移动文件	1-5
1.5.10 删除和恢复文件	1-5
1.5.11 删除文件夹	1-6
1.5.12 打包文件/文件夹	1-6
1.5.13 解包文件/文件夹	1-6
1.5.14 压缩文件	1-6
1.5.15 解压缩文件	1-6
1.5.16 计算文件摘要	1-7

1 文件系统管理

1.1 文件系统管理简介

本章介绍了如何对文件系统文件进行管理和操作。

1.1.1 存储介质和文件系统

设备支持的存储介质为固定存储介质 **flash**。设备上一个存储介质即为一个文件系统。

1. 存储介质和文件系统名称

存储介质 **flash** 及其文件系统名称由如下部分组成：

- 存储介质类型：**flash** 的类型名称即为“**flash**”。
- 冒号：存储介质名称的结束符。



说明

文件系统名称中的英文字符输入时区分大小写，必须为小写字符。

2. 文件系统位置的指定方法

对文件系统进行操作时，需要指定存储介质的位置，存储介质位置的表示方式为：**slot n #**。其中 n 为 IRF 中成员设备的编号。例如：**slot2#**代表成员设备 2 上的存储介质。不指定 **slot** 参数时，表示 IRF 中主设备的存储介质。



说明

文件系统位置中的所有英文字符输入时区分大小写，必须为小写字符。

3. 缺省文件系统

设备支持多个存储介质，用户登录设备后缺省使用的文件系统即为缺省文件系统。例如，保存当前配置时，如果不输入存储介质位置及名称，则配置文件将保存在缺省文件系统的根目录下。

通过设置 **Bootware** 菜单或者 **Bootrom** 菜单可以更改缺省文件系统，详情请参见配套发布的版本说明书。

1.1.2 目录

设备的文件系统采用树形目录结构，用户可以通过文件夹操作来改变目录层级，方便的管理文件。

1. 根目录

用户登录设备后，缺省目录即为根目录。

根目录用“/”表示。例如 **flash:/**表示 **flash** 的根目录。

2. 工作目录

工作目录也被称为当前工作目录。

3. 文件夹的命名

文件夹名称中可以包含数字、字母或特殊字符（除了*|V?<>":.）。为文件夹命名时，首字符不能使用“.”。否则，系统将把名称首字符为“.”的文件夹处理为隐藏文件夹。

4. 常用文件夹

设备出厂时会携带一些文件夹，在运行过程中可能会自动产生一些文件夹，这些文件夹包括：

- **diagfile**: 用于存放诊断信息文件的文件夹
- **logfile**: 用于存放日志文件的文件夹
- **seclog**: 用于存放安全日志文件的文件夹
- **versionInfo**: 用于存放版本信息文件的文件夹
- 其他名称的文件夹

1.1.3 文件

1. 文件的命名

文件名中可以输入以数字、字母、特殊字符（除了*|V?<>":.）为组合的字符串。为文件命名时，首字母请不要使用“.”。因为系统会把名称首字母为“.”的文件当成隐藏文件。

2. 常见文件类型

设备出厂时会携带一些文件，在运行过程中可能会自动产生一些文件，这些文件包括：

- **xx.ipe**（复合软件包套件，是启动软件包的集合）
- **xx.bin**（启动软件包）
- **xx.cfg**（配置文件）
- **xx.mdb**（二进制格式的配置文件）
- **xx.log**（用于存放日志的文件）
- 其他后缀的文件

1.1.4 文件夹和文件指定方法

路径是指文件或文件夹所在的位置，包括绝对路径和相对路径。

1. 文件夹指定方法

设备支持使用相对路径和绝对路径指定文件夹。例如，当前工作目录为 **flash:/**，可以通过绝对路径 **flash:/test/test1/test2/**（末尾的“/”为可选）或相对路径 **test/test1/test2/**（末尾的“/”为可选）进入 **test2** 文件夹。

2. 文件指定方法

设备支持使用相对路径和绝对路径指定文件。例如，当前工作目录为 **flash:/test/**，可以通过绝对路径 **flash:/test/test1/test2/samplefile.cfg** 或相对路径 **test1/test2/samplefile.cfg** 指定 **test2** 文件夹下的 **samplefile.cfg** 文件。

1.2 FIPS相关说明

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”。

1.3 文件系统配置限制和指导

- 在执行文件系统操作过程中，禁止对存储介质进行插拔或主设备和从设备的倒换操作。否则，可能会引起文件系统的损坏。
- 当一个用户对存储介质或文件系统执行 **fixdisk**、**format** 操作时，其他用户不能访问该存储介质或文件系统。

1.4 存储介质和文件系统操作

1.4.1 格式化文件系统

1. 配置限制和指导

格式化操作将导致文件系统的所有文件丢失，并且不可恢复，请谨慎使用。

用户对文件系统执行格式化操作时，如果同时还有其他用户在访问该文件系统，系统会提示格式化操作失败。

2. 配置步骤

请在用户视图下执行本命令，格式化文件系统。

```
format filesystem
```

1.4.2 恢复文件系统的空间

1. 配置限制和指导

由于异常操作等原因，文件系统的某些空间可能不可用，用户可以通过 **fixdisk** 命令来恢复文件系统的空间。

用户对文件系统执行 **fixdisk** 操作时，如果同时还有其他用户在访问该文件系统，系统会提示 **fixdisk** 操作失败。

2. 配置步骤

请在用户视图下执行本命令，恢复文件系统的空间。

```
fixdisk filesystem
```

1.5 文件和文件夹操作

1.5.1 设置操作文件和文件夹时是否提示

1. 功能简介

用户可以通过命令行来设置执行文件或文件夹操作时是否提示：

- 当设置为 **alert**，并且用户对文件或文件夹进行有危险性的操作时，系统会要求用户进行交互确认。
- 当设置为 **quiet**，则用户对文件或文件夹进行任何操作，系统均不要求用户进行确认。该方式可能会导致一些因误操作而发生的、不可恢复的、对系统造成破坏的情况产生。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 设置操作文件或文件夹时是否提示。

```
file prompt { alert | quiet }
```

缺省情况下，用户对文件或文件夹进行操作时，系统会要求用户进行交互确认。

1.5.2 显示文件和文件夹信息

请在用户视图下执行本命令，显示文件夹和文件信息。

```
dir [ /all ] [ file | directory | /all-filesystems ]
```

多用户同时执行文件操作时，比如同时创建或删除文件或文件夹，可能导致该命令显示结果不准确。

1.5.3 显示文本文件内容

请在用户视图下执行本命令，显示文本文件的内容。

```
more file
```

1.5.4 显示当前工作路径

请在用户视图下执行本命令，显示当前工作路径。

```
pwd
```

1.5.5 修改当前工作路径

1. 功能简介

用户登录设备后，缺省的工作目录为主设备缺省文件系统的根目录。

2. 配置步骤

请在用户视图下执行本命令，修改当前工作路径。

```
cd { directory | .. }
```

1.5.6 创建文件夹

请在用户视图下执行本命令，创建文件夹。

```
mkdir directory
```

1.5.7 重命名文件和文件夹

请在用户视图下执行本命令，重命名文件和文件夹。

```
rename { source-file | source-directory } { dest-file | dest-directory }
```

1.5.8 复制文件

请在用户视图下执行本命令，复制文件。

（非 FIPS 模式）

```
copy source-file { dest-file | dest-directory } [ source interface  
interface-type interface-number ]
```

（FIPS 模式）

```
copy source-file { dest-file | dest-directory }
```

1.5.9 移动文件

请在用户视图下执行本命令，移动文件。

```
move source-file { dest-file | dest-directory }
```

1.5.10 删除和恢复文件

1. 功能简介

可以通过以下方式删除文件：

- 临时删除文件：执行 **delete file** 命令删除文件。采用该方式删除的文件被转移到回收站中，可以通过 **undelete file** 命令恢复。
- 永久删除文件：永久删除的文件不能恢复。

回收站文件夹名均为“.trash”，用户可以进入相应的存储介质，用 **dir /all .trash**，或者 **cd .trash** 进入回收站文件夹，使用 **dir** 命令查看回收站中的文件。

每个文件系统下都有一个回收站。

2. 配置限制和指导

不能对回收站中的文件执行 **delete** 命令，否则会影响回收站的正常使用。如果需要删除回收站中的文件，请执行 **reset recycle-bin** 命令。

通过临时删除文件的方式删除的文件仍然占用存储空间，如果用户经常临时删除文件，则可能导致设备的存储空间不足。此时请查看回收站中是否有文件，通过执行 **reset recycle-bin** 命令彻底删除回收站中的文件，以释放空间。

3. 删除文件

请在用户视图下执行本命令，删除文件。

- 删除文件到回收站。
delete file
- 删除回收站中的文件。
reset recycle-bin [**/force**]
- 永久删除文件。
delete /unreserved file

4. 恢复回收站中的文件

请在用户视图下执行该命令，恢复回收站中的文件。

```
undelete file
```

1.5.11 删除文件夹

1. 配置限制和指导

在删除文件夹前，必须先永久删除或者暂时删除文件夹中的所有文件和子文件夹。

临时删除文件后，执行 **rmdir** 删除该文件所在文件夹时，该文件将从回收站中彻底删除。

2. 配置步骤

请在用户视图下执行该命令，删除文件夹。

```
rmdir directory
```

1.5.12 打包文件/文件夹

1. 功能简介

打包是将用户指定的原文件或文件夹打包保存成一个新文件（原文件或文件夹仍然存在）。该功能可用于文件备份和整理。

用户可选择直接打包保存或者打包后压缩保存。选择打包后压缩保存可节省存储空间。

2. 配置步骤

请在用户视图下执行本命令，将多个文件或文件夹打包成一个新文件。

```
tar create [ gz ] archive-file dest-file [ verbose ] source { source-file  
| source-directory }&<1-5>
```

1.5.13 解包文件/文件夹

1. 功能简介

解包是打包的逆向操作，是将打包文件还原成原文件或文件夹。

2. 配置步骤

(1) （可选）请在用户视图下执行本命令，显示指定打包文件夹中包含的文件和文件夹的名称。

```
tar list archive-file file
```

(2) 解包文件和文件夹。

```
tar extract archive-file file [ verbose ] [ screen | to directory ]
```

1.5.14 压缩文件

请在用户视图下执行本命令，压缩指定的文件。

```
gzip file
```

1.5.15 解压缩文件

请在用户视图下执行本命令，解压缩指定的文件。

gunzip *file*

1.5.16 计算文件摘要

1. 功能简介

使用摘要算法计算文件的摘要值，通常用于验证文件的正确性和完整性。

2. 配置步骤

请在用户视图下执行以下命令，计算文件的摘要值。

- 使用 SHA-256 摘要算法计算文件的摘要值。

sha256sum *file*

- 使用 MD5 摘要算法计算文件的摘要值。

md5sum *file*

目 录

1 配置文件管理.....	1-1
1.1 配置文件简介.....	1-1
1.1.1 配置的类型.....	1-1
1.1.2 配置文件的类型及其选择规则.....	1-2
1.1.3 下次启动配置文件.....	1-2
1.1.4 配置文件的内容与格式.....	1-3
1.1.5 配置回滚.....	1-3
1.2 FIPS相关说明.....	1-3
1.3 开启配置文件加密功能.....	1-3
1.4 保存当前配置.....	1-4
1.5 显示配置差异.....	1-5
1.6 配置回滚.....	1-5
1.6.1 配置回滚任务简介.....	1-5
1.6.2 配置备份参数.....	1-6
1.6.3 备份当前配置.....	1-7
1.6.4 执行配置回滚.....	1-8
1.7 配置延迟提交功能.....	1-9
1.8 配置下次启动配置文件.....	1-9
1.9 备份/恢复主用下次启动配置文件.....	1-10
1.9.1 功能简介.....	1-10
1.9.2 配置限制和指导.....	1-10
1.9.3 配置准备.....	1-10
1.9.4 备份主用下次启动配置文件.....	1-10
1.9.5 恢复主用下次启动配置文件.....	1-11
1.10 删除下次启动配置文件.....	1-11
1.11 配置文件管理显示和维护.....	1-11

1 配置文件管理

1.1 配置文件简介

配置文件是用来保存配置的文件。设备重启后，这些配置继续生效。当网络中多台设备需要批量配置时，可以将相同的配置保存到配置文件，再上传/下载到所有设备，在所有设备上执行该配置文件来实现设备的批量配置。

1.1.1 配置的类型

1. 空配置

软件版本中所有的软件功能都被赋予一个缺省值，这些缺省值的集合被称为“空配置”。缺省值无法通过命令行直接查看，可通过查看产品当前软件版本的命令手册，了解各软件功能的缺省值。

2. 出厂配置

设备在出厂时，通常会带有一些基本的配置，称为出厂配置。它用来保证设备在没有配置文件或者配置文件损坏的情况下，能够正常启动、运行。

可以使用 **display default-configuration** 命令查看设备的出厂配置。



说明

出厂配置可能与命令行的缺省情况不一致，不同型号的设备会根据需要定制各自的出厂配置。

3. 启动配置

设备启动时运行的配置即为启动配置。如果没有指定启动配置文件或者启动配置文件损坏，则系统会使用出厂配置作为启动配置。

可以通过以下方式查看启动配置：

- 设备启动后且还没有进行配置前，使用 **display current-configuration** 命令查看当前启动配置。
- 使用 **display startup** 命令查看本次启动使用的配置文件和下次启动使用的主用、备用配置文件，再使用 **more** 命令查看相应配置文件的内容。（**more** 命令的详细介绍请参见“基础配置命令参考”中“文件系统管理”）
- 使用 **display saved-configuration** 命令查看下次启动配置文件的内容。

4. 当前配置

系统当前正在运行的配置称为当前配置。它包括启动配置和设备运行过程中用户进行的配置。当前配置存放在设备的临时缓存中，如果不保存，设备运行过程中用户进行的配置在设备重启后会丢失。

可以使用 **display current-configuration** 命令查看设备的当前配置。

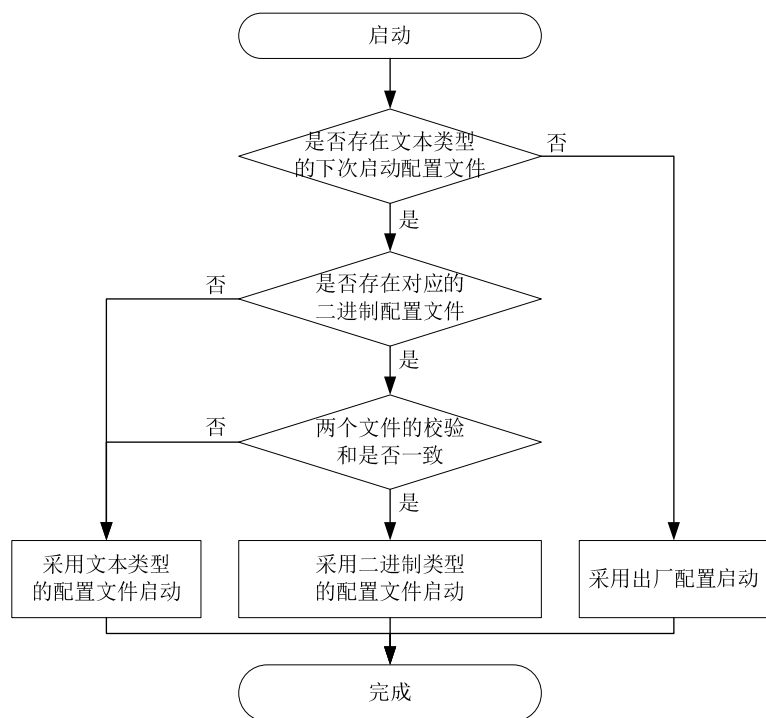
1.1.2 配置文件的类型及其选择规则

执行 **save** 命令保存配置时，系统将自动生成一个文本类型的配置文件和一个二进制类型的配置文件，两个文件的内容完全相同。

- 文本类型配置文件：后缀名为“.cfg”，可以通过 **more** 命令查看，或使用文本编辑器修改该文件的内容。文本类型配置文件可以单独保存到存储介质中，无需对应的二进制类型的配置文件。
- 二进制类型配置文件：后缀为“.mdb”，仅能够使用软件解析该类配置文件，用户不能读取和编辑文件内容。二进制类型的配置文件不能单独保存到存储介质中，必须有对应的文本类型的配置文件。该类型配置文件的加载速度快，设备启动时优先使用该类型配置文件。

设备启动时，文本类型配置文件和二进制类型配置文件的选择规则如 [图 1-1](#) 所示。

图1-1 文本类型配置文件和二进制类型配置文件的选择规则



如无特殊说明，下文描述的配置文件均指文本类型的配置文件。

1.1.3 下次启动配置文件

设备上可以同时存在多个配置文件。设备本次启动使用的配置文件称为当前启动配置文件；设备下次启动使用的配置文件称为下次启动配置文件。

设备支持配置两个下次启动配置文件，一个为主用配置文件，一个为备用配置文件。

设备启动时，配置文件的选择规则如下：

- (1) 优先使用主用下次启动配置文件。
- (2) 如果主用下次启动配置文件不存在或损坏，使用备用下次启动配置文件。
- (3) 如果主用和备用下次启动配置文件都不存在或损坏，则使用出厂配置启动。

1.1.4 配置文件的内容与格式

配置文件对内容和格式有严格定义，为保证配置文件的正确运行，建议使用设备自动生成的配置文件。如果需要手工修改配置文件，请遵循配置文件的内容和格式规则。

配置文件的内容和格式规则如下：

- 配置文件的内容为命令的完整形式。
- 配置文件以命令视图为基本框架，同一命令视图的命令组织在一起，形成一节，节与节之间用#隔开。
- 以 return 结束。

下面摘录了配置文件的部分内容。

```
#
local-user root class manage
    password hash
    $h$6$Twd73mLrN8O2vvD5$Cz1vgdpR4KoTiRQNE9pg33gU14Br2p1VguczLSVyJLO2huV5Syx/LfDIIf8ROLtVErJ
    /C31oq2rFtmNuyZf4STw==
    service-type ssh telnet terminal
    authorization-attribute user-role network-admin
    authorization-attribute user-role network-operator
#
interface Vlan-interface1
    ip address 192.168.1.84 255.255.255.0
#
```

