H3C MSR 系列路由器

基础配置指导(V7)

杭州华三通信技术有限公司
http://www.h3c.com.cn

资料版本：6W103-20140512
产品版本：MSR-CMW710-R0105

前 言

H3C MSR 系列路由器 配置指导(V7)共分为十五本手册，介绍了 MSR 系列路由器各软件特性的原理及其配置方法，包含原理简介、配置任务描述和配置举例。《基础配置指导》主要介绍设备的基本配置和管理，包括 CLI 配置、登录设备配置、FTP 和 TFTP 配置、文件系统管理配置、配置文件管理、软件升级管理和设备管理配置等内容。

前言部分包含如下内容：

适用款型

本手册所描述的内容适用于 MSR 系列路由器中的如下款型：

款型	
MSR 2600	MSR 26-30
MSR 3600	MSR 36-10
	MSR 36-20
	MSR 36-40
	MSR 36-60
	MSR3600-28
	MSR3600-51
MSR 5600	MSR 56-60
	MSR 56-80

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。
斜体	命令行参数（命令中必须由实际值进行替代的部分）采用*斜体*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 | ...]	表示从多个选项中选取一个或者不选。
{ x | y | ... }*	表示从多个选项中至少选取一个。
[x | y | ...]*	表示从多个选项中选取一个、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. 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。

3. 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。

4. 端口编号示例约定

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。

产品配套资料

H3C MSR 系列路由器的配套资料包括如下部分：

大类	资料名称	内容介绍
产品知识介绍	路由器产品彩页	帮助您了解产品的主要规格参数及亮点
硬件描述与安装	路由器安装指导	帮助您详细了解设备硬件规格和安装方法，指导您对设备进行安装
	MSR 系列路由器接口模块手册	帮助您详细了解单板的硬件规格
业务配置	MSR 系列路由器配置指导(V7)	帮助您掌握设备软件功能的配置方法及配置步骤
	MSR 系列路由器命令参考(V7)	详细介绍设备的命令，相当于命令字典，方便您查阅各个命令的功能
运行维护	路由器版本说明书	帮助您了解产品版本的相关信息（包括：版本配套说明、兼容性说明、特性变更说明、技术支持信息）及软件升级方法

资料获取方式

您可以通过H3C网站（www.h3c.com.cn）获取最新的产品资料：

H3C 网站与产品资料相关的主要栏目介绍如下：

- [服务支持/文档中心]：可以获取硬件安装类、软件升级类、配置类或维护类等产品资料。
- [产品技术]：可以获取产品介绍和技术介绍的文档，包括产品相关介绍、技术介绍、技术白皮书等。
- [解决方案]：可以获取解决方案类资料。
- [服务支持/软件下载]：可以获取与软件版本配套的资料。

技术支持

用户支持邮箱：service@h3c.com

技术支持热线电话：400-810-0504（手机、固话均可拨打）

网址：http://www.h3c.com.cn

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 命令行接口简介

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，比如通过Console口/Telnet/SSH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”。设备的命令行接口界面如 图 1-1 所示。

图1-1 命令行接口界面

```
******************************************************************************
* Copyright (c) 2004-2013 Hangzhou H3C Tech. Co., Ltd. All rights reserved.  *
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************

User interface aux0 is available.


Please press ENTER.

<H3C>
```

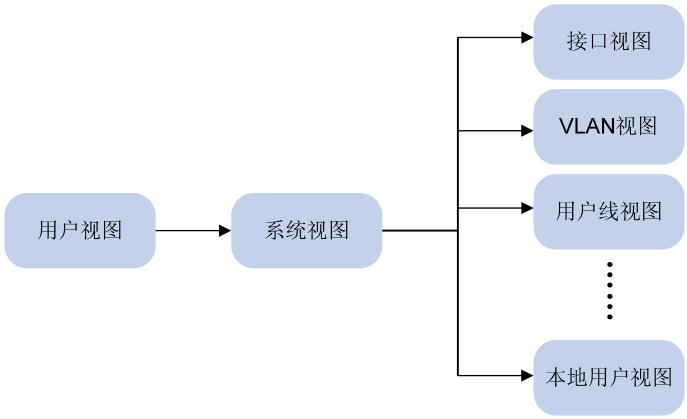
1.2 命令视图

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，比如提示符[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 1-2 所示。

图1-2 命令视图示意图



- 用户登录设备后，直接进入用户视图。此时屏幕显示的提示符是：<*设备名*>。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，此时屏幕显示的提示符是：[*设备名*]。系统视图下能对设备运行参数以及部分功能进行配置，比如配置夏令时、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，比如：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，比如 BGP 视图下还包含 BGP IPv4 单播实例视图和 BGP-VPN IPv4 单播实例视图等，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<?>。