1.1.5 配置回滚

配置回滚是在不重启设备的情况下，将当前的配置回退到指定配置文件中的配置状态。

配置回滚主要应用于：

- 当前配置错误，且错误配置太多不方便定位或逐条回退，需要将当前配置回滚到某个正确的配置状态。
- 设备的应用环境变化，需要使用某个配置文件中的配置信息运行，在不重启设备的情况下将当前配置回滚到指定配置文件中的配置状态。

1.2 FIPS相关说明

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”。

1.3 开启配置文件加密功能

1. 功能简介

配置文件加密功能就是设备在执行 save 命令将当前配置保存到配置文件的同时，将配置文件加密。

2. 配置限制和指导

加密后的文件能被所有运行 Comware V7 平台软件的设备识别和解析。因此，为了防止非法用户对加密后配置文件的解析，需确保只有合法用户才能获取加密后的配置文件。运行其它平台软件的设备不能识别和解析。

开启配置文件加密功能后，执行 **save** 命令生成的配置文件是加密后的配置文件，将不能使用 **more** 命令查看加密配置文件（后缀名为“.cfg”的配置文件）的内容，且加密配置文件将不能参与配置差异的比较（如不能使用 **display current-configuration diff** 命令比较下次启动配置文件与运行配置之间的差异、不能将加密后的配置文件作为 **display diff** 命令的参数）。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 开启配置文件加密功能。

```
configuration encrypt { private-key | public-key }
```

缺省情况下，配置文件加密功能处于关闭状态。

1.4 保存当前配置

1. 功能简介

保存配置前，配置仅保存在内存中，设备重启后，设备将恢复为出厂配置。如果要使当前配置在设备重启后仍然生效，则需要将当前配置保存到下次启动配置文件中。

2. 配置限制和指导

在保存当前运行配置时，请不要重启设备或者给设备断电，以免造成下次启动配置文件丢失。

如果成员设备退出 IRF，该成员设备的配置不会丢失，仍然保存在内存中，但是会从当前运行配置中删除。成员设备再次加入 IRF 时，对应配置自动从内存中恢复到当前运行配置中。

如果成员设备退出后，将当前运行配置保存到了下次启动配置文件中，该成员设备的配置不会写入到配置文件中。如需将退出的成员设备的配置保存到下次启动配置文件中，请执行如下操作：

- (1) 将成员设备重新加入 IRF 并重启该成员设备。
- (2) 待成员设备正常工作后，执行 **display current-configuration** 命令，确认成员设备的配置已恢复到当前运行配置中。
- (3) 保存当前运行配置到下次启动配置文件中。



注意

如果在成员设备退出 IRF 后，执行了重启操作，该成员设备的配置将无法恢复。

3. 配置步骤

可在任意视图下执行本命令，保存当前配置。

- 将当前配置保存到指定文件，但不会将该文件设置为下次启动配置文件。

```
save file-url [ all | slot slot-number ]
```

- 将当前配置保存到所有成员设备存储介质的根目录下，并将该文件设置为下次启动配置文件。

```
save [ safely ] [ backup | main ] [ force ] [ changed ]
```

为了安全起见，建议选用 **safely** 参数。执行该命令时，请不要重启设备或者给设备断电，以免造成下次启动配置文件丢失。

1.5 显示配置差异

1. 功能简介

用户通过命令可以查看两份配置文件、指定配置文件与当前运行配置、指定配置文件与下次启动文件、当前运行配置与下次启动文件之间的差异。用户可根据差异来决定是否保存当前配置或者进行配置替换。

2. 配置步骤

可在任意视图下执行本命令，显示配置差异。请选择其中一项进行配置。

- 显示指定配置文件和指定配置文件、当前运行配置、下次启动配置文件之间的差异。
display diff configfile file-name-s { configfile file-name-d | current-configuration | startup-configuration }
- 显示当前运行配置和指定配置文件、下次启动配置文件之间的差异。
display diff current-configuration { configfile file-name-d | startup-configuration }
- 显示下次启动配置文件和指定配置文件之间的差异。
display diff startup-configuration configfile file-name-d
- 显示下次启动配置文件与当前运行配置之间的差异。请选择其中一项进行配置。
 - 方式一
display diff startup-configuration current-configuration
 - 方式二
display current-configuration diff

1.6 配置回滚

1.6.1 配置回滚任务简介

配置回滚配置任务如下：

- (1) [配置备份参数](#)
- (2) [备份当前配置](#)
 - [自动备份当前配置](#)
 - [手动备份当前配置](#)
- (3) [执行配置回滚](#)

1.6.2 配置备份参数

1. 功能简介

备份当前配置前必须设置备份文件的保存路径和文件名前缀。可以设置将备份文件保存在本地，或者保存在远程 SCP 服务器上。

如果设置备份文件保存在本地，设备备份当前运行配置时，将当前的配置以前缀_序号.cfg 格式（例如 archive_1.cfg）保存到该命令指定路径下的配置文件中。序号自动从 1 开始编号，依次加 1，累加至 1000 后重新从 1 开始编号。

如果设置备份文件保存在本地，修改备份文件的保存路径或文件名前缀或设备重启后，备份序号从 1 开始重新自动编号，原来的备份文件不再作为备份文件而作为普通配置文件存在。执行 **display archive configuration** 命令不会显示原来的回滚配置信息。

如果设置备份文件保存在远程 SCP 服务器，设备备份当前运行配置时，将在远程服务器指定的路径下生成以“前缀_YYYYMMDD_HHMMSS.cfg”命名的配置文件（例如 archive_20170526_203430.cfg）。

2. 配置限制和指导

FIPS 模式下，不支持将配置文件备份到远程 SCP 服务器的功能。

archive configuration server 命令和 **archive configuration location** 命令具有互斥性，不能同时配置。设置备份文件保存在远程 SCP 服务器后，如要使用 **archive configuration location** 命令指定配置文件备份到本地时使用的参数，需先使用 **undo archive configuration server** 恢复缺省情况。同理，设置备份文件保存在本地后，要指定配置文件备份到远程 SCP 服务器时使用的参数，需先使用 **undo archive configuration location** 命令恢复缺省情况。

如果设置备份文件保存在本地，备份文件数量达到上限后，再次保存备份文件时，系统将删除保存时间最早的备份文件，以保存新的备份文件。

配置文件在远程 SCP 服务器上的备份数量不受 **archive configuration max** 配置的限制。

执行 **undo archive configuration location** 命令后，用户将不能手工备份当前配置到本地，系统也不再自动备份当前配置到本地。同时，**archive configuration max** 和 **archive configuration interval** 命令会恢复为缺省情况、**display archive configuration** 的显示信息会被清除。

执行 **undo archive configuration server** 命令后，用户将不能手工备份当前配置到远程 SCP 服务器，系统也不再自动备份当前配置到远程 SCP 服务器。同时，**archive configuration interval** 命令会恢复为缺省情况、**display archive configuration** 的显示信息会被清除。

3. 配置本地备份参数

- (1) 进入系统视图。

```
system-view
```

- (2) 配置备份配置文件的本地保存路径和文件名前缀。

```
archive configuration location directory filename-prefix  
filename-prefix
```

缺省情况下，未配置备份配置文件的本地保存路径和文件名前缀。

directory 必须是主设备上已存在的路径，且参数中不能包含成员编号。

- (3) (可选) 配置备份配置文件的最大数。

```
archive configuration max file-number
```

缺省情况下, 备份配置文件的最大数为 5。

请根据系统剩余存储空间配置备份配置文件的最大数。

4. 配置远程备份参数

- (1) 进入系统视图。

```
system-view
```

- (2) 配置备份配置文件在远程 SCP 服务器的保存路径、文件名前缀。

```
archive configuration server scp { ipv4-address | ipv6 ipv6-address }  
[ port port-number ] [ directory directory ] filename-prefix  
filename-prefix
```

缺省情况下, 未配置备份配置文件在远程 SCP 服务器的保存路径和文件名前缀。

- (3) 配置登录远程 SCP 服务器的用户名。

```
archive configuration server user user-name
```

缺省情况下, 未配置登录远程 SCP 服务器的用户名。

- (4) 配置登录远程 SCP 服务器的密码。

```
archive configuration server password { cipher | simple } string
```

缺省情况下, 未配置登录远程 SCP 服务器的密码。

1.6.3 备份当前配置

1. 功能简介

设备支持自动备份和手动备份两种备份配置的方式。

- 自动备份当前配置: 系统按照已配置的时间间隔自动备份当前配置。
- 手动备份当前配置: 用户随时可以执行手动备份命令行备份当前配置。例如, 需要对设备进行复杂配置过程中, 不定期手动备份当前配置, 以便配置错误时, 使用配置回滚功能将当前配置回滚至正确情况。

2. 配置限制和指导

如果设置备份文件保存在本地, 该功能只将当前配置备份到主设备, 不会保存到从设备。

在自动或手动备份配置文件时, 不能清除 **display archive configuration** 命令显示的回滚配置信息。

3. 自动备份当前配置

- (1) 进入系统视图。

```
system-view
```

- (2) 开启自动备份当前配置功能, 并设置自动备份的时间间隔。

```
archive configuration interval interval
```

缺省情况下, 自动备份当前配置功能处于关闭状态。

4. 手动备份当前配置

请在用户视图下执行本命令，手动备份当前配置。

archive configuration

1.6.4 执行配置回滚

1. 功能简介

配置回滚时，系统将对当前配置和回滚配置文件中配置的差异，并做如下处理：

- 不处理当前配置与回滚配置文件中相同的命令。
- 对于存在于当前配置但不存在于回滚配置文件的命令，回滚操作将取消当前配置中的命令，即执行相应的反向操作。
- 对于存在于回滚配置文件但不存在于当前配置的命令，回滚操作将执行这些命令。
- 对于当前配置和回滚配置文件中不同的命令，配置回滚将先取消这些配置，再执行回滚配置文件中的相应命令。

2. 配置限制和指导

执行配置回滚操作时（执行 **configuration replace file** 命令）不能进行主从设备倒换操作，否则可能造成配置回滚终止。

配置能否回滚成功由命令的具体处理决定，存在以下情况时，某条命令会回滚失败，系统会跳过回滚失败的命令，直接处理下一条命令：

- 命令不支持完整 **undo** 命令，即直接在配置命令前添加 **undo** 关键字构成的命令不存在，设备不识别。比如命令 **A [B] C**，对应的 **undo** 命令为 **undo A C**，但是配置 **A B C** 回滚的时候，系统会去自动执行 **undo A B C**，此时系统会认为不支持 **undo A B C** 而造成配置 **A B C** 回滚失败。
- 配置不能取消（如硬件相关的命令）。
- 若不同视图下的各配置命令存在依赖关系，命令可能执行失败。
- 使用的配置文件不是由 **save** 命令、自动备份或手工备份生成的完整文件，或是不同类型设备的配置文件，配置回滚可能不能完全恢复至配置文件中的配置状态。因此，需要用户确保回滚配置文件中配置的正确性和与当前设备的兼容性。

3. 配置步骤

- (1) 进入系统视图。

system-view

- (2) 执行配置回滚。

configuration replace file filename

filename 只能是明文配置文件，不能是被加密的配置文件，且必须是本地保存的配置文件。

1.7 配置延迟提交功能

1. 功能简介

使用配置延迟提交功能,需要使用 **configuration commit delay** 命令指定配置提交超时时间,之后所进行的配置,可以使用 **configuration commit** 命令延迟提交。

执行 **configuration commit delay** 命令后,系统会创建一个定时器和一个配置回滚点(配置回滚点记录了系统当前的配置),之后所做的配置会下发生效,但是如果在定时器超时前,没有执行 **configuration commit** 命令,系统会自动将配置回滚到配置回滚点的状态。

在用户对设备进行远程配置时,可以使用本功能,以防止错误配置导致网络中断,用户不能再连接到设备。

2. 配置限制和指导

使用配置延迟提交功能时,请注意:

- 请在单一用户的环境下使用配置延迟提交功能。
- 在设备执行配置回滚时,请停止其他配置,等待配置回滚完成后再继续操作。
- 在定时器超时前,如果再次执行 **configuration commit delay** 命令,系统会更新定时器为新指定的配置提交超时时间间隔,但不再创建配置回滚点。
- **configuration commit delay** 命令是一次生效命令。使用此命令指定了配置提交超时时间后,若执行了 **configuration commit** 命令或者延迟时间超时,需要再次使用配置延迟提交功能,请重新指定配置提交超时时间。

3. 配置步骤

(1) 进入系统视图。

```
system-view
```

(2) 设置配置提交超时时间。

```
configuration commit delay delay-time
```

(3) (可选) 提交当前配置。

```
configuration commit
```

提交执行 **configuration commit delay** 命令后的配置。

1.8 配置下次启动配置文件

1. 配置限制和指导

执行 **undo startup saved-configuration** 命令并重启 IRF 或 IRF 中的成员设备时,会导致 IRF 分裂,请谨慎使用。

主用下次启动配置文件和备用下次启动配置文件可以设置为同一文件,但为了更可靠,建议设置为不同的文件,或者将一份配置保存在两个不同名的文件中,一个设置为主用,一个设置为备用。

在执行 **undo startup saved-configuration** 命令之后,系统会将主用/备用下次启动配置文件均设置为 NULL,但不会删除该文件。

执行 **save** 命令将当前配置保存到指定配置文件时,系统会自动把该文件设置为设备的主用下次启动配置文件。详细配置请参见“[1.4 保存当前配置](#)”。

2. 配置准备

所有成员设备的下次启动配置文件必须是相同的文件，因此，使用本命令前，请确保指定的配置文件已经保存在所有成员设备相同类型存储介质的根目录下，否则，操作失败。

3. 配置步骤

(1) 配置下次启动时的配置文件。请选择其中一项进行配置。

- 请在用户视图下执行本命令，配置下次启动时的配置文件。

```
startup saved-configuration cfgfile [ backup | main ]
```

缺省情况下，没有配置下次启动配置文件。

- 可在任意视图下执行本命令，在保存当前配置到配置文件的同时设置该配置文件为下次启动配置文件。

```
save [ safely ] [ backup | main ] [ force ]
```

本命令的详细介绍请参见 [1.4 保存当前配置](#)。

不指定 **main** 和 **backup** 参数时，缺省使用 **main**。

(2) （可选）可在任意视图下执行以下命令，验证配置。

- 显示用于本次及下次启动的配置文件的名称。

```
display startup
```

- 查看下次启动配置文件的内容。

```
display saved-configuration
```

1.9 备份/恢复主用下次启动配置文件

1.9.1 功能简介

备份是指将设备的主用下次启动配置文件备份到指定的 TFTP 服务器。

恢复是指将 TFTP 服务器上保存的配置文件下载到设备并设置为主用下次启动配置文件。

1.9.2 配置限制和指导

设备运行于 FIPS 模式时，不支持备份或者恢复主用下次启动配置文件。

1.9.3 配置准备

在执行配置文件的备份操作前，请进行以下操作：

- 保证设备与服务器之间的路由可达，服务器端开启了 TFTP 服务，执行备份操作的客户端设备已获得了相应的读写权限。
- 在任意视图下使用 **display startup** 命令查看设备是否设置了下次启动配置文件。如果没有指定下次启动配置文件，或者配置文件不存在，备份操作将失败。

1.9.4 备份主用下次启动配置文件

请在用户视图下执行本命令，将设备的主用下次启动配置文件备份到指定的 TFTP 服务器。

```
backup startup-configuration to { ipv4-server | ipv6 ipv6-server }  
[ dest-filename ]
```

1.9.5 恢复主用下次启动配置文件

- (1) 请在用户视图下执行本命令，将 TFTP 服务器上保存的配置文件下载到设备并设置为主用下次启动配置文件。

```
restore startup-configuration from { ipv4-server | ipv6 ipv6-server }  
src-filename
```

- (2) （可选）可在任意视图下执行以下命令，验证配置。

- 显示用于本次及下次启动的配置文件的名称。

```
display startup
```

- 查看下次启动配置文件的内容。

```
display saved-configuration
```

1.10 删除下次启动配置文件

1. 功能简介

当用户不再使用当前系统指定的下次启动配置文件启动设备时，使用该功能可将下次启动配置文件从设备上删除。

主备用下次启动配置文件都删除后，设备重启将采用出厂配置启动。

用户可以只删除主用下次启动配置文件，或者只删除备用下次启动配置文件。

如果设备的主用下次启动配置文件和备用下次启动配置文件相同，仅执行一次删除操作（例如指定了 **backup** 参数），系统只将相应的下次启动配置文件设置为 **NULL**，不删除该文件，需要再次执行删除操作（指定 **main** 参数），才能将该配置文件彻底删除。

2. 配置限制和指导

本特性会将下次启动配置文件从所有成员设备上彻底删除，请谨慎使用。

3. 配置步骤

请在用户视图下执行本命令，删除下次启动配置文件。

```
reset saved-configuration [ backup | main ]
```

不指定 **main** 和 **backup** 参数时，删除主用下次启动配置文件。

1.11 配置文件管理显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置文件的使用情况。用户可以通过查看显示信息验证配置的效果。

表1-1 配置文件管理显示和维护

操作	命令
显示配置回滚功能的相关信息	display archive configuration

操作	命令
显示设备当前生效的配置	display current-configuration [[configuration [<i>module-name</i>] interface [<i>interface-type</i> [<i>interface-number</i>]]] slot <i>slot-number</i>]
显示下次启动配置文件与运行配置之间的差异	display current-configuration diff
显示出厂配置	display default-configuration
查看两份配置之间的差异	display diff configfile <i>file-name-s</i> { configfile <i>file-name-d</i> current-configuration startup-configuration } display diff current-configuration { configfile <i>file-name-d</i> startup-configuration } display diff startup-configuration { configfile <i>file-name-d</i> current-configuration }
显示下次启动配置文件的内容	display saved-configuration
显示用于本次及下次启动的配置文件的名称	display startup
显示当前视图下生效的配置	display this

目 录

1 软件升级.....	1-1
1.1 软件升级简介.....	1-1
1.1.1 软件包类型.....	1-1
1.1.2 软件包的发布形式.....	1-1
1.1.3 设备支持的软件升级方式.....	1-2
1.1.4 设备软件升级.....	1-2
1.2 软件升级限制和指导.....	1-3
1.3 通过Boot-Loader方式升级设备软件.....	1-3
1.3.1 升级任务简介.....	1-3
1.3.2 升级准备.....	1-3
1.3.3 加载BootWare程序.....	1-3
1.3.4 指定新的启动软件包并完成升级.....	1-4
1.3.5 将IRF主设备的当前软件包同步到从设备.....	1-4
1.4 通过Feature包或补丁包方式升级启动软件.....	1-5
1.4.1 安装Feature包或补丁包.....	1-5
1.4.2 卸载Feature包或补丁包.....	1-5
1.5 软件升级显示和维护.....	1-6
1.6 软件升级典型配置举例.....	1-6
1.6.1 通过重启方式升级启动软件包配置举例.....	1-6

1 软件升级

1.1 软件升级简介

软件升级用于对软件包进行版本升级、增加特定软件特性或是对软件缺陷进行修复。本章简要介绍了软件升级涉及的主要软件包类型、软件升级方式、以及如何从命令行通过 **Boot-Loader** 方式对软件进行升级。

1.1.1 软件包类型

软件升级涉及的软件包有：**BootWare** 程序和 **Comware** 软件包。

1. BootWare程序

BootWare 程序也称为 **Boot ROM** 程序，包括基本段和扩展段。基本段用于引导系统启动。扩展段用于硬件初始化并提供系统管理菜单。在设备无法正常启动的时，用户可通过这些菜单加载软件和下次启动配置文件，并管理文件。为避免软件适配错误，**BootWare** 程序通常集成到 **Comware** 软件的 **Boot** 包中。

2. Comware软件包

Comware 软件包包含 **Boot** 包、**System** 包、**Feature** 包和补丁包。

- (1) **Boot** 包：包含 **Linux** 内核程序，提供进程管理、内存管理、文件系统管理等功能的 **.bin** 文件。
- (2) **System** 包：包含 **Comware** 内核和基本功能模块的 **.bin** 文件，比如设备管理、接口管理、配置管理和路由模块等。
- (3) **Feature** 包：包含高级或定制业务的 **.bin** 文件。用户可根据需要购买 **Feature** 包。
- (4) 补丁（**Patch**）包：用来修复设备软件缺陷的 **.bin** 程序文件。补丁包只能修复启动软件包的缺陷，不涉及功能的添加和删除。补丁包分为叠加补丁包和非叠加补丁包，具体定义如下：
 - 叠加补丁包：不同版本的叠加补丁包能够同时安装多个，并且最新版本的补丁包可以包含、不包含或不完全包含旧版本的补丁包所解决的问题。
 - 非叠加补丁包：设备只能安装一个非叠加补丁包，安装新版本补丁包的同时，设备会卸载旧版本的补丁包，新版本的补丁包包含旧版本的补丁包所解决的所有问题。

叠加补丁包和非叠加补丁包可以同时安装到设备上。

设备必须具有 **Boot** 包和 **System** 包才能正常运行。

1.1.2 软件包的发布形式

软件包有如下两种发布形式：

- 以 **.bin** 文件的形式独立发布。这种发布形式需要用户关注软件包之间的适配关系。
- 打包为 **.ipe** 的 **IPE**（**Image Package Envelope**，复合软件包套件）文件发布，减少软件包之间的版本适配错误。设备在加载 **IPE** 文件时，会自动将它解压缩成多个 **.bin** 文件，并使用这些 **.bin** 文件来升级设备。



说明

软件包文件的名称采用“设备简称-Comware 版本-软件包类型-release 号”的形式。在本文档中，Boot 包和 System 包的文件名统一采用 boot.bin 和 system.bin。

1.1.3 设备支持的软件升级方式

表1-1 软件升级方式

升级方式	升级对象	说明
通过命令行的Boot-Loader方式升级	<ul style="list-style-type: none"> • BootWare 程序 • Comware 软件包（该方式不能升级补丁包） 	该方式需要重启设备，会导致当前业务中断
通过BootWare菜单进行升级	<ul style="list-style-type: none"> • BootWare 程序 • Comware 软件包 	<p>该方式用于无法启动Comware系统时进行软件升级和修复</p> <p>该升级方式需要连接到Console接口，断电重启。启动过程中根据提示按<Ctrl+B>进入BootWare菜单，通过BootWare来重新加载软件包，具体操作请参见产品随软件发布的版本说明书</p>



说明

本章仅涉及如何通过命令行的 Boot-Loader 方式进行软件升级。

1.1.4 设备软件升级

1. 启动软件包

在进行软件升级时，用户需要将升级软件包指定为启动软件包，作为设备下次启动时加载的软件包。在升级时，用户可为设备指定主用启动软件包和备用启动软件包。加载软件包时，系统会优先选择主用软件包。只有当主用软件包不可用时，才会选择备用软件包。

2. 启动软件包加载过程

设备加载并初始化 BootWare 之后，会按如下流程来选择加载的启动软件包，进入 Comware 系统：

- (1) 优先加载主用软件包。
- (2) 如果任何指定的主用软件包不存在或不可用，尝试加载备用软件包。
- (3) 如果任何指定的备用软件包不可用，设备加载失败，无法正常启动。

1.2 软件升级限制和指导

如果将可插拔存储介质内的软件包指定为设备下次启动时使用的软件包，重启设备时不要将可插拔存储介质从设备上拔出，否则可能导致设备无法正常启动。建议将固定存储介质中的软件包指定为设备下次启动时使用的软件包。

1.3 通过Boot-Loader方式升级设备软件

1.3.1 升级任务简介

(1) 升级整机

a. (可选) [加载BootWare程序](#)

预先加载 **BootWare** 程序能缩短后续软件包升级的时间，减小升级过程中断电引起的升级失败。如果未执行本步骤，那么设备在升级 **Boot** 包时会自动升级 **BootWare** 程序。

b. [指定新的启动软件包并完成升级](#)

(2) (可选) [将IRF主设备的当前软件包同步到从设备](#)

IRF从设备的软件与IRF主设备的软件不一致时，可通过本任务将IRF主设备的启动软件包同步到IRF从设备。

1.3.2 升级准备

升级设备软件前，请进行如下操作：

- (1) 使用 **display version** 命令查看设备当前运行的 **BootWare** 程序以及启动软件的版本。
- (2) 获取新软件的版本发布说明书，了解新软件的版本号、软件大小以及和当前运行的 **BootWare** 程序以及 **Comware** 软件的兼容性。
- (3) 使用 **dir** 命令查看存储介质是否有足够的空间存储新的软件。如果存储空间不足，可使用 **delete** 命令删除一些暂时不用的文件。关于 **dir** 和 **delete** 命令的详细描述请参见“基础配置命令参考”中的“文件系统管理”。
在IRF中，请保证所有成员设备上都有足够的存储空间。
- (4) 使用 **FTP**、**TFTP** 方式将新软件包下载到任一文件系统的根目录下。**FTP**、**TFTP** 和文件系统管理的具体配置和介绍请参见“基础配置指导”中的“**FTP** 和 **TFTP**”和“文件系统管理”。

1.3.3 加载BootWare程序

请在用户视图下执行以下操作。

(1) 加载新的 **BootWare** 程序。

```
bootrom update file file slot slot-number-list
```

执行本命令后，系统会将文件系统中的 **BootWare** 程序加载到 **BootWare** 的 **Normal** 区。

要使新的 **BootWare** 程序生效，需要重启设备。

1.3.4 指定新的启动软件包并完成升级

请在用户视图下执行以下操作。

- (1) 为所有成员设备指定启动软件包。请选择其中一项进行配置。

- o **boot-loader file** *ipe-filename* [**patch filename**&<1-16>] { **all** | **slot slot-number** } { **backup** | **main** }
- o **boot-loader file boot filename system filename** [**feature filename**&<1-30>] [**patch filename**&<1-16>] { **all** | **slot slot-number** } { **backup** | **main** }

对于有多台成员设备组成的 IRF 系统中，建议使用 **all** 参数升级软件包，逐一升级 **slot** 会导致升级期间 **slot** 之间的版本不一致。

- (2) 保存当前配置。

save

- (3) 重启设备。

reboot

- (4) （可选）可选检查升级后的软件版本。

display version

确认当前的软件版本为升级后的版本。

1.3.5 将IRF主设备的当前软件包同步到从设备

1. 功能简介

当从设备和主设备的下次启动软件版本不一致时，需要刷新从设备的软件版本，使其软件版本和主设备当前运行的软件版本保持一致。

在进行软件同步时，系统会进行如下处理：

- 如果主设备是使用主用启动软件包启动的，则将其主用下次启动软件包拷贝到从设备的对应目录下，并设置为从设备的主用启动软件包。如果这些软件包中有任一软件包不存在或者不可用，则命令执行失败。
- 如果主设备是使用备用启动软件包列表启动的，则将其备用下次启动软件包列表中的软件包拷贝到从设备的对应目录下，并设置为从设备的主用下次启动软件包。如果这些软件包中有任一软件包不存在或者不可用，则命令执行失败。

2. 升级限制和指导

如果主设备刚安装了补丁，在执行本命令前，请执行 **install commit** 命令刷新主设备的主用启动软件包列表。否则，可能导致备设备升级后与主设备的版本不一致。

3. 升级步骤

请在用户视图下执行以下操作。

- (1) 指定需要同步主设备的从设备。

boot-loader update { **all** | **slot slot-number** }

- (2) 重启涉及同步的从设备。

reboot slot slot-number [**force**]

1.4 通过Feature包或补丁包方式升级启动软件

1.4.1 安装Feature包或补丁包

1. 配置限制和指导

安装补丁包前，需进行如下判断：

- 如果当前设备上未安装补丁包，那么直接安装补丁包。
- 如果当前设备上已安装补丁包，则需查看版本说明书，对比新旧补丁包之间的功能差异：
 - 若新版本的补丁包中包含旧版本补丁包中的所有功能，且在安装完新版本的补丁包后旧版本的补丁包还存在，为了清理存储空间，可以手工卸载并删除旧版本的补丁包，不会影响设备的运行。
 - 若新版本的补丁包中不包含或不完全包含旧版本补丁包中的所有功能，请不要对旧版本的补丁包进行卸载和删除操作。

安装 Feature 包或补丁包过程中，不要对设备进行重启或进行主设备与从设备倒换等操作，否则可能导致安装失败。

安装 Feature 包完成后请重新登录设备，才能使用新 Feature 包内的命令。

2. 配置步骤

(1) 下载 Feature 包或补丁包。

使用 FTP、TFTP 方式将 Feature 包或补丁包下载到主设备缺省文件系统的根目录下。

从设备上无需逐一下载 Feature 包或补丁包，为从设备安装 Feature 包或补丁包时，系统会自动将主设备上的 Feature 包或补丁包拷贝并安装到从设备。

FTP 及 TFTP 具体配置请参见“基础配置指导”中的“FTP 及 TFTP”。

(2) 激活 Feature 包或补丁包。

- **install activate feature filename**<1-30> **slot slot-number**
- **install activate patch filename { all | slot slot-number }**

指定 **all** 参数表示同时激活所有硬件上的补丁包，此时无需执行 **install commit** 命令，所有补丁包在设备重启后继续生效。

(3) 确认 Feature 包或补丁包更改。

install commit

激活 Feature 包或补丁包以后，Feature 包或补丁包仅对设备本次启动生效，设备重启后这些 Feature 包或补丁包不再有效。用户只有确认 Feature 包或补丁包更改后，才能使此次激活的 Feature 包或补丁包在系统重启后仍然有效。

1.4.2 卸载Feature包或补丁包

1. 配置限制和指导

卸载 Feature 包完成后请重新登录设备，Feature 包内的命令才会被清除。

2. 配置步骤

(1) 卸载 Feature 包或补丁包。

- **install deactivate feature filename**<1-30> **slot slot-number**

- `install deactivate patch filename { all | slot slot-number }`

指定 **all** 参数表示同时卸载所有硬件上的补丁包，此时无需执行 **install commit** 命令，所有补丁包在设备重启后不再生效。

卸载 **Feature** 包或补丁包只能使 **Feature** 包或补丁包不再运行，但 **Feature** 包或补丁包依旧保存在设备的缺省文件系统中。

(2) 确认补丁包更改。

install commit

卸载 **Feature** 包或补丁包以后，**Feature** 包或补丁包仅从当前启动软件包列表中删除，设备重启后这些 **Feature** 包或补丁包继续生效。用户只有确认 **Feature** 包或补丁包更改后，才能使此次删除的 **Feature** 包或补丁包在系统重启后不再生效。

1.5 软件升级显示和维护

在完成上述配置后，可在任意视图下执行 **display** 命令，通过查看显示信息验证配置的效果。

表1-2 软件升级显示和维护

操作	命令
显示本次启动和下次启动所采用的启动软件包的名称	display boot-loader [slot slot-number]

1.6 软件升级典型配置举例

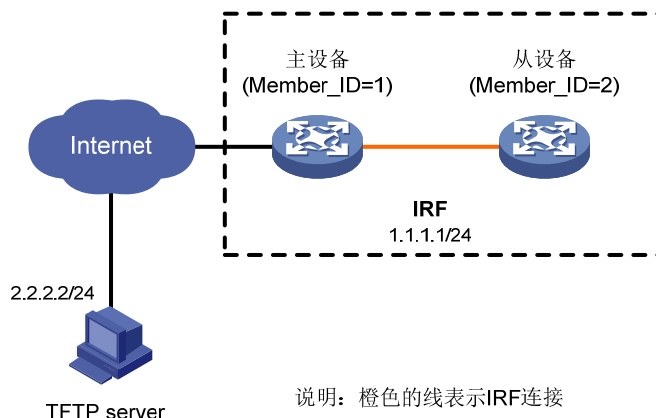
1.6.1 通过重启方式升级启动软件包配置举例

1. 配置需求

- IRF 由两个成员设备组成：主设备的成员编号为 1，从设备的成员编号为 2。
- 现要求对设备启动软件包进行升级，使设备使用新的启动软件包运行。

2. 组网图

图1-1 通过重启方式升级启动软件包配置举例组网图



3. 配置步骤



说明

- 本举例只给出配置步骤和涉及的命令，关于命令的提示信息，请以设备的实际情况为准。
 - 为了保险起见，在配置主用下次启动软件包/IPE 文件时，建议将主用下次启动软件包/IPE 文件进行备份，再将备份文件设置为备用下次启动软件包/IPE 文件。如果 Flash 上存储空间有限，可以不备份。
-

配置 IP 地址以及路由，确保 IRF 和 TFTP server 之间路由可达。配置步骤略。

查看设备当前使用的启动软件包的版本。

```
<Sysname> display version
```

复制设备当前使用的启动软件包。

```
<Sysname> copy boot.bin boot_backup.bin
```

```
<Sysname> copy system.bin system_backup.bin
```

指定主设备和从设备下次启动时使用的备用软件包为 **boot_backup.bin/system_backup.bin**。

```
<Sysname> boot-loader file boot flash:/boot_backup.bin system flash:/system_backup.bin slot 1 backup
```

```
<Sysname> boot-loader file boot flash:/boot_backup.bin system flash:/system_backup.bin slot 2 backup
```

将待升级的 IPE 文件 **startup-a2105.ipe** 从 TFTP server 下载到主设备 Flash 的根目录下。

```
<Sysname> tftp 2.2.2.2 get startup-a2105.ipe
```

指定主设备和从设备下次启动时使用 **startup-a2105.ipe** 作为主用 IPE 文件。

```
<Sysname> boot-loader file flash:/startup-a2105.ipe slot 1 main
```

```
<Sysname> boot-loader file flash:/startup-a2105.ipe slot 2 main
```

查看主用、备用下次启动 IPE 文件是否配置成功。

```
<Sysname> display boot-loader
```

重启所有成员设备，以便运行新的启动软件包完成升级。

```
<Sysname> reboot
```

4. 验证配置

设备重启后，查看 IRF 使用的启动软件包的版本。

```
<Sysname> display version
```

目 录

1 设备管理.....	1-1
1.1 设备管理任务简介.....	1-1
1.2 配置设备名称.....	1-1
1.3 配置系统时间.....	1-2
1.3.1 功能简介.....	1-2
1.3.2 配置限制和指导.....	1-2
1.3.3 配置任务简介.....	1-2
1.3.4 通过命令行配置系统时间.....	1-2
1.3.5 通过网络协议获取UTC时间.....	1-3
1.3.6 配置时区.....	1-3
1.3.7 配置夏令时.....	1-3
1.4 开启版权信息显示功能.....	1-3
1.5 配置欢迎信息.....	1-4
1.6 配置密码恢复功能.....	1-5
1.7 配置端口状态检测定时器.....	1-6
1.8 监控CPU利用率.....	1-6
1.9 配置内存告警门限.....	1-8
1.10 配置温度告警门限.....	1-9
1.11 配置断电通知功能.....	1-10
1.12 可插拔接口模块的识别与诊断.....	1-10
1.12.1 识别可插拔接口模块.....	1-10
1.12.2 诊断可插拔接口模块.....	1-11
1.13 配置定时执行任务功能.....	1-11
1.13.1 功能简介.....	1-11
1.13.2 配置限制和指导.....	1-11
1.13.3 配置步骤.....	1-12
1.13.4 定时执行任务典型配置举例.....	1-13
1.14 重启设备.....	1-16
1.14.1 功能简介.....	1-16
1.14.2 配置限制和指导.....	1-16
1.14.3 通过reboot命令行立即重启设备.....	1-16
1.14.4 通过scheduler reboot定时重启设备.....	1-17
1.15 恢复出厂状态.....	1-17

1.16 设备管理显示和维护	1-18
----------------------	------

1 设备管理

通过设备管理功能，用户能够查看设备当前的工作状态，配置设备运行的相关参数，实现对设备的日常维护和管理。

1.1 设备管理任务简介

设备管理的所有配置任务均为可选配置，配置时无先后顺序要求，请根据实际需要选择配置。设备管理配置任务如下：

- 配置设备的基本参数
 - [配置设备名称](#)
 - [配置系统时间](#)
 - [开启版权信息显示功能](#)
 - [配置欢迎信息](#)
- [配置密码恢复功能](#)
- [配置端口状态检测定时器](#)
- 监控设备
 - [监控CPU利用率](#)
 - [配置内存告警门限](#)
 - [配置温度告警门限](#)
- 管理设备上的资源
 - [配置断电通知功能](#)
 - [可插拔接口模块的识别与诊断](#)
- 维护设备
 - [配置定时执行任务功能](#)
 - [重启设备](#)
 - [恢复出厂状态](#)