说明

“*设备名*”是设备的名称，可以通过在系统视图下执行 **sysname** 命令来配置。关于 **sysname** 命令的详细介绍请参见“基础配置命令参考”中的“设备管理”。

1.2.2 进入系统视图

表1-1 进入系统视图

操作	命令	说明
进入系统视图	**system-view**	该命令在用户视图下执行

1.2.3 返回上一级视图

当前视图下的功能配置完成，使用本命令可以退出当前视图返回到上一级视图。需要注意的是：

- 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。

表1-2 返回上一级视图

操作	命令	说明
从当前视图返回上一级视图	**quit**	该命令可在任意视图下执行

1.2.4 返回用户视图

本命令为用户提供了一种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。用户也可以直接按组合键<Ctrl+Z>从当前视图返回用户视图。

表1-3 返回用户视图

操作	命令	说明
返回用户视图	**return**	该命令可在任意的非用户视图下执行

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。

(1) 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
  backup            Backup the startup configuration file to a TFTP server
  boot-loader       Set boot loader
……略……
```

(2) 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 ?
  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。

(3) 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。例如：

```
<Sysname> f?
   fixdisk
   format
```

```
  free
  ftp
<Sysname> display ftp?
  ftp
  ftp-server
  ftp-user
```

1.4 命令的undo形式

命令的 **undo** 形式一般用来恢复缺省情况、禁用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 1-4 所示的单个按键和如 表 1-7 所示的组合键。

表1-4 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
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： • 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

用户通过键盘输入命令行后，按<Enter>键执行该命令。

1.5.2 STRING和TEXT类型参数的输入

输入命令行时，如果命令行中的参数是 STRING 类型的，则设备对该参数的基本要求为：除“?”、“"”、“\”、空格之外的可见字符，可见字符对应的 ASCII 码区间为 32～126。

如果命令行中的参数是 TEXT 类型的，则除了“?”外的其他字符都可输入。

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

1.5.3 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。

比如用户视图下以 **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。

1.5.4 配置命令关键字的别名

使用本特性，可以给设备当前支持的命令行的第一个关键字或者 **undo** 命令的第二关键字取一个您惯用的关键字作为别名。比如将 **display** 的别名设置为 **show**，这样在设备上执行 **display clock** 命令时可以输入 **display clock**，也可以输入 **show clock**。

使用本特性后：

- 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，而不会以别名的形式。
- 当用户输入不完整关键字并回车，且该关键字与用户定义的别名以及现有某关键字同时部分匹配时，则只执行别名对应的命令。如果用户输入的字符串与多个别名部分匹配，则输出错误提示信息。
- 当用户输入不完整关键字并使用<Tab>键补全，且该关键字与用户定义的别名以及现有某关键字同时部分匹配时，则第一次使用<Tab>键，将联想出别名对应的原始关键字；再次使用<Tab>键，系统才会联想出现有关键字。

表1-5 配置命令关键字的别名

操作	命令	说明
进入系统视图	**system-view**	-
使能命令关键字别名功能	**command-alias enable**	缺省情况下，命令关键字别名功能处于关闭状态
给指定的命令关键字配置别名	**command-alias mapping** *cmdkey alias*	缺省情况下，没有给命令关键字配置别名 配置该命令时，输入的*cmdkey*参数必须是当前设备支持的命令行第一个关键字或者**undo**命令的第二个关键字的完整形式
（可选）显示命令关键字别名功能的相关配置	**display command-alias**	该命令可在任意视图下执行

1.5.5 配置命令行的快捷键

为便于用户对常用命令进行快捷操作，系统提供了一系列的快捷键。其中用户可自定义的快捷键有五个，配置步骤见 表 1-6，其他快捷键（见 表 1-7）为系统保留的，不能通过命令行配置。

只要用户按下某个快捷键，系统即可执行对应的指令。需要注意的是，当用户使用终端软件与设备进行交互时，且终端软件定义了这些快捷键（包括用户可定义的和系统保留的），则快捷键会遵从终端软件的定义，不会对设备生效。

表1-6 配置命令行的快捷键

操作	命令	说明
进入系统视图	**system-view**	-
配置命令行的快捷键	**hotkey** { **ctrl_g** | **ctrl_l** | **ctrl_o** | **ctrl_t** | **ctrl_u** } *command*	缺省情况下： • <Ctrl+G>对应命令 **display current-configuration**（显示当前配置） • <Ctrl+L>对应命令 **display ip routing-table**（显示 IPv4 路由表信息） • <Ctrl+O>对应命令 **undo debugging all**（关闭设备支持的所有功能项的调试开关） • <Ctrl+T>没有关联任何命令行 • <Ctrl+U>没有关联任何命令行