1.2 配置设备名称

1. 功能简介

设备名称用于在网络中标识某台设备，在系统内部，设备名称对应于命令行接口的提示符，如设备的名称为 Sysname，则用户视图的提示符为<Sysname>。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 配置设备名称。

```
sysname sysname
```

缺省情况下，设备的名称为 H3C。

1.3 配置系统时间

1.3.1 功能简介

为了保证与其它设备协调工作，为了更好的监控和维护设备，请确保设备的系统时间是准确的。设备可通过以下方式获取系统时间：

- 命令行配置。用户通过命令行指定系统时间后，设备会使用内部晶体振荡器产生的时钟信号继续计时。
- 网络时钟同步。设备周期性的同步 NTP 服务器的 UTC（Coordinated Universal Time，国际协调时间）时间，并用同步得到的 UTC 时间和设备上配置的本地时区、夏令时参数运算，得出当前的系统时间。关于 NTP 的详细介绍，请参见“网络管理和监控配置指导”中的“NTP”。

从网络时钟源获取的时间比命令行配置的时间更精准，推荐使用。

1.3.2 配置限制和指导

通过命令行配置系统时间时，不管当前是否已经配置夏令时和时区，**clock datetime** 命令中指定的时间即为当前的系统时间。

设备通过命令行配置或者网络同步获取到系统时间后，如果再修改夏令时或者时区，设备会用修改后的夏令时和时区重新计算系统时间，计算后得到的系统时间可通过 **display clock** 命令查看。

1.3.3 配置任务简介

系统时间的配置任务如下：

- (1) 配置系统时间的获取方式。请选择其中一项进行配置。
 - [通过命令行配置系统时间](#)
 - [通过网络协议获取UTC时间](#)
- (2) （可选）[配置时区](#)
请将所有网络设备的时区和当地地理时区保持一致。
- (3) （可选）[配置夏令时](#)
请将所有网络设备的夏令时和当地夏令时保持一致。

1.3.4 通过命令行配置系统时间

- (1) 进入系统视图。

system-view

- (2) 通过命令行配置系统时间。

clock protocol none

缺省情况下，通过 NTP 协议获取时间。

多次执行 **clock protocol** 命令，最后一次执行的命令生效，可能会导致系统时间被修改。

- (3) 返回用户视图。

quit

- (4) 配置系统时间。

clock datetime *time date*

设备的系统时间为 UTC 时间 2013 年 1 月 1 日零点。

1.3.5 通过网络协议获取UTC时间

- (1) 进入系统视图。

system-view

- (2) 通过网络协议获取 UTC 时间。

clock protocol ntp

缺省情况下，通过 NTP 协议获取时间。

多次执行 **clock protocol** 命令，最后一次执行的命令生效，可能会导致系统时间被修改。

- (3) 配置 NTP 的相关参数。关于 NTP 的配置，请参见“网络管理和监控配置指导”中的“NTP”。

1.3.6 配置时区

- (1) 进入系统视图。

system-view

- (2) 配置系统所在的时区。

clock timezone *zone-name* { **add** | **minus** } *zone-offset*

缺省情况下，系统所在的时区为零时区，即设备采用 UTC 时间。

1.3.7 配置夏令时

- (1) 进入系统视图。

system-view

- (2) 配置夏令时。

clock summer-time *name start-time start-date end-time end-date add-time*

缺省情况下，未配置夏令时。

1.4 开启版权信息显示功能

1. 功能简介

开启版权信息显示功能后，使用 Telnet 或 SSH 方式登录设备时会显示版权信息，使用 Console 口登录设备再退出用户视图时，由于设备会自动再次登录，因此也会显示版权信息，其它情况不显示版权信息。

禁止版权信息显示功能后，在任何情况下都不会显示版权信息。

2. 配置步骤

- (1) 进入系统视图。

system-view

- (2) 开启版权信息显示功能。

copyright-info enable

缺省情况下，版权信息显示功能处于开启状态。

1.5 配置欢迎信息

1. 功能简介

欢迎信息是用户在连接到设备后、进入 CLI 配置界面时系统显示的一段提示信息。管理员可以根据需要，配置欢迎信息。

系统支持如下几种欢迎信息：

- **legal** 欢迎信息。系统在用户登录前会给出一些版权或者授权信息，然后显示 **legal** 条幅，并等待用户确认是否继续登录。如果用户输入“Y”或者按<Enter>键，则继续登录过程；如果输入“N”，则断开连接，退出登录过程。“Y”和“N”不区分大小写。
- **MOTD**（Message Of The Day，每日提示）欢迎信息。
- **login** 欢迎信息。只有用户界面下配置了 **password** 或者 **scheme** 认证方式时，才显示该欢迎信息。
- **shell** 欢迎信息。用户登录进入用户视图时，显示 **shell** 欢迎信息。

以上几种欢迎信息的显示顺序为：**legal** 欢迎信息、**MOTD** 欢迎信息、**login** 欢迎信息或 **shell** 欢迎信息。

2. 欢迎信息输入方式

欢迎信息可以单行或多行输入。

- 单行输入

该方式下，命令关键字与欢迎信息的所有内容在同一行中输入，输入内容 *text* 的第一个字符和最后一个字符分别作为起始符和结束符，起始符和结束符可以为任意可见字符但两者必须相同，且不属于欢迎信息的内容。此时包括命令关键字、起始符和结束符在内，一共可以输入 511 个字符。在该方式下输入欢迎信息过程中不能回车（按<Enter>键）。例如，配置 **shell** 欢迎信息为“Have a nice day.”，可参照如下步骤：

```
<System> system-view
[System] header shell %Have a nice day.%
```



说明

单行输入方式配置的欢迎信息本身不能包含换行符。

- 多行输入

该方式下，通过回车键将欢迎信息分多行输入。如果输入的内容中包括换行，则换行算两个字符。多行输入又分三种方式：

- 命令关键字后直接回车，输入欢迎信息并以“%”作为欢迎信息的结束符结束配置，“%”不属于欢迎信息的内容。该方式，不包括起始符但包括结束符在内，一共可以输入 1999 个字符。例如，配置的欢迎信息为“Have a nice day.”，可参照如下步骤：

```
<System> system-view
[System] header shell
```

```
Please input banner content, and quit with the character '%'.
Have a nice day.%
```

- 命令关键字后输入一个字符后回车，以这个字符作为欢迎信息的起始符和结束符，输入完欢迎信息以后，以结束符结束配置。起始符和结束符不属于欢迎信息的内容。该方式，不包括起始符但包括结束符在内，一共可以输入 1999 个字符。例如，配置的欢迎信息为“Have a nice day.”，可参照如下步骤：

```
<System> system-view
[System] header shell A
Please input banner content, and quit with the character 'A'.
Have a nice day.A
```

- 命令关键字后输入多个字符（首尾不相同）后回车，以命令关键字后的第一个字符作为欢迎信息的起始符和结束符，输入完欢迎信息以后，以结束符结束配置。起始符和结束符不属于欢迎信息的内容。该方式，包括起始符和结束符在内，一共可以输入 2002 个字符。例如，配置的欢迎信息为“Have a nice day.”，可参照如下步骤：

```
<System> system-view
[System] header shell AHave a nice day.
Please input banner content, and quit with the character 'A'.
A
```



说明

多行输入方式配置的欢迎信息本身可以包含换行符。配置欢迎信息内容时键入的回车，即对应最终显示的欢迎信息中的换行。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 配置欢迎信息。请至少选择其中一项进行配置。

- 配置 legal 欢迎信息。

```
header legal text
```

- 配置 MOTD 欢迎信息。

```
header motd text
```

- 配置 login 欢迎信息。

```
header login text
```

- 配置 shell 欢迎信息。

```
header shell text
```

1.6 配置密码恢复功能

1. 功能简介

使能密码恢复功能后，当用户忘记 Console 口认证密码或者登录认证失败，导致无法使用 Console 口登录设备时，可通过 Console 口连接设备，硬件重启设备，并在启动过程中根据提示按<Ctrl+B>

进入 **BootWare** 菜单，再选择对应的 **BootWare** 菜单选项来修复这个问题。关闭密码恢复功能后，设备将处于一个安全性更高的状态，即当出现上述情况时，若想继续使用 **Console** 口登录设备，只能通过 **BootWare** 菜单选择将设备恢复为出厂配置之后方可继续操作，这样可以有效地防止非法用户获取启动配置文件。

BootWare 菜单的详细描述，请参见产品的版本说明书。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 使能密码恢复功能。

```
password-recovery enable
```

缺省情况下，密码恢复功能处于使能状态。

1.7 配置端口状态检测定时器

1. 功能简介

某些协议模块（比如 **STP**、**DLDP** 等）在特定情况下会自动关闭某个端口。此时，可以配置一个端口状态检测定时器。当定时器超时，如果该端口仍处于关闭状态，则协议模块会自动取消关闭动作，使端口恢复到真实的物理状态。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 配置端口状态检测定时器的时长。

```
shutdown-interval time
```

缺省情况下，端口状态检测定时器时长为 30 秒。

1.8 监控CPU利用率

1. 功能简介

- CPU 告警功能

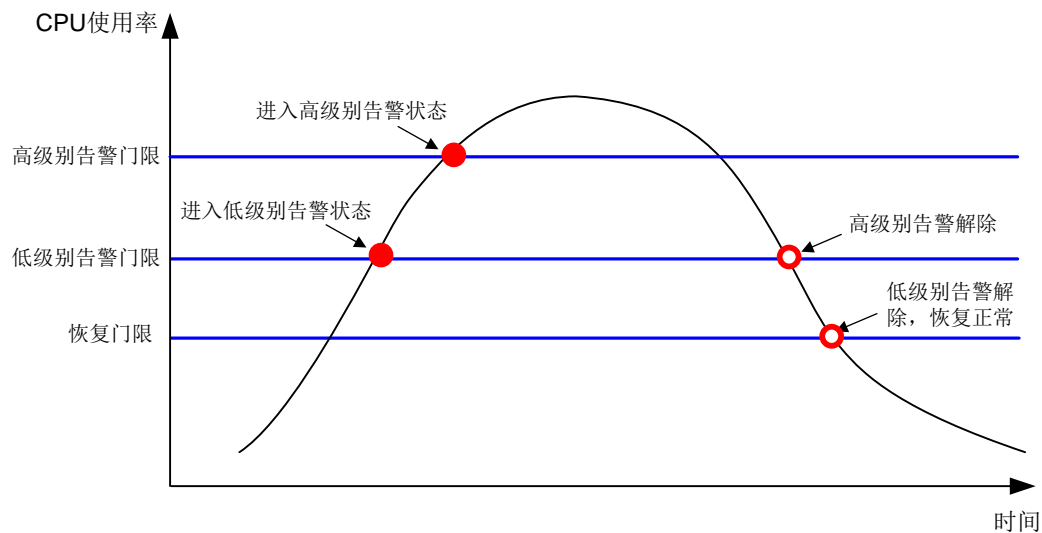
系统每隔 1 分钟会对 **CPU** 的利用率进行采样，并将采样值和用户配置的 **CPU** 利用率告警门限比较。

- 当采样值大于低级别告警门限时，则 **CPU** 进入低级别告警状态，会周期发送 **CPU** 低级别告警通知，直到 **CPU** 进入高级别告警状态或者低级别告警状态解除。
- 当采样值大于高级别告警门限时，则 **CPU** 进入高级别告警状态，会周期发送 **CPU** 高级别告警通知，直到高级别告警状态解除。
- 当采样值回落，小于 **CPU** 利用率恢复门限时，则认为 **CPU** 利用率已经恢复到正常范围，并发送恢复告警通知。

CPU 告警通知会同时向 **NETCONF**、**SNMP**、信息中心三个方向输出，通过配置 **NETCONF**、**SNMP**、信息中心功能，**CPU** 告警最终能以 **NETCONF** 事件、**SNMP** Trap 或 Inform 消息、

日志的形式发送给用户。NETCONF、SNMP、信息中心的详细介绍请参见“网络管理和监控配置指导”中的“NETCONF”、“SNMP”、“信息中心”。

CPU 告警示意图



- CPU 利用率历史记录功能

开启 CPU 利用率历史记录功能后，系统会每隔一定时间（可通过 `monitor cpu-usage interval` 命令配置）对 CPU 的利用率进行采样，并把采样结果保存到历史记录区。这些记录可通过 `display cpu-usage history` 命令查看，以使用户监控设备近期的运行情况。

2. 配置步骤

(1) 进入系统视图。

```
system-view
```

(2) 配置 CPU 利用率阈值。

```
monitor cpu-usage threshold severe-threshold minor-threshold  
minor-threshold recovery-threshold recovery-threshold [ slot  
slot-number [ cpu cpu-number ] ]
```

缺省情况下，CPU 利用率高级别告警门限为 99%，低级别告警门限为 98%，恢复门限为 50%。

(3) 配置发送 CPU 告警事件的间隔。

```
monitor resend cpu-usage { minor-interval minor-interval |  
severe-interval severe-interval } * [ slot slot-number [ cpu  
cpu-number ] ]
```

缺省情况下，持续 300 秒超过低级别告警门限则上报一次 CPU 低级别告警事件，持续 60 秒超过高级别告警门限则上报一次 CPU 高级别告警事件。

(4) 配置 CPU 利用率历史记录采样周期。

```
monitor cpu-usage interval interval [ slot slot-number [ cpu  
cpu-number ] ]
```

缺省情况下，CPU 使用率历史记录采样周期为 1 分钟。

(5) 开启 CPU 利用率历史记录功能。

```
monitor cpu-usage enable [ slot slot-number [ cpu cpu-number ] ]
```

缺省情况下，CPU 使用率历史记录功能处于开启状态。

1.9 配置内存告警门限

1. 功能简介

系统实时监控系统剩余空闲内存大小，当条件达到一级、二级、三级告警门限或者恢复正常状态门限时，就产生相应的告警/告警解除通知，通知关联的业务模块/进程采取相应的措施，以便最大限度的利用内存，又能保证设备的正常运行。

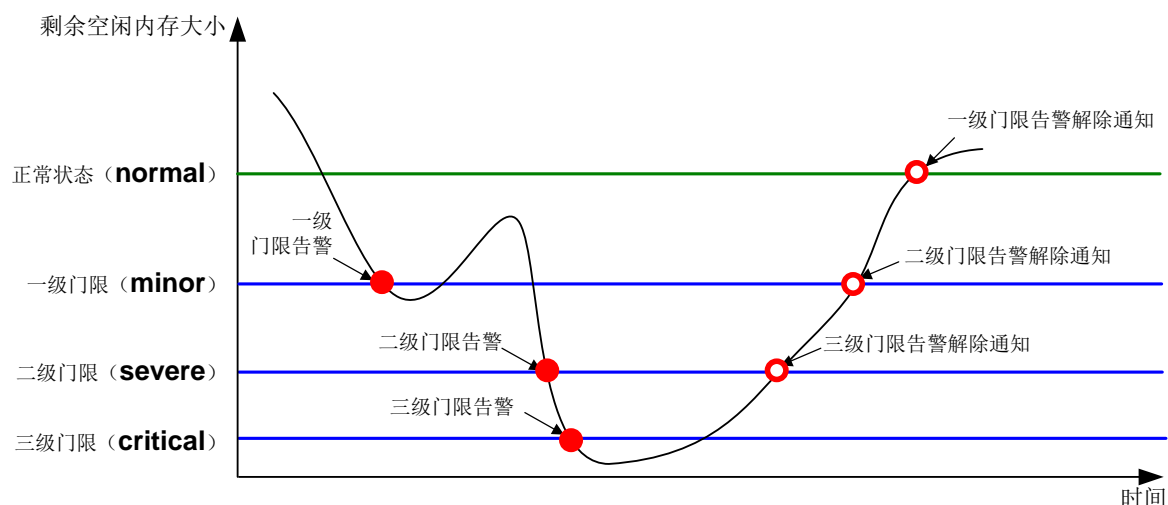
一级 (**minor**)、二级 (**severe**) 和三级 (**critical**) 门限，对应的系统剩余空闲内存越来越少，紧急程度越来越严重。

- 当系统剩余空闲内存第一次小于等于一级告警门限时，产生一级告警；
- 当系统剩余空闲内存第一次小于等于二级告警门限时，产生二级告警；
- 当系统剩余空闲内存第一次小于等于三级告警门限时，产生三级告警；
- 当系统剩余空闲内存大于等于二级告警门限时，产生三级告警解除通知；
- 当系统剩余空闲内存大于等于一级告警门限时，产生二级告警解除通知；
- 当系统剩余空闲内存大于等于正常内存大小时，产生一级告警解除通知；

同一级别的告警/告警解除通知是交替进行的：当系统剩余空闲内存小于等于某级告警门限，设备产生相应级别的告警，后续只有该告警解除了，系统剩余空闲内存再次小于等于某级告警门限时，才会再次生成该级别的告警。

当系统的剩余空闲内存大小如 [图 1-1](#) 中曲线所示时，会生成如 [图 1-1](#) 所示的告警和解除告警通知。

图1-1 内存告警示意图



2. 配置步骤

(1) 进入系统视图。

```
system-view
```

- (2) 配置内存利用率阈值。

```
memory-threshold [ slot slot-number [ cpu cpu-number ] ] usage  
memory-threshold
```

缺省情况下，内存利用率阈值为 100%。

- (3) 配置空闲内存告警的门限值。

```
memory-threshold [ slot slot-number [ cpu cpu-number ] ] [ ratio ] minor  
minor-value severe severe-value critical critical-value normal  
normal-value
```

缺省情况下，一级告警门限为 60MB，二级告警门限为 56MB，三级告警门限为 52MB，系统恢复到正常的内存门限为 64MB。

- (4) 配置发送内存告警事件的间隔。

```
monitor resend memory-threshold { critical-interval critical-interval  
| minor-interval minor-interval | severe-interval severe-interval } *  
[ slot slot-number [ cpu cpu-number ] ]
```