（可选）显示系统中快捷键的分配信息	**display hotkey**	该命令可在任意视图下执行

表1-7 系统保留的快捷键

快捷键	功能
<Ctrl+A>	将光标移动到当前行的开头
<Ctrl+B>	将光标向左移动一个字符
<Ctrl+C>	停止当前正在执行的功能
<Ctrl+D>	删除当前光标所在位置的字符
<Ctrl+E>	将光标移动到当前行的末尾
<Ctrl+F>	将光标向右移动一个字符
<Ctrl+H>	删除光标左侧的一个字符
<Ctrl+K>	终止呼出的连接
<Ctrl+R>	重新显示当前行信息
<Ctrl+V>	粘贴剪贴板的内容
<Ctrl+W>	删除光标左侧连续字符串内的所有字符
<Ctrl+X>	删除光标左侧所有的字符
<Ctrl+Y>	删除光标右侧所有的字符

快捷键	功能
<Ctrl+Z>	退回到用户视图
<Ctrl+]>	终止当前连接
<Esc+B>	将光标移动到左侧连续字符串的首字符处
<Esc+D>	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>	将光标向右移到下一个连续字符串之前
<Esc+N>	将光标向下移动一行（输入回车前有效）
<Esc+P>	将光标向上移动一行（输入回车前有效）
<Esc+<>	将光标所在位置指定为剪贴板的开始位置
<Esc+>>	将光标所在位置指定为剪贴板的结束位置

1.5.6 命令行输入回显功能

当用户在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。

表1-8 配置命令行输入回显功能

操作	命令	说明
进入系统视图	**system-view**	-
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语法检查。如果通过语法检查，则正确执行；否则，输出错误信息，常见的错误信息如 表 1-9 所示。

表1-9 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
% 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

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。两缓冲区的详细描述请参见 表 1-10。

表1-10 历史命令缓冲区描述表

历史命令缓冲区	是否可查看	是否可调用	退出登录后，历史命令是否继续保存	大小是否可调
独享历史命令缓冲区，每个用户线对应一个独享历史命令缓冲区	可通过**display history-command**来查看	• 使用上光标键↑并回车，可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	不保存	可通过**history-command max-size** *size-value*命令来配置（该命令的详细介绍请参见“基础配置命令参考”中的“登录设备”）。缺省情况下，可存放10条历史命令；如果将*size-value*设置为0，则不会缓存历史命令；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
共享历史命令缓冲区，所有用户线共用一个共享历史命令缓冲区	可通过**display history-command all**来查看	不能调用	保存	为固定大小1024条。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

设备保存历史命令时，遵循下列原则：

- 设备保存的历史命令与用户输入的命令格式相同。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关键字的别名形式，保存的历史命令也是别名形式。
- 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。

需要注意的是，在 Windows 200X 及 Windows XP 的超级终端和 Telnet 下可使用光标键访问历史命令，但对于 Windows 9X 的超级终端，↑、↓光标键无效，这是由于 Windows 9X 的超级终端对这两个键作了不同解释所致。

1.8 便捷地查看显示信息

1.8.1 分屏显示

1. 控制分屏显示

当显示信息较多并超过一屏时，系统会将信息分屏显示，并在屏间自动暂停，方便查看显示信息。这时用户可以使用 表 1-11 所示的按键来选择下一步操作。

表1-11 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

缺省情况下，一屏显示 24 行信息，也可以使用 **screen-length** 命令设置用户线下一屏显示的行数（**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”）。

2. 关闭分屏显示功能

可以通过以下配置禁用当前登录用户的分屏显示功能。禁止分屏显示时，会一次显示所有信息，如果信息较多，则会连续刷屏，不方便查看。

表1-12 禁止分屏显示

操作	命令	说明
禁用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 该操作在用户视图下执行，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

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。如果不带 **by-linenum** 参数，则不会显示行号。

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。

操作	命令
按行显示**display**命令执行结果（显示信息带行号）	**display** *command* **| by-linenum**

下面将通过举例示意如何查看带行号的显示信息。

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:  IP address: 192.168.2.1
    5:  Subnet mask: 255.255.255.0
```

```
  6:  Description: For LAN Access
  7:  Name: VLAN 0999
  8:  Tagged ports:   None
  9:  Untagged ports:
 10:      GigabitEthernet2/1/0
```

1.8.3 使用正则表达式过滤显示信息

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 1-13 所示。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。