缺省情况下，持续 12 小时超过一级告警门限则上报一次一级告警事件通知，持续 3 小时超过二级告警门限则上报一次二级告警事件通知，持续 1 小时超过三级告警门限则上报一次三级告警事件通知。

1.10 配置温度告警门限

1. 功能简介

通过以下配置任务，用户可以根据实际应用的需要配置不同的温度告警门限，来监控设备上不同位置温度传感器的温度。

设备可配置的温度告警门限包括：低温告警门限、一般级（Warning）高温告警门限、严重级（Alarm）高温告警门限。

如果温度低于低温告警门限、高于一般级或严重级高温门限，系统均会生成相应的日志信息和告警信息提示用户，并通过设备面板上的指示灯来告警，以便用户及时进行处理。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 配置设备的温度告警门限。

```
temperature-limit slot slot-number hotspot sensor-number lowlimit  
warninglimit [ alarmlimit ]
```

不同温度传感器的温度门限可能不同，请先使用 **undo temperature-limit** 命令恢复缺省情况后，再通过 **display environment** 命令查看设备的缺省温度告警门限。

高温告警门限必须大于低温告警门限；Alarm 高温告警门限必须大于 Warning 高温告警门限。

1.11 配置断电通知功能

1. 功能简介

配置该功能后，如果设备断电，设备会利用余电立即以 SNMP Trap 和（或）日志的形式给目的主机发送断电告警、日志，来告知设备已掉电。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 配置发送断电告警/日志的源接口。

```
dying-gasp source interface-type interface-number
```

缺省情况下，未配置发送断电告警/日志的源接口。在 IPv4 网络中，设备将使用报文出接口的主 IPv4 地址作为发送断电告警/日志报文的源 IP 地址；在 IPv6 网络中，设备自动选择断电告警/日志报文的源 IPv6 地址，具体选择原则请参见 RFC 3484。

- (3) 配置接收断电告警的目的主机的参数。

```
dying-gasp host { ip-address | ipv6 ipv6-address } snmp-trap version { v1  
| v2c } securityname security-string
```

缺省情况下，未配置接收断电告警的目的主机的参数。

多次配置该命令可指定多个目的主机，使得设备可以向多个主机发送断电告警信息。

- (4) 配置接收断电日志的目的主机的参数。

```
dying-gasp host { ip-address | ipv6 ipv6-address } syslog
```

缺省情况下，未配置接收断电日志的目的主机的参数。

多次配置该命令可指定多个目的主机，使得设备可以向多个主机发送断电日志信息。

1.12 可插拔接口模块的识别与诊断

1.12.1 识别可插拔接口模块

1. 功能简介

可以通过显示可插拔接口模块的主要特征参数或者电子标签信息来识别可插拔接口模块。

- 可插拔接口模块的主要特征参数包括：模块型号、连接器类型、发送激光的中心波长、信号的有效传输距离、模块生产厂商名称等信息。
- 电子标签信息也可以称为永久配置数据或档案信息，在光模块或者设备的调试、测试过程中被写入到光模块或者设备的存储器件中，包括光模块或者设备的名称、生产序列号、MAC 地址、制造商等信息。

另外，当设备上插入的光模块的生产厂商不是 H3C 时，设备会打印 Log 信息提醒用户，要求用户更换成 H3C 的光模块，以便管理和维护光模块。关于 Log 输出规则的配置请参见“网络管理和监控配置指导”中的“信息中心”。

2. 配置步骤

请在任意视图下执行以下命令。

- 显示可插拔接口模块的主要特征参数。

```
display transceiver interface [ interface-type interface-number ]
```

- 显示可插拔接口模块的电子标签信息。

```
display transceiver manuinfo interface [ interface-type  
interface-number ]
```

1.12.2 诊断可插拔接口模块

1. 功能简介

系统提供故障告警信息描述了可插拔接口模块的故障来源，以使用户诊断和解决故障。系统还提供了数字诊断功能，其原理是对影响光模块工作的关键参数进行监控（这些关键参数包括：温度、电压、激光偏置电流、发送光功率和接收光功率等），当这些参数的值异常时，用户可以采取相应的措施，预防故障发生。

2. 配置步骤

请在任意视图下执行以下命令。

- 显示可插拔接口模块的当前故障告警信息。

```
display transceiver alarm interface [ interface-type interface-number ]
```

- 显示可插拔光模块的数字诊断参数的当前测量值。

```
display transceiver diagnosis interface [ interface-type  
interface-number ]
```

1.13 配置定时执行任务功能

1.13.1 功能简介

通过配置定时执行任务功能可以让设备在指定时刻或延迟指定时间后，自动执行指定命令，使设备能够在无人值守的情况下完成某些配置。该功能不但增强了设备的自动控制和管理能力，提高了易用性，而且可以起到有效节能的作用。

定时执行任务有两种类型：一次性执行方式和循环执行方式。两种方式都支持在同一任务中执行多条命令。一次性执行的配置任务不能保存到配置文件，设备重启后该任务将取消。循环执行的配置任务能保存到配置文件，等下次时间到达，任务将自动执行。

1.13.2 配置限制和指导

- 设备重启后，系统时间会恢复到出厂配置。请重新配置系统时间，或者配置 NTP 功能，保证设备能够获得准确的时间，以便配置的定时执行任务能够在期望的时间点执行。NTP 的配置请参见“网络管理和监控配置指导”中的“NTP”。
- 通过 **command** 分配的命令行必须是设备上可成功执行的命令行，但不能包括 **telnet**、**ftp**、**ssh2** 和 **monitor process**。由用户保证配置的正确性，否则，命令行不能自动被执行。
- 如果需要分配的命令（假设为 A）是用户视图下的命令，则直接使用 **command** 命令分配即可，比如：**command 1 display interface**；如果需要分配的命令（假设为 A）是非用户视图下的命令，则必须先分配进入 A 所在视图的命令（指定较小的 *id* 值），再分配 A。比如：要使用

Job 定时执行 **shutdown** 命令，则需执行三次 **command** 命令，分别分配 **system-view**、**interface**、**shutdown** 命令，且各 **command** 命令的 *id* 值逐渐增大。

- 定时执行任务时，设备不会与用户交互信息。当需要用户交互确认时，系统将自动输入 “Y” 或 “Yes”；当需要用户交互输入字符信息时，系统将自动输入缺省字符串，没有缺省字符串的将自动输入空字符串。
- 系统将在后台定时执行任务，不显示任何输出信息（log、trap、debug 等系统信息除外）。

1.13.3 配置步骤

- (1) 进入系统视图。

system-view

- (2) 创建 Job。

scheduler job *job-name*

- (3) 为 Job 分配命令。

command *id* *command*

缺省情况下，没有为 Job 分配命令。

多次执行该命令可以为 Job 分配多条命令，命令的执行顺序由 *id* 参数的大小决定，数值小的先执行。

- (4) 退回系统视图。

quit

- (5) 创建 Schedule。

scheduler schedule *schedule-name*

- (6) 为 Schedule 分配 Job。

job *job-name*

缺省情况下，没有为 Schedule 分配 Job。

多次执行该命令可以为 Schedule 分配多个 Job，各个 Job 之间并发执行。

- (7) 配置执行 Schedule 的定时任务时使用的用户角色。

user-role *role-name*

缺省情况下，Schedule 执行定时任务时使用的用户角色，为创建该 Schedule 的用户的用户角色。

多次执行本命令可给 Schedule 配置多个用户角色，系统会使用这些用户角色权限的并集去执行 Schedule。

- (8) 配置执行 Schedule 的时间。请选择其中一项进行配置。

- 配置在指定时刻执行 Schedule。

time at *time date*

time once at *time* [**month-date** *month-day* | **week-day** *week-day*&<1-7>]

- 配置延迟执行 Schedule 的时间。

time once delay *time*

- 为 Schedule 配置循环执行时间。

```
time repeating at time [ month-date [ month-day | last ] | week-day  
week-day&<1-7> ]
```

- 为 Schedule 配置循环执行周期。

```
time repeating [ at time [date ] ] interval interval
```

缺省情况下，没有为 Schedule 配置执行时间。

一个 Schedule 只能配置一个时间，最后一次执行的命令生效。

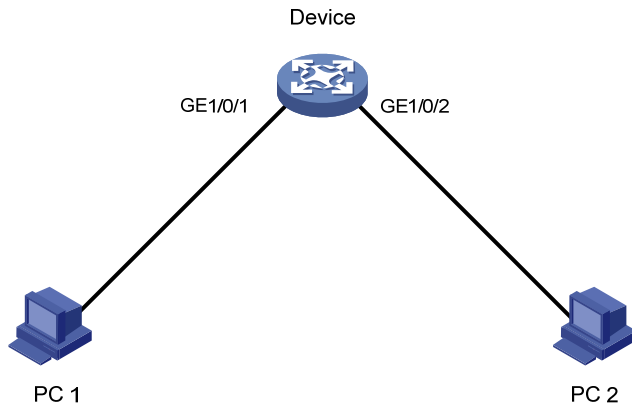
1.13.4 定时执行任务典型配置举例

1. 组网需求

对 Device 进行配置，在星期一到星期五的上午八点到下午十八点开启 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2，其它时间关闭端口，以便起到有效节能的作用。

2. 组网图

图1-2 定时执行任务典型配置举例组网图



3. 配置步骤

进入系统视图。

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

创建关闭 GigabitEthernet1/0/1 的 Job。

```
[Sysname] scheduler job shutdown-GigabitEthernet1/0/1
```

```
[Sysname-job-shutdown-GigabitEthernet1/0/1] command 1 system-view
```

```
[Sysname-job-shutdown-GigabitEthernet1/0/1] command 2 interface gigabitethernet 1/0/1
```

```
[Sysname-job-shutdown-GigabitEthernet1/0/1] command 3 shutdown
```

```
[Sysname-job-shutdown-GigabitEthernet1/0/1] quit
```

创建开启 GigabitEthernet1/0/1 的 Job。

```
[Sysname] scheduler job start-GigabitEthernet1/0/1
```

```
[Sysname-job-start-GigabitEthernet1/0/1] command 1 system-view
```

```
[Sysname-job-start-GigabitEthernet1/0/1] command 2 interface gigabitethernet 1/0/1
```

```
[Sysname-job-start-GigabitEthernet1/0/1] command 3 undo shutdown
```

```
[Sysname-job-start-GigabitEthernet1/0/1] quit
```

创建关闭 GigabitEthernet1/0/2 的 Job。

```
[Sysname] scheduler job shutdown-GigabitEthernet1/0/2
```

```
[Sysname-job-shutdown-GigabitEthernet1/0/2] command 1 system-view
[Sysname-job-shutdown-GigabitEthernet1/0/2] command 2 interface gigabitethernet 1/0/2
[Sysname-job-shutdown-GigabitEthernet1/0/2] command 3 shutdown
[Sysname-job-shutdown-GigabitEthernet1/0/2] quit
```

创建开启 GigabitEthernet1/0/2 的 Job。

```
[Sysname] scheduler job start-GigabitEthernet1/0/2
[Sysname-job-start-GigabitEthernet1/0/2] command 1 system-view
[Sysname-job-start-GigabitEthernet1/0/2] command 2 interface gigabitethernet 1/0/2
[Sysname-job-start-GigabitEthernet1/0/2] command 3 undo shutdown
[Sysname-job-start-GigabitEthernet1/0/2] quit
```

配置定时执行任务，使 Device 在星期一到星期五的上午八点开启 pc1、pc2 对应的以太网端口。

```
[Sysname] scheduler schedule START-pc1/pc2
[Sysname-schedule-START-pc1/pc2] job start-GigabitEthernet1/0/1
[Sysname-schedule-START-pc1/pc2] job start-GigabitEthernet1/0/2
[Sysname-schedule-START-pc1/pc2] time repeating at 8:00 week-day mon tue wed thu fri
[Sysname-schedule-START-pc1/pc2] quit
```

配置定时执行任务，使 Device 在星期一到星期五的下午十八点关闭 pc1、pc2 对应的以太网端口。

```
[Sysname] scheduler schedule STOP-pc1/pc2
[Sysname-schedule-STOP-pc1/pc2] job shutdown-GigabitEthernet1/0/1
[Sysname-schedule-STOP-pc1/pc2] job shutdown-GigabitEthernet1/0/2
[Sysname-schedule-STOP-pc1/pc2] time repeating at 18:00 week-day mon tue wed thu fri
[Sysname-schedule-STOP-pc1/pc2] quit
```

4. 验证配置

显示 Job 的配置信息。

```
[Sysname] display scheduler job
Job name: shutdown-GigabitEthernet1/0/1
  system-view
  interface gigabitethernet 1/0/1
  shutdown

Job name: shutdown-GigabitEthernet1/0/2
  system-view
  interface gigabitethernet 1/0/2
  shutdown
```

```
Job name: start-GigabitEthernet1/0/1
  system-view
  interface gigabitethernet 1/0/1
  undo shutdown
```

```
Job name: start-GigabitEthernet1/0/2
  system-view
  interface gigabitethernet 1/0/2
  undo shutdown
```

显示定时任务的运行信息。

```
[Sysname] display scheduler schedule
Schedule name      : START-pc1/pc2
```

Schedule type : Run on every Mon Tue Wed Thu Fri at 08:00:00
Start time : Wed Sep 28 08:00:00 2011
Last execution time : Wed Sep 28 08:00:00 2011
Last completion time : Wed Sep 28 08:00:03 2011
Execution counts : 1

```
-----  
Job name                               Last execution status  
start-GigabitEthernet1/0/1           Successful  
start-GigabitEthernet1/0/2           Successful
```

Schedule name : STOP-pc1/pc2
Schedule type : Run on every Mon Tue Wed Thu Fri at 18:00:00
Start time : Wed Sep 28 18:00:00 2011
Last execution time : Wed Sep 28 18:00:00 2011
Last completion time : Wed Sep 28 18:00:01 2011
Execution counts : 1

```
-----  
Job name                               Last execution status  
shutdown-GigabitEthernet1/0/1         Successful  
shutdown-GigabitEthernet1/0/2         Successful
```

显示 Job 运行的输出信息。

[Sysname] display scheduler logfile

Job name : start-GigabitEthernet1/0/1
Schedule name : START-pc1/pc2
Execution time : Wed Sep 28 08:00:00 2011
Completion time : Wed Sep 28 08:00:02 2011

----- Job output -----

```
<Sysname>system-view  
System View: return to User View with Ctrl+Z.  
[Sysname]interface gigabitethernet 1/0/1  
[Sysname-GigabitEthernet1/0/1]undo shutdown
```

Job name : start-GigabitEthernet1/0/2
Schedule name : START-pc1/pc2
Execution time : Wed Sep 28 08:00:00 2011
Completion time : Wed Sep 28 08:00:02 2011

----- Job output -----

```
<Sysname>system-view  
System View: return to User View with Ctrl+Z.  
[Sysname]interface gigabitethernet 1/0/2  
[Sysname-GigabitEthernet1/0/2]undo shutdown
```

Job name : shutdown-GigabitEthernet1/0/1
Schedule name : STOP-pc1/pc2
Execution time : Wed Sep 28 18:00:00 2011
Completion time : Wed Sep 28 18:00:01 2011

----- Job output -----

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



```
System View: return to User View with Ctrl+Z.
```

```
[Sysname]interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1]shutdown
```

```
Job name          : shutdown-GigabitEthernet1/0/2
```

```
Schedule name     : STOP-pc1/pc2
```

```
Execution time    : Wed Sep 28 18:00:00 2011
```

```
Completion time   : Wed Sep 28 18:00:01 2011
```

```
----- Job output -----
```

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

```
System View: return to User View with Ctrl+Z.
```

```
[Sysname]interface gigabitethernet 1/0/2
```

```
[Sysname-GigabitEthernet1/0/2]shutdown
```

1.14 重启设备

1.14.1 功能简介

重启设备的方式有以下几种：

(1) 硬件重启

通过断电后重新上电来重启设备。该方式对设备影响较大，如果对运行中的设备进行强制断电，可能会造成数据丢失。一般情况下，建议不要使用这种方式。

(2) 命令行重启

主要用于远程重启设备，而不需要到设备所在地进行断电/上电重启。设备支持以下配置方式：

- 通过 **reboot** 命令行立即重启设备。
- 通过 **scheduler reboot** 定时重启设备。该方式效果同执行 **reboot** 命令，只是使用该方式用户可以配置时间点，让设备在该时间点自动重启，或者配置一个时延，让设备经过指定时间后自动重启。比“通过 **reboot** 命令行立即重启设备”方式灵活。

1.14.2 配置限制和指导

重新启动会导致业务中断，请谨慎使用。

如果设备在准备重启时，用户正在进行文件操作，为了安全起见，系统将不会执行此次重启操作。

1.14.3 通过reboot命令行立即重启设备

1. 配置准备

请在任意视图下执行以下命令。

(1) 确认是否配置了正确的下次启动配置文件。

```
display startup
```

本命令的详细介绍请参见“基础配置命令参考”中的“配置文件管理”。

(2) 确认是否配置了正确的下次启动文件。

```
display boot-loader
```

如果主用启动文件损坏或者不存在，则不允许通过 **reboot** 命令重启设备。请指定新的主用启动文件后再重启。

本命令的详细介绍请参见“基础配置命令参考”中的“软件升级”。

- (3) 为避免重启后配置丢失，将当前配置保存到下次启动配置文件。

save

请根据需保存当前配置，以免重启后配置丢失。

本命令的详细介绍请参见“基础配置命令参考”中的“配置文件管理”。

2. 配置步骤

请在用户视图下执行以下命令，重启设备。

```
reboot [ slot slot-number ] [ force ]
```

1.14.4 通过scheduler reboot定时重启设备

1. 配置限制和指导

该配置对所有成员设备生效。配置定时重启后，如果发生主设备和从设备倒换，则定时重启配置将自动取消。

当多次执行 **scheduler reboot** 命令，最新的配置生效。

2. 配置步骤

请在用户视图下执行本命令，配置重启设备的具体时间或延迟时间。

- **scheduler reboot at time** [*date*]
- **scheduler reboot delay time**

缺省情况下，未配置设备重启的时间。

1.15 恢复出厂状态

1. 功能简介

当设备使用场景更改，或者设备出现故障时，可以使用本特性将设备恢复到出厂状态，仅保留“.bin”文件。

2. 配置限制和指导

请谨慎使用本特性。

3. 配置步骤

- (1) 请在用户视图下执行本命令，将设备恢复到出厂状态。

```
restore factory-default
```

- (2) 重启设备。

```
reboot
```

执行 **reboot** 命令时，请不要选择保存当前配置，否则，设备将以保存的配置重启。

1.16 设备管理显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后设备的运行情况，通过查看显示信息验证配置的效果。

请在系统视图下执行 **reset version-update-record** 命令，在用户视图下执行 **reset scheduler logfile** 命令。

表1-1 设备管理显示和维护

操作	命令
显示系统当前的时间、日期、本地时区以及夏令时配置	display clock
显示设备的版权信息	display copyright
显示CPU利用率的统计信息	display cpu-usage [summary] [slot <i>slot-number</i> [cpu <i>cpu-number</i> [core { <i>core-number</i> all }]]]
显示CPU利用率历史信息记录功能相关配置	display cpu-usage configuration [slot <i>slot-number</i> [cpu <i>cpu-number</i>]]
以图表方式显示CPU利用率的历史记录	display cpu-usage history [job <i>job-id</i>] [slot <i>slot-number</i> [cpu <i>cpu-number</i>]]
显示设备信息	display device [flash] [slot <i>slot-number</i> verbose]
显示设备的电子标签信息	display device manuinfo [slot <i>slot-number</i>]
收集诊断信息	display diagnostic-information [hardware infrastructure 12 13 service] [key-info] [<i>filename</i>]
显示接收断电告警的目的主机的信息	display dying-gasp host
显示设备的温度信息	display environment [slot <i>slot-number</i>]
显示风扇的工作状态	display fan [slot <i>slot-number</i> [<i>fan-id</i>]]
显示设备的内存使用状态	display memory [summary] [slot <i>slot-number</i> [cpu <i>cpu-number</i>]]
显示内存告警门限相关信息	display memory-threshold [slot <i>slot-number</i> [cpu <i>cpu-number</i>]]
显示设备的电源状态	display power [slot <i>slot-number</i> [<i>power-id</i>]]
显示Job的配置信息	display scheduler job [<i>job-name</i>]
显示Job的执行日志信息	display scheduler logfile
显示定时重启功能的相关配置	display scheduler reboot
显示Schedule的相关信息	display scheduler schedule [<i>schedule-name</i>]
显示系统的稳定状态	display system stable state
显示系统版本信息	display version
显示启动软件包版本更新操作的记录	display version-update-record
清除Schedule日志文件的相关信息	reset scheduler logfile

操作	命令
清除启动软件包版本更新操作的记录	reset version-update-record

目 录

1 Tcl.....	1-1
1.1 Tcl在Cowmare V7 中的使用.....	1-1
1.2 Tcl配置限制和指导.....	1-1
1.3 通过Tcl脚本配置设备.....	1-1
1.3.1 配置限制和指导.....	1-1
1.3.2 配置步骤.....	1-1
1.4 在Tcl配置视图下执行Comware命令.....	1-2
1.4.1 功能简介.....	1-2
1.4.2 配置限制和指导.....	1-2
1.4.3 配置步骤.....	1-2

1 Tcl

1.1 Tcl在Comware V7中的使用

ComwareV7 系统内嵌了 Tcl（Tool Command Language，工具命令语言）解析器，支持直接在设备上执行 Tcl 脚本命令，以实现通过 Tcl 脚本配置设备。

在用户视图下执行 **tclsh** 命令，会进入 Tcl 配置视图。为兼容 Comware 配置方式，在 Tcl 配置视图下，用户可以直接输入 Tcl 脚本命令，也可以输入 Comware 系统的命令。命令输入完成后，直接回车即可执行。

Tcl 配置视图下，支持 Tcl8.5 版本的所有命令。

对于 Comware 系统的命令，Tcl 配置视图相当于用户视图，配置方式同用户视图下的配置。

1.2 Tcl配置限制和指导

通过 Tcl 脚本配置设备或在 Tcl 配置视图下执行 Comware 命令的过程中，如需退回上一级视图，只能使用 **quit** 命令。如需退回 Tcl 配置视图，不能使用 **return** 命令，可以使用组合键<Ctrl+Z>。

1.3 通过Tcl脚本配置设备

1.3.1 配置限制和指导

在 Tcl 配置视图下编辑命令时，遵循以下约定：

- 用户需保证输入的 Tcl 脚本命令可以正确执行。
- 由于执行 Tcl 脚本命令过程无法使用快捷键或命令行方式中断，如果用户通过 Telnet/SSH 方式登录设备并执行脚本命令时出现问题，需要关闭当前连接来终止执行过程；如果用户通过 Console 口方式登录设备并执行脚本命令时出现问题，则必须重启设备。因此建议用户通过 Telnet/SSH 方式登录设备并进入 Tcl 视图执行脚本命令。
- 在 Tcl 中定义的环境变量可以应用到 Comware 系统的命令。
- Tcl 脚本命令不支持输入“？”键获得在线帮助和 Tab 键补全功能。
- 已经成功执行的 Tcl 脚本命令不会记录在历史命令缓冲区中。
- 通过 Tcl 脚本命令 **read stdin** 进行读取操作时，可以通过<Ctrl+D>结束读取。

1.3.2 配置步骤

(1) 从用户视图进入 Tcl 配置视图。

tclsh

(2) 根据需求执行 Tcl 脚本。

Tcl command

(3) 从 Tcl 配置视图退回到用户视图。

◦ **tclquit**

- **quit**

1.4 在Tcl配置视图下执行Comware命令

1.4.1 功能简介

在 Tcl 配置视图下执行 Comware 命令有两种方式：一种是在 Tcl 配置视图下直接输入 Comware 命令，如果 Tcl 命令与 Comware 命令的命令字冲突，则执行 Tcl 命令；另一种是在 Comware 命令前添加 **cli** 命令关键字，该方式在 Tcl 命令与 Comware 命令的命令字冲突时能够优先执行 Comware 命令。

1.4.2 配置限制和指导

在 Tcl 配置视图下执行 Comware 命令时，遵循以下约定：

- 当 Comware 命令配置的字符串被特殊字符"或{}包围时，只有在特殊字符前加上\，该特殊字符才有效。例如，在接口视图下设置描述信息为"a"时，需要执行 **description \"a\"**；如果执行 **description "a"**，配置结果为 **description a**。
- Comware 系统的命令支持输入“？”键获得在线帮助和 Tab 键补全功能。关于输入“？”键获得在线帮助和 Tab 键补全功能的详细描述，请参见“基础配置指导”中的“CLI”。
- **cli** 命令是 Tcl 脚本命令，不支持输入“？”键获得在线帮助和 Tab 键补全功能。
- 已经成功执行的 Comware 系统的命令会记录在历史命令缓冲区中，使用上下光标键可以调用执行过的命令。
- 通过以下三种方式，可以一次执行多条 Comware 命令：
 - 在同一行连续键入多条 Comware 系统的命令，命令间用分号隔开。多条命令会按顺序下发并执行。例如 **ospf 100 ; area 0**。
 - 在 **cli** 命令后连续键入需要执行的多条 Comware 命令，每条 Comware 命令之间使用空格加分号进行分隔，在第一条 Comware 命令的前方和最后一条 Comware 命令的后方添加英文格式的双引号。例如 **cli "ospf 100 ; area 0"**。
 - 多次输入 **cli** 命令和 Comware 命令的组合，每组之间使用空格加分号分隔。例如 **cli ospf 100 ; cli area 0**。

1.4.3 配置步骤

- (1) 从用户视图进入 Tcl 配置视图。

tclsh

- (2) 执行 Comware 命令。

- 直接执行 Comware 命令。

Command

- 通过增加 **cli** 命令关键字执行 Comware 命令。

cli *command*

- (3) 从 Tcl 配置视图退回到用户视图。

- **tclquit**

- quit

目 录

1 Python	1-1
1.1 Python简介	1-1
1.2 执行Python脚本文件	1-1
1.3 进入Python shell	1-1
1.4 导入Comware包以使用扩展API	1-1
1.4.1 导入整个Comware包并执行扩展API	1-1
1.4.2 导入单个API函数并执行该函数	1-2
1.5 退出Python shell	1-2
1.6 Python典型配置举例	1-2
1.6.1 Python基础配置举例	1-2
2 Comware扩展Python API	2-1
2.1 CLI	2-1
2.2 get_error	2-1
2.3 get_output	2-2
2.4 get_self_slot	2-2
2.5 get_slot_info	2-3
2.6 get_slot_range	2-3
2.7 get_standby_slot	2-4
2.8 Transfer	2-4

1 Python

1.1 Python简介

Python 是一种简单易学，功能强大的编程语言，它有高效率的高层数据结构，简单而有效地实现了面向对象编程。Python 简洁的语法和对动态输入的支持，再加上解释性语言的本质，使得它在大多数平台上的许多领域都是一个理想的脚本语言，特别适用于快速的应用程序开发。

在 Comware V7 系统上可以采用如下方式使用 Python：

- 通过执行 Python 脚本进行自动化配置系统。
- 进入Python shell，使用Python2.7 版本的命令、标准API或扩展API对设备进行配置。其中，扩展API是Comware对Python进行的扩展，用来方便用户进行系统配置。关于Comware的Python扩展，可以参考“[2 Comware扩展Python API](#)”。

1.2 执行Python脚本文件

请在用户视图下执行本命令，执行 Python 脚本文件。

```
python filename
```

1.3 进入Python shell

请在用户视图下执行本命令，进入 Python shell。

```
python
```

1.4 导入Comware包以使用扩展API

用户如需使用扩展 Python API，必须先导入 Comware 包。导入时，可选择导入整个 Comware 包或单个 API。

1.4.1 导入整个Comware包并执行扩展API

1. 配置步骤

- (1) 请在用户视图下执行本命令，进入 Python shell。

```
python
```

- (2) 导入整个 Comware 包。

```
import comware
```

- (3) 执行扩展 API。

```
comware.api
```

2. 配置举例

下例采用 API Transfer 将 TFTP 服务器（192.168.1.26）上的文件 test.cfg 下载到设备上。

```
<Sysname> python
```

```

Python 2.7.3 (default)
[GCC 4.4.1] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> import comware
>>> comware.Transfer('tftp', '192.168.1.26', 'test.cfg', 'flash:/test.cfg', user='',
password='')
<comware.Transfer object at 0xb7eab0e0>

```

1.4.2 导入单个API函数并执行该函数

1. 配置步骤

- (1) 请在用户视图下执行本命令，进入 Python shell。

```
python
```

- (2) 导入单个 API 函数。

```
from comware import api-name
```

- (3) 执行扩展 API 函数。

```
api-function
```

2. 配置举例

下例采用 API Transfer 将 TFTP 服务器（192.168.1.26）上的文件 test.cfg 下载到设备上。

```

<Sysname> python
Python 2.7.3 (default)
[GCC 4.4.1] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> from comware import Transfer
>>> Transfer('tftp', '192.168.1.26', 'test.cfg', 'flash:/test.cfg', user='', password='')
<comware.Transfer object at 0xb7e5e0e0>

```

1.5 退出Python shell

请在 Python shell 下执行本命令，退出 Python shell。

```
exit()
```

1.6 Python典型配置举例

1.6.1 Python基础配置举例

1. 组网需求

使用 Python 脚本，下载 main.cfg 和 backup.cfg 两个配置文件到设备上，并设置为下次主用配置文件和备用配置文件。

2. 组网图

图1-1 Python 典型配置举例组网图



3. 配置步骤

在 PC 上使用写字板编辑 Python 脚本文件 test.py，内容如下：

```
#!/usr/bin/python
import comware

comware.Transfer('tftp', '192.168.1.26', 'main.cfg', 'flash:/main.cfg')
comware.Transfer('tftp', '192.168.1.26', 'backup.cfg', 'flash:/backup.cfg')
comware.CLI('startup saved-configuration flash:/main.cfg main ;startup saved-configuration
flash:/backup.cfg backup')
```

通过 TFTP 将 test.py 文件下载到设备上

```
<Sysname> tftp 192.168.1.26 get test.py
```

执行 Python 脚本文件

```
<Sysname> python flash:/test.py
<Sysname>startup saved-configuration flash:/main.cfg main
Please wait..... Done.
<Sysname>startup saved-configuration flash:/backup.cfg backup
Please wait..... Done.
```

4. 验证结果

使用 **display startup** 命令查看下次启动文件已经变为 main.cfg 和 backup.cfg。

```
<Sysname> display startup
Current startup saved-configuration file: flash:/startup.cfg
Next main startup saved-configuration file: flash:/main.cfg
Next backup startup saved-configuration file: flash:/backup.cfg
```

2 Comware扩展Python API

本文描述在 Comware V7 中提供的扩展 Python API，扩展 Python API 必须遵循标准 Python 语言语法。

2.1 CLI

用来执行 Comware V7 系统的命令并创建 CLI 对象。

【命令】

```
CLI(command="", do_print=True)
```

【参数】

command: 表示要下发的命令，缺省为空。CLI 下发命令是从用户视图开始，如果 *command* 中不指定视图，直接输入命令，表示该命令在用户视图下执行；当需要执行其它视图的命令时，需要先输入进视图的命令，再输入具体的配置命令。多条命令之间以空格加分号分隔，如 'system-view ;local-user test class manage'。

do_print: 表示是否输出执行结果，True 表示输出执行结果，False 表示不输出执行结果。缺省值为 True。

【返回值】

CLI 对象

【使用指导】

需要注意的是，CLI 仅支持 Comware 命令，不支持 Linux、Python、Tcl 命令。

【举例】

使用 API CLI 添加本地用户 test。

```
<Sysname> python
Python 2.7.3 (default)
[GCC 4.4.1] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> import comware
>>> comware.CLI('system-view ;local-user test class manage')
```

【结果】

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] local-user test class manage
New local user added.
<comware.CLI object at 0xb7f680a0>
```

2.2 get_error

用来获取下载文件过程中的错误信息。

【命令】

```
Transfer.get_error()
```

【返回值】

下载文件过程中的错误信息，若没有错误信息则返回 **None**。

【举例】

使用 API Transfer 将 TFTP 服务器（1.1.1.1）上的文件 **test.cfg** 下载到设备上。

```
<Sysname> python
Python 2.7.3 (default)
[GCC 4.4.1] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> import comware
>>> c = comware.Transfer('tftp', '1.1.1.1', 'test.cfg', 'flash:/test.cfg', user='',
password='')
>>> c.get_error()
```

【结果】

```
"Timeout was reached"
```

2.3 get_output

用来获取命令执行的输出信息。

【命令】

```
CLI.get_output()
```

【返回值】

命令执行的输出信息

【举例】

使用 API CLI 添加本地用户，并输出命令行执行结果。

```
<Sysname> python
Python 2.7.3 (default)
[GCC 4.4.1] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> import comware
>>> c = comware.CLI('system-view ;local-user test class manage', False)
>>> c.get_output()
```

【结果】

```
['<Sysname>system-view', 'System View: return to User View with Ctrl+Z.',
 '[Sysname]local-user test class manage', 'New local user added.']
```

2.4 get_self_slot

get_self_slot 接口用来获取主设备的成员编号。

【命令】

```
get_self_slot()
```

【返回值】

返回一个列表对象，格式为：[-1,*slot-number*]，其中 *slot-number* 表示主设备在 IRF 中的成员编号。

【举例】

使用 API 获取主设备所在的成员编号。

```
<Sysname> python
Python 2.7.3 (default)
[GCC 4.4.1] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> import comware
>>> comware.get_self_slot()
```

【结果】

```
[-1,0]
```

2.5 get_slot_info

get_slot_info 接口用来获取指定成员设备的信息。

【命令】

```
get_slot_info()
```

【返回值】

返回一个字典对象，返回值始终为{'Slot': *slot-number*, 'Status': '*status*', 'Chassis': *chassis-number*, 'Role': '*role*', 'Cpu': *CPU-number*}。 *slot-number* 表示设备在 IRF 中的成员编号，*status* 表示成员设备的状态，*chassis-number* 取值固定为 0，*role* 表示成员设备的角色，*CPU-number* 取值固定为 0。

【举例】

使用 API 获取成员编号/槽位号信息。

```
<Sysname> python
Python 2.7.3 (default)
[GCC 4.4.1] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> import comware
>>> comware.get_slot_info(1)
```

【结果】

```
{ 'Slot': 1, 'Status': 'Normal', 'Chassis': 0, 'Role': 'Master', 'Cpu': 0 }
```

2.6 get_slot_range

get_slot_range 接口用来获取当前系统所支持的成员编号范围。

【命令】

```
get_slot_range()
```

【返回值】

返回一个字典对象，返回值始终为{'MaxSlot': *max-slot-number*, 'MinSlot': *min-slot-number*}。
max-slot-number 表示设备支持的最大成员编号，*min-slot-number* 表示设备支持的最小成员编号。

【举例】

使用 API 获取系统成员编号范围。

```
<Sysname> python
Python 2.7.3 (default)
[GCC 4.4.1] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> import comware
>>> comware.get_slot_range()
```

【结果】

```
{'MaxSlot': 10, 'MinSlot': 1}
```

2.7 get_standby_slot

get_standby_slot 接口用来获取所有从设备的成员编号。

【命令】

```
get_standby_slot()
```

【返回值】

返回一个列表对象，格式为：[[-1, *slot-number*]]，其中 *slot-number* 表示从设备在 IRF 中的成员编号。如果 IRF 中没有从设备，则返回[]；当 IRF 中有多个从设备时，则返回：[[-1, *slot-number1*], [-1, *slot-number2*], ……]。

【举例】

使用 API 获取从设备所在的成员编号。

```
<Sysname> python
Python 2.7.3 (default)
[GCC 4.4.1] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> import comware
>>> comware.get_standby_slot()
```

【结果】

```
[[-1, 1], [-1, 2]]
```

2.8 Transfer

用来将指定文件通过指定协议下载到本地。

【命令】

```
Transfer(protocol="", host="", source="", dest="", login_timeout=10, user="", password="")
```


【参数】

protocol: 表示下载文件时使用的协议。取值为:

- **ftp**: 表示使用 FTP 协议传输文件。
- **tftp**: 表示使用 TFTP 协议传输文件。
- **http**: 表示使用 HTTP 协议传输文件。

host: 表示远程服务器的 IP 地址。

source: 表示服务器上源文件的名称。

dest: 表示保存到本地的目的文件的名称。

login_timeout: 表示下载文件时登录的超时时间, 单位为秒, 缺省值为 10。

user: 表示登录时使用的用户名称。

password: 表示登录时使用的用户密码。

【返回值】

Transfer 对象

【举例】

使用 API Transfer 将 TFTP 服务器 (192.168.1.26) 上的文件 test.cfg 下载到设备上。

```
<Sysname> python
Python 2.7.3 (default)
[GCC 4.4.1] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> import comware
>>> comware.Transfer('tftp', '192.168.1.26', 'test.cfg', 'flash:/test.cfg', user='',
password='')
```

【结果】

```
<comware.Transfer object at 0xb7f700e0>
```

目 录

1 自动配置.....	1-1
1.1 自动配置简介.....	1-1
1.2 服务器自动配置.....	1-1
1.2.1 服务器自动配置典型组网	1-1
1.2.2 服务器自动配置任务简介	1-2
1.2.3 配置文件服务器	1-2
1.2.4 准备配置文件	1-2
1.2.5 准备配置脚本	1-3
1.2.6 配置DHCP服务器	1-4
1.2.7 配置DNS服务器.....	1-5
1.2.8 配置网关.....	1-6
1.2.9 准备获取配置文件的接口	1-6
1.2.10 完成自动配置	1-6
1.3 自动配置典型配置举例.....	1-6
1.3.1 服务器自动配置举例（TFTP方式）	1-6
1.3.2 服务器自动配置举例（HTTP Tcl方式）	1-11
1.3.3 服务器自动配置举例（HTTP Python方式）	1-12
1.3.4 服务器自动配置实现IRF零配置举例	1-13

1 自动配置

1.1 自动配置简介

自动配置功能是指设备在启动时自动获取并执行配置文件。网络管理员只需将配置文件保存在指定的存储介质上，启动设备，即可实现自动配置，从而简化了网络配置，大大降低了网络管理员的工作量，便于实现对设备的集中管理。

自动配置的实现方式如 [表 1-1](#) 所示：

表1-1 自动配置实现方式

配置方式	配置文件保存位置	应用场景
服务器自动配置	文件服务器	网络规模较大，设备位置相对分散

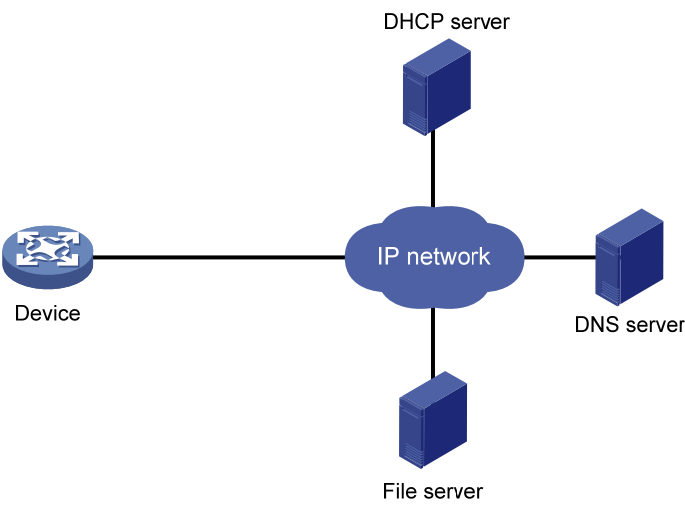
设备空配置启动时，首先自动检查存储介质的根目录下是否存在 `autocfg.py`、`autocfg.tcl` 或 `autocfg.cfg` 配置文件。如果存在，则直接执行此文件；如果不存在，则通过自动从文件服务器上获取并执行配置脚本文件或配置文件，实现自动配置功能。`autocfg.py`、`autocfg.tcl` 和 `autocfg.cfg` 配置文件同时只能在设备上存在一个。

1.2 服务器自动配置

1.2.1 服务器自动配置典型组网

服务器自动配置的典型组网环境如 [图 1-1](#) 所示。设备需要在DHCP服务器、文件服务器（TFTP服务器或HTTP服务器）和DNS服务器的配合下，实现服务器自动配置功能。

图1-1 服务器自动配置典型组网图



1.2.2 服务器自动配置任务简介

服务器自动配置任务如下：

- (1) [配置文件服务器](#)
- (2) 准备配置文件或配置脚本
 - [准备配置文件](#)
 - [准备配置脚本](#)
- (3) [配置DHCP服务器](#)
- (4) （可选）[配置DNS服务器](#)
- (5) （可选）[配置网关](#)
- (6) [准备获取配置文件](#)
- (7) [完成自动配置](#)

1.2.3 配置文件服务器

设备可以通过 HTTP 或 TFTP 获取配置文件，管理员需要根据选用的方式在文件服务器上配置相应的 HTTP 服务或 TFTP 服务。

1.2.4 准备配置文件

1. 配置文件类型

配置文件包括特定配置文件、部分或全部公用配置文件以及缺省配置文件（`device.cfg`）三种类型，如 [表 1-2](#) 所示。

表1-2 配置文件类型以及支持的文件服务器

配置文件类型	适用的设备	文件名要求	支持的文件服务器
特定配置文件	具有特定配置需求的设备	配置文件名.cfg 为了方便辨识文件名，尽量不要使用包含空格的配置文件名。	<ul style="list-style-type: none">• HTTP 服务器• TFTP 服务器
部分或全部公用配置文件	配置需求全部或者部分相同的设备	配置文件名.cfg “配置文件名”可以是任意文件名。	<ul style="list-style-type: none">• HTTP 服务器• TFTP 服务器
缺省配置文件	其它设备 包含一般设备启动的公用配置信息	device.cfg	TFTP服务器

2. 配置文件准备过程

管理员可以根据网络中不同设备的需求和文件服务器类型选择配置：

- (1) 在文件服务器上为每个具有特定配置需求的设备准备特定配置文件。
- (2) 在文件服务器上以.cfg 为后缀名为部分或全部具有相同配置的设备保存一个配置文件。

- (3) 在 TFTP 服务器上保存名为 **device.cfg** 的缺省配置文件为既没有特定配置文件也没有部分或全部共用配置文件的设备提供缺省配置。

3. 在 TFTP 服务器上准备主机名文件

如果 DHCP 服务器未下发配置文件名, 管理员还可以在 TFTP 服务器上创建主机名文件提供主机名和设备 IP 地址的对应关系, 以保证执行自动配置的设备获取到配置文件。

按照如下方式配置:

- (1) 创建主机名文件, 文件名必须设置为 “**network.cfg**”。
- (2) 按照以下格式手工在文件中添加主机 IP 地址与主机名的映射关系, 保证一行一条映射。

```
ip host host-name ip-address
```

例如, 主机名文件中可以包括以下内容:

```
ip host host1 101.101.101.101
ip host host2 101.101.101.102
ip host client1 101.101.101.103
ip host client2 101.101.101.104
```

主机名必须与主机的配置文件名保持一致。

1.2.5 准备配置脚本

1. 功能简介

配置脚本可以实现自动更新版本、下发配置等功能。

目前设备支持的配置脚本包括 Python 脚本和 Tcl 脚本。Python 脚本使用的文件后缀固定为 **py**, Tcl 脚本使用的文件后缀固定为 **tcl**。关于 Python 脚本的详细介绍, 请参见“基础配置指导”中的“Python”。关于 Tcl 脚本的详细介绍, 请参见“基础配置指导”中的“Tcl”。

2. 配置限制和指导

使用 Tcl 脚本配置文件对设备进行自动配置时, 若配置文件中的命令行错误 (例如: 命令行拼写错误、视图错误、设备不支持所配置的命令等), 那么设备在执行到错误命令行时将直接中断自动配置操作。

使用配置脚本与使用配置文件有如下区别:

- 在文件服务器上只支持配置特定配置脚本和部分或全部共用配置脚本两种形式, 不支持缺省配置脚本。
- 在文件服务器上不支持使用主机名文件提供主机名和 IP 地址的对应关系。

有关“特定配置”、“部分或全部共用配置”、“缺省配置”以及“主机名和 IP 地址的对应关系”请参见“[1.2.4 准备配置文件](#)”。

3. 配置脚本准备过程

管理员可以根据网络中不同设备的需求和文件服务器类型选择配置:

- (1) 在文件服务器上为每个具有特定配置需求的设备准备特定配置脚本。
- (2) 在文件服务器上以 **.tcl** 或 **.py** 为后缀名为部分或全部具有相同配置的设备保存一个配置文件。

1.2.6 配置DHCP服务器

1. 功能简介

DHCP 服务器为执行服务器自动配置的设备分配 IP 地址，并向设备通告获取自动配置文件或配置脚本的途径。

DHCP 服务器可以根据管理员需要的配置文件类型，进行相应的配置（下发配置脚本和下发配置文件实现一致，下面以下发配置文件为例）：

- 如果管理员为每台设备分配特定配置文件，则需要在 DHCP 服务器上配置静态绑定关系，为每台设备分配特定的 IP 地址和配置文件名。由于一个地址池下只能配置一条配置文件的命令，所以 DHCP 服务器上每一个地址池视图只能配置一个静态绑定关系。
- 如果管理员为局域网内的部分设备分配相同的配置文件，可以在 DHCP 服务器上为使用部分共用配置文件的设备配置静态绑定关系，并指定文件服务器和部分共用配置文件名。这时，这部分静态绑定关系需要在同一个 DHCP 地址池中配置。也可以使用动态分配 IP 地址的方式，管理员需要划分合适的动态地址段，为这部分设备分配 IP 地址，并指定文件服务器和部分共用配置文件名。
- 如果管理员为局域网内的所有设备分配相同的配置文件，则需要在 DHCP 服务器上配置动态分配 IP 地址的方式。为设备动态分配 IP 地址的同时，分配全部共用配置文件名。如果采用这种方式，全部共用配置文件中只能包含这些设备共有的配置，每个设备特有的配置还需要其他方式完成（如管理员使用 Telnet 登录到设备上手工配置）。

以上三种分配方式可以同时在一台 DHCP 服务器上配置。

2. 使用HTTP服务器下发配置文件或配置脚本

- (1) 进入系统视图。

```
system-view
```

- (2) 开启 DHCP 服务。

```
dhcp enable
```

缺省情况下，DHCP 服务处于关闭状态。

- (3) 创建 DHCP 地址池，并进入 DHCP 地址池视图。

```
dhcp server ip-pool pool-name
```

- (4) 为客户端分配 IP 地址。请至少选择其中一项进行配置。

- 配置 DHCP 地址池动态分配的主网段。

```
network network-address [ mask-length | mask mask ]
```

缺省情况下，未配置动态分配的主网段。

- 配置静态地址绑定。

```
static-bind ip-address ip-address [ mask-length | mask mask ]  
{ client-identifier client-identifier | hardware-address  
hardware-address [ ethernet | token-ring ] }
```

缺省情况下，未配置静态地址绑定。

多次执行本命令，可以配置多个静态地址绑定。同一地址只能绑定给一个客户端。若需修改绑定必须先解除绑定。

- (5) 配置 DHCP 客户端使用的远程启动配置文件的 HTTP 形式 URL。

bootfile-name *url*

缺省情况下，未配置 DHCP 客户端使用的远程启动配置文件的 HTTP 形式 URL。

3. 使用TFTP服务器下发配置文件或配置脚本

- (1) 进入系统视图。

system-view

- (2) 开启 DHCP 服务。

dhcp enable

缺省情况下，DHCP 服务处于关闭状态。

- (3) 创建 DHCP 地址池，并进入 DHCP 地址池视图。

dhcp server ip-pool *pool-name*

- (4) 为客户端分配 IP 地址。请至少选择其中一项进行配置。

- 配置 DHCP 地址池动态分配的主网段。

network *network-address* [*mask-length* | **mask** *mask*]

缺省情况下，未配置动态分配的主网段。

- 配置静态地址绑定。

static-bind ip-address *ip-address* [*mask-length* | **mask** *mask*]
{ **client-identifier** *client-identifier* | **hardware-address**
hardware-address [**ethernet** | **token-ring**] }

缺省情况下，未配置静态地址绑定。

多次执行本命令，可以配置多个静态地址绑定。同一地址只能绑定给一个客户端。若需修改绑定必须先解除绑定。

- (5) 指定 TFTP 服务器。请选择其中一项进行配置。

- 配置 DHCP 客户端使用的 TFTP 服务器地址。

tftp-server ip-address *ip-address*

缺省情况下，未配置 DHCP 客户端使用的 TFTP 服务器地址。

- 配置 DHCP 客户端使用的 TFTP 服务器名。

tftp-server domain-name *domain-name*

缺省情况下，未配置 DHCP 客户端使用的 TFTP 服务器名。

使用此方式指定 TFTP 服务器需要在网络中架设 DNS 服务器。

- (6) 配置 DHCP 客户端使用的启动配置文件名。

bootfile-name *bootfile-name*

缺省情况下，未配置 DHCP 客户端使用的启动配置文件名。

1.2.7 配置DNS服务器

在使用服务器自动配置功能时，在如下两种情况时，管理员需要配置 DNS 服务器：

- 当 TFTP 服务器上不存在主机名文件时，执行服务器自动配置的设备可以通过 DNS 服务器将自己的 IP 地址解析为主机名，以便从 TFTP 服务器获取到配置文件；

- 如果设备从 DHCP 应答报文中获取到 TFTP 服务器的域名，设备还可以通过 DNS 服务器将 TFTP 服务器的域名解析为 TFTP 服务器的 IP 地址。

1.2.8 配置网关

如果 DHCP 服务器、文件服务器和 DNS 服务器与执行服务器自动配置的设备不在同一网段，则需要部署网关设备，使得各个服务器和设备之间路由可达，并在网关上配置 DHCP 中继功能。

如果 DHCP 应答报文中不包括 TFTP 服务器 IP 地址和域名信息，或 TFTP 服务器 IP 地址和域名信息不合法，设备将以广播方式向 TFTP 服务器发送请求消息。由于广播报文只能在本网段内传播，如果设备与 TFTP 服务器不在同一个网段，则需要在网关设备上配置 UDP Helper 功能，将广播报文转换成单播报文，转发给指定的 TFTP 服务器。有关 UDP Helper 功能的详细介绍，请参见“三层技术-IP 业务配置指导”中的“UDP-helper”。

1.2.9 准备获取配置文件的接口

设备在进行自动配置时，系统按照如下规则选取符合条件的接口：

- (1) 若有处于链路状态 UP 的二层以太网接口，则选取默认 VLAN 对应的 VLAN 虚接口。
- (2) 若没有处于链路状态 UP 的二层以太网接口，则在 30 秒后开始下次服务器自动配置接口选择过程。

1.2.10 完成自动配置

- (1) 上电启动需要进行自动配置的设备。

设备进入服务器自动配置时：

- 如果获取并执行配置文件成功，则整个服务器自动配置过程结束。
- 如果获取不到自动配置文件，则本次自动配置尝试失败，设备将继续尝试自动配置。用户可以等待尝试次数达到上限，设备自动结束自动配置，或根据提示信息，使用<Ctrl+C>或<Ctrl+D>快捷键手工终止自动配置。自动配置失败并结束后，设备将以空配置启动。

- (2) 在完成自动配置的设备上保存配置。

save

设备在文件服务器获取到的配置文件执行完成后，该文件将被删除。建议在配置文件执行完成后保存配置。本命令的详细介绍请参见“基础配置命令参考”中的“配置文件管理”。

1.3 自动配置典型配置举例

1.3.1 服务器自动配置举例（TFTP方式）

1. 组网需求

如 [图 1-2](#) 所示，某公司下属两个部门：市场部门和研发部门，两个部门通过不同的网关设备连入网络。要求连接终端主机的设备 Switch D、Switch E、Switch F 和 Switch G 执行自动配置功能，启动后自动获取并执行配置文件，以实现：

- 网络管理员能够通过 Telnet 方式登录、控制设备。

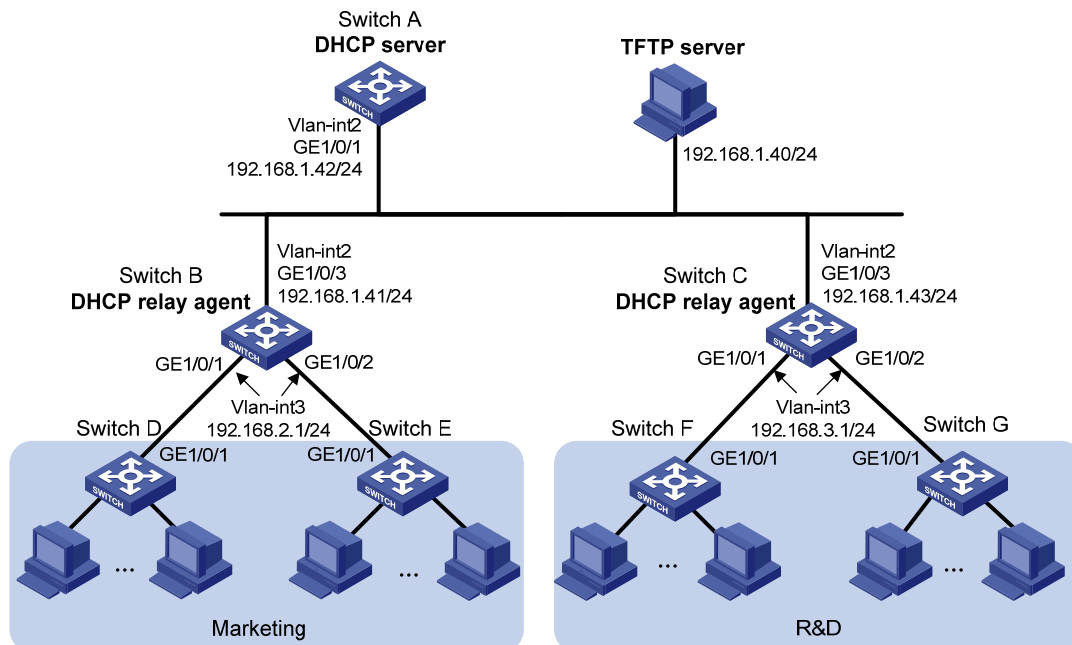
- 登录设备时需要进行认证，且登录不同部门的设备使用的用户名和密码不能相同，以提供一定的安全保证。

具体组网情况如下：

- Switch A 作为 DHCP 服务器，分别为市场部和研发部的主机分配 IP 地址和其他网络配置参数。
- 网关 Switch B 和 Switch C 作为 DHCP 中继设备。
- 一台运行 TFTP 管理软件的 TFTP 服务器上保存配置文件。

2. 组网图

图1-2 服务器自动配置组网图（TFTP 方式）



3. 配置步骤

(1) Switch A 的配置

配置接口 IP 地址

```
<SwitchA> system-view
[SwitchA] vlan 2
[SwitchA-vlan2] port gigabitethernet 1/0/1
[SwitchA-vlan2] quit
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] ip address 192.168.1.42 24
[SwitchA-Vlan-interface2] quit
```

开启 DHCP 服务。

```
[SwitchA] dhcp enable
```

配置 VLAN 接口 2 工作在 DHCP 服务器模式。

```
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] dhcp select server
[SwitchA-Vlan-interface2] quit
```

配置 DHCP 地址池 market，为市场部动态分配 192.168.2.0/24 网段的地址，并指定 TFTP server 地址、网关地址和配置文件名。

```
[SwitchA] dhcp server ip-pool market
[SwitchA-dhcp-pool-market] network 192.168.2.0 24
[SwitchA-dhcp-pool-market] tftp-server ip-address 192.168.1.40
[SwitchA-dhcp-pool-market] gateway-list 192.168.2.1
[SwitchA-dhcp-pool-market] bootfile-name market.cfg
[SwitchA-dhcp-pool-market] quit
```

配置 DHCP 地址池 rd，为研发部动态分配 192.168.3.0/24 网段的地址，并指定 TFTP server 地址、网关地址和配置文件名。

```
[SwitchA] dhcp server ip-pool rd
[SwitchA-dhcp-pool-rd] network 192.168.3.0 24
[SwitchA-dhcp-pool-rd] tftp-server ip-address 192.168.1.40
[SwitchA-dhcp-pool-rd] gateway-list 192.168.3.1
[SwitchA-dhcp-pool-rd] bootfile-name rd.cfg
[SwitchA-dhcp-pool-rd] quit
```

配置到达 DHCP 中继的静态路由。

```
[SwitchA] ip route-static 192.168.2.0 24 192.168.1.41
[SwitchA] ip route-static 192.168.3.0 24 192.168.1.43
[SwitchA] quit
```

(2) Switch B 的配置

配置接口的 IP 地址

```
<SwitchB> system-view
[SwitchB] vlan 2
[SwitchB-vlan2] port gigabitethernet 1/0/3
[SwitchB-vlan2] quit
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] ip address 192.168.1.41 24
[SwitchB-Vlan-interface2] quit
[SwitchB] vlan 3
[SwitchB-vlan3] port gigabitethernet 1/0/1
[SwitchB-vlan3] port gigabitethernet 1/0/2
[SwitchB-vlan3] quit
[SwitchB] interface vlan-interface 3
[SwitchB-Vlan-interface3] ip address 192.168.2.1 24
[SwitchB-Vlan-interface3] quit
```

开启 DHCP 服务。

```
[SwitchB] dhcp enable
```

配置 VLAN 接口 3 工作在 DHCP 中继模式。

```
[SwitchB] interface vlan-interface 3
[SwitchB-Vlan-interface3] dhcp select relay
```

配置 DHCP 服务器的地址。

```
[SwitchB-Vlan-interface3] dhcp relay server-address 192.168.1.42
```

(3) Switch C 的配置

配置接口的 IP 地址

```

<SwitchC> system-view
[SwitchC] vlan 2
[SwitchC-vlan2] port gigabitethernet 1/0/3
[SwitchC-vlan2] quit
[SwitchC] interface vlan-interface 2
[SwitchC-Vlan-interface2] ip address 192.168.1.43 24
[SwitchC-Vlan-interface2] quit
[SwitchC] vlan 3
[SwitchC-vlan3] port gigabitethernet 1/0/1
[SwitchC-vlan3] port gigabitethernet 1/0/2
[SwitchC-vlan3] quit
[SwitchC] interface vlan-interface 3
[SwitchC-Vlan-interface3] ip address 192.168.3.1 24
[SwitchC-Vlan-interface3] quit
# 开启 DHCP 服务。
[SwitchC] dhcp enable
# 配置 VLAN 接口 3 工作在 DHCP 中继模式。
[SwitchC] interface vlan-interface 3
[SwitchC-Vlan-interface3] dhcp select relay
# 配置 DHCP 服务器的地址。
[SwitchC-Vlan-interface3] dhcp relay server-address 192.168.1.42

```

(4) TFTP 服务器配置

在 TFTP server 创建配置文件 market.cfg，文件内容如下：

```

#
 sysname Market
#
 telnet server enable
#
vlan 3
#
local-user market
 password simple market
 service-type telnet
 quit
#
interface Vlan-interface3
 ip address dhcp-alloc
 quit
#
interface gigabitethernet 1/0/1
 port access vlan 3
 quit
#
user-interface vty 0 63
 authentication-mode scheme
 user-role network-admin
#

```

```
return
```

在 TFTP 服务器创建配置文件 `rd.cfg`，文件内容如下：

```
#
sysname RD
#
telnet server enable
#
vlan 3
#
local-user rd
password simple rd
service-type telnet
quit
#
interface Vlan-interface3
ip address dhcp-alloc
quit
#
interface gigabitethernet 1/0/1
port access vlan 3
quit
#
user-interface vty 0 63
authentication-mode scheme
user-role network-admin
#
return
```

启动 TFTP 管理软件，并指定 TFTP 的工作路径为保存上述配置文件的路径。

以 Windows XP 系统的主机为例，需保证 TFTP 服务器与 DHCP 中继之间路由可达。

4. 验证配置

- (1) Switch D、Switch E、Switch F 和 Switch G 在没有配置文件的情况下启动。启动成功后，在 Switch A 上查看地址池中的地址绑定信息。

```
<SwitchA> display dhcp server ip-in-use
```

IP address	Client-identifier/ Hardware address	Lease expiration	Type
192.168.2.2	3030-3066-2e65-3233-642e-3561-6633-2d56-6c61-6e2d-696e-7465-7266-6163-6533	May 6 05:21:25 2013	Auto(C)
192.168.2.3	3030-3066-2e65-3230-302e-3232-3033-2d56-6c61-6e2d-696e-7465-7266-6163-6533	May 6 05:22:50 2013	Auto(C)
192.168.3.2	3030-6530-2e66-6330-302e-3335-3131-2d56-6c61-6e2d-696e-7465-7266-6163-6531	May 6 05:23:15 2013	Auto(C)

```
192.168.3.3      3030-6530-2e66-6330- May 6 05:24:10 2013   Auto(C)
                 302e-3335-3135-2d56-
                 6c61-6e2d-696e-7465-
                 7266-6163-6532
```

(2) 在 Switch A 上执行如下命令：

```
<SwitchA> telnet 192.168.2.2
```

(3) 输入用户名 market、密码 market 后，可以登录 Switch D 或 Switch E。

1.3.2 服务器自动配置举例（HTTP Tcl方式）

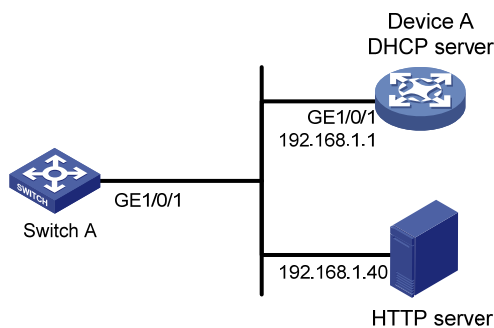
1. 组网需求

如 图 1-3 所示，Switch A 启动后自动从 HTTP 服务器获取 Tcl 脚本启动配置文件，并执行该文件，以实现：

- 网络管理员能够通过 Telnet 方式登录、控制设备。
- 登录设备时需要进行认证，以提供一定的安全保证。

2. 组网图

图1-3 服务器自动配置组网图（HTTP Tcl 方式）



3. 配置步骤

(1) 配置 DHCP 服务器

开启 DHCP 服务，创建名称为 1 的 DHCP 地址池，配置地址池动态分配 IP 地址的网段为 192.168.1.0/24。

```
<DeviceA> system-view
[DeviceA] dhcp enable
[DeviceA] dhcp server ip-pool 1
[DeviceA-dhcp-pool-1] network 192.168.1.0 24
```

配置 DHCP 客户端远程启动配置文件为 HTTP 形式的 URL。

```
[DeviceA-dhcp-pool-1] bootfile-name http://192.168.1.40/device.tcl
```

(2) 配置 HTTP 服务器，保证 Switch A 可以从 HTTP 服务器成功下载配置文件 device.tcl。

在 HTTP 服务器创建配置文件 device.tcl，文件内容如下：

```
return
system-view
telnet server enable
local-user user
```

```

password simple abcabc
service-type telnet
quit
user-interface vty 0 63
authentication-mode scheme
user-role network-admin
quit

```

```

interface Vlan-interface 1
ip address dhcp-alloc
return

```

启动 HTTP 管理软件，开启 HTTP 服务（配置过程略）。

4. 验证配置

- (1) Switch A 在没有配置文件的情况下启动。启动成功后，在 Device A 上查看地址池中的地址绑定信息。

```

<DeviceA> display dhcp server ip-in-use

```

IP address	Client identifier/ Hardware address	Lease expiration	Type
192.168.1.2	0030-3030-632e-3239- 3035-2e36-3736-622d- 4574-6830-2f30-2f32	Dec 12 17:41:15 2013	Auto(C)

- (2) 在 Device A 上执行如下命令：

```

<SwitchA> telnet 192.168.1.2

```

- (3) 输入用户名 **user**、密码 **abcabc** 后，用户可以登录 Switch A。

1.3.3 服务器自动配置举例（HTTP Python方式）

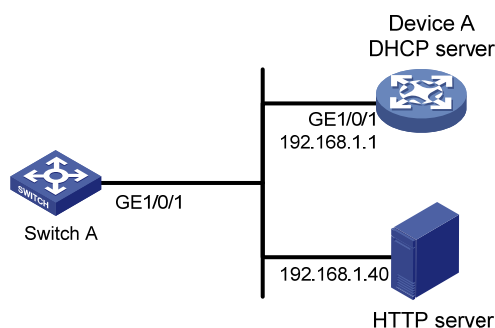
1. 组网需求

如 [图 1-4](#) 所示，Switch A 启动后自动从 HTTP 服务器获取 Python 脚本启动配置文件，并执行该文件，以实现：

- 网络管理员能够通过 Telnet 方式登录、控制设备。
- 登录设备时需要进行认证，以提供一定的安全保证。

2. 组网图

图1-4 服务器自动配置组网图（HTTP Python 方式）



3. 配置步骤

(1) 配置 DHCP 服务器

开启 DHCP 服务，创建名称为 1 的 DHCP 地址池，配置地址池动态分配 IP 地址的网段为 192.168.1.0/24。

```
<DeviceA> system-view
[DeviceA] dhcp enable
[DeviceA] dhcp server ip-pool 1
[DeviceA-dhcp-pool-1] network 192.168.1.0 24
```

配置 DHCP 客户端远程启动配置文件为 HTTP 形式的 URL。

```
[DeviceA-dhcp-pool-1] bootfile-name http://192.168.1.40/device.py
```

(2) 配置 HTTP 服务器，保证 Switch A 可以从 HTTP 服务器成功下载配置文件 device.py。

在 HTTP 服务器创建配置文件 device.py，文件内容如下：

```
#!/usr/bin/python
```

```
import comware
comware.CLI('system-view ;telnet server enable ;local-user user ;password simple
abcabc ;service-type telnet ;quit ;user-interface vty 0 63 ;authentication-mode
scheme ;user-role network-admin ;quit ;interface Vlan-interface 1 ;ip address
dhcp-alloc ;return')
```

启动 HTTP 管理软件，开启 HTTP 服务（配置过程略）。

4. 验证配置

(1) Switch A 在没有配置文件的情况下启动。启动成功后，在 Device A 上查看地址池中的地址绑定信息。

```
<DeviceA> display dhcp server ip-in-use
```

IP address	Client identifier/ Hardware address	Lease expiration	Type
192.168.1.2	0030-3030-632e-3239- 3035-2e36-3736-622d- 4574-6830-2f30-2f32	Dec 12 17:41:15 2013	Auto(C)

(2) 在 Device A 上执行如下命令：

```
<DeviceA> telnet 192.168.1.2
```

(3) 输入用户名 user、密码 abcabc 后，用户可以登录 Switch A。

1.3.4 服务器自动配置实现IRF零配置举例

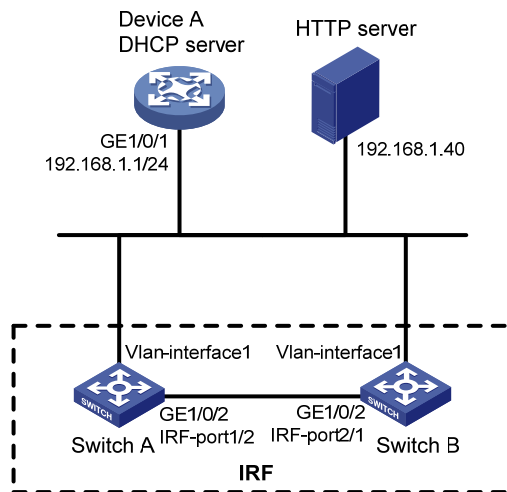
1. 组网需求

如 [图 1-5](#) 所示，Switch A 和 Switch B 通过 Vlan1 虚接口分别与 HTTP 服务器和 Device A 相连。Device A 上开启 DHCP 服务。为网络中的设备动态分配 192.168.1.0/24 网段的 IP 地址。

现要求通过自动配置实现 Switch A 和 Switch B 根据脚本自动执行 IRF 配置的相关命令。然后再连接 Switch A 和 Switch B 之间的线缆，完成 IRF 的建立。

2. 组网图

图1-5 服务器自动配置实现 IRF 零配置组网图



3. 配置步骤

(1) 配置设备接口地址，保证设备间路由可达。

配置 HTTP 服务器。启动 HTTP 管理软件，开启 HTTP 服务（配置过程略）。针对 IRF 零配置，HTTP 服务器上需要配置 Python 脚本文件、配置文件、sn.txt 和软件启动包等文件。以下是关于各文件的介绍：

- **Python 脚本文件：**Python 脚本是设备进行 IRF 零配置操作的主要文件，需要管理员自行准备并保存在 HTTP 服务器上。Python 脚本需要完成的操作：
 - 设备判断 flash 是否存在足够的存储空间（可选）；
 - 设备从 HTTP 服务器下载配置文件；
 - 设备从 HTTP 服务器下载启动软件包（可选）；
 - 设备从 HTTP 服务器下载 sn.txt 文件；
 - 配置设备下次启动时使用的启动软件包（可选）；
 - 解析 sn.txt 文件并修改设备的 IRF 成员编号；
 - 配置设备下次启动时使用的配置文件；
 - 设备重新启动。
- **配置文件：**配置文件包含了所有设备进行 IRF 的相关命令，管理员可以在已经成功创建 IRF 的设备上，将配置文件导出并修改然后保存在 HTTP 服务器上，供需要创建类似拓扑 IRF 的设备下载使用。
- **sn.txt 文件：**每个设备都有唯一的设备序列号，sn.txt 文件根据设备的序列号来指定设备在 IRF 组中的成员编码。设备通过运行 Python 脚本来解析 sn.txt 文件，然后修改设备的 IRF 成员编号，并根据自身的成员编号来完成相应的 IRF 配置。
- **软件启动包：**软件启动包是设备启动、运行的必备软件，需保存在 HTTP 服务器上。如果现有设备（包括主设备和从设备）的启动软件包全部一致且不需要升级软件版本，可不需要准备该文件。

(2) 在 Device A 上配置 DHCP 服务器

开启 DHCP 服务，创建名称为 1 的 DHCP 地址池，配置地址池动态分配 IP 地址的网段为 192.168.1.0/24。

```
<DeviceA> system-view
[DeviceA] dhcp enable
[DeviceA] dhcp server ip-pool 1
[DeviceA-dhcp-pool-1] network 192.168.1.0 24
```

配置 DHCP 客户端远程启动配置文件为 HTTP 形式的 URL。

```
[DeviceA-dhcp-pool-1] bootfile-name http://192.168.1.40/device.py
[DeviceA-dhcp-pool-1] quit
```

配置接口 GigabitEthernet1/0/1 工作在 DHCP 服务器模式。

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] dhcp select server
[DeviceA-GigabitEthernet1/0/1] quit
```

- (3) 设备根据 DHCP 服务器获取到 Python 脚本文件，执行 Python 脚本下载配置文件和软件启动包；解析 sn.txt 文件生成 IRF 成员编号。然后，所有设备会执行重启操作。
- (4) 设备重启完毕后，连接 Switch A 和 Switch B 之间的线缆，连接好线缆后设备将进行 IRF 选举，选举失败的一台设备会再次重启。当设备自动重启后，Switch A 和 Switch B 成功组成 IRF。

4. 验证配置

下面以 Switch A 为例验证设备是否成功组成 IRF，Switch B 和 Switch A 类似，不再赘述。

显示 IRF 中所有成员设备的相关信息。

```
<Switch A> display irf
```

MemberID	Slot	Role	Priority	CPU-Mac	Description
1	1	Standby	1	00e0-fc0f-8c02	---
*+2	1	Master	30	00e0-fc0f-8c14	---

* indicates the device is the master.

+ indicates the device through which the user logs in.

The Bridge MAC of the IRF is: 000c-1000-1111

```
Auto upgrade           : yes
Mac persistent         : always
Domain ID              : 0
Auto merge             : yes
```

以上显示信息表明 IRF 已经成功建立。