表1-13 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	^user只能匹配以user开始的行，不能匹配以Auser开始的行
$	匹配以指定字符结束的行	user$只能匹配以user结尾的行，不能匹配以userA结尾的行
.	通配符，可代表任何一个字符	.s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	• zo*可以匹配 z 以及 zoo • (zo)*可以匹配 zo 以及 zozo
+	匹配+前面的字符或字符串一次或多次	zo+可以匹配zo以及zoo，但不能匹配z
|	匹配|左边的整个字符串或者右边的整个字符串	def|int只能匹配包含def或者int的字符串
( )	表示字符串，一般与“+”或“*”等符号一起使用	(123A)表示字符串123A；408(12)+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	(string)\1表示把string重复一次，匹配的字符串必须包含stringstring；(string1)(string2)\2表示把string2重复一次，匹配的字符串必须包含string1string2string2；(string1)(string2)\1\2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	• [16A]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 • [1-36A] 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） 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[]string]，才能匹配到]。[没有这样的限制

特殊字符	含义	举例
[^]	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	[^16A]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。比如[^16A]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	o{2}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	o{2,}不能匹配Bob，但能匹配fooooood
{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	o{1,3}能匹配fod、food、foood、foooood，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	\<do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	do\>匹配单词undo，还可以匹配字符串cdo
\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	v\w能匹配vlan，v\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	• \\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

下面将通过举例示意如何使用正则表达式过滤显示信息。

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（该显示信息与用户的当前配置有关）。

```
<Sysname> display current-configuration | begin line
line class aux
 user-role network-admin
#
line class tty
 user-role network-operator
#
line class vty
 user-role network-operator
#
line aux 0
 user-role network-admin
#
```

```
line vty 0 63
 authentication-mode none
 user-role level-15
 user-role network-operator
#
domain system
#
role name level-0
 description Predefined level-0 role
#
role name level-1
 description Predefined level-1 role
#
role name level-2
 description Predefined level-2 role
#
role name level-3
 description Predefined level-3 role
#
role name level-4
 description Predefined level-4 role
#
role name level-5
 description Predefined level-5 role
#
role name level-6
 description Predefined level-6 role
#
role name level-7
 description Predefined level-7 role
#
role name level-8
 description Predefined level-8 role
#
role name level-9
 description Predefined level-9 role
#
role name level-10
 description Predefined level-10 role
#
role name level-11
 description Predefined level-11 role
#
role name level-12
 description Predefined level-12 role
#
role name level-13
 description Predefined level-13 role
```

```
#
role name level-14
 description Predefined level-14 role
#
user-group system
#
return
```

查看路由表中的非直连路由（该显示信息与用户的当前配置有关）。

```
<Sysname> display ip routing-table | exclude Direct

Destinations : 12       Routes : 12

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
2.2.2.0/24          OSPF   10   2            1.1.2.2         GE2/1/0
```

查看 SNMP 相关配置（该显示信息与用户的当前配置有关）。

```
<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

display 命令显示的内容通常是统计信息、功能是否使能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。

表1-14 将显示信息保存到指定文件

操作	命令
将显示信息独立保存到指定文件	**display** *command* **>** *filename*
将显示信息以追加方式保存到已有文件	**display** *command* **>>** *filename*

下面将通过举例示意如何将显示信息保存到指定文件以及保存效果。

将 display vlan 1 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:
    GigabitEthernet2/1/0
```

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:
    GigabitEthernet2/1/0

 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:
    GigabitEthernet2/1/1
```

1.8.5 各种便捷查看方式的综合应用

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”。

表1-15 各种便捷查看方式的综合应用

操作	命令
各种便捷查看方式的综合应用	**display** *command* [**|** [**by-linenum**] { **begin** | **exclude** | **include** } *regular-expression*] [**>** *filename* | **>>** *filename*]

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
```

1.9 保存当前配置

在设备上，可以输入 **save** 命令，将当前配置保存到配置文件中。这样在设备重启后，所有保存的配置不会丢失。

配置保存不涉及一次性执行命令，比如：**display** 命令（执行后即显示相关信息）和 **reset** 命令（执行后即清除相关信息）。**save** 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”。

目 录

1 RBAC

说明

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

1.1 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。

由于权限与用户的分离，RBAC 具有以下优势：

- 管理员不需要针对用户去逐一指定权限，只需要预先定义具有相应权限的角色，再将角色赋予用户即可。因此 RBAC 更能适应用户的变化，提高了用户权限分配的灵活性。
- 由于角色与用户的关系常常会发生变化，但是角色和权限的关系相对稳定，因此利用这种稳定的关联可减小用户授权管理的复杂性，降低管理开销。

1.1.1 权限与角色的关联

权限与角色的关联是通过为角色赋予权限建立的，具体实现包括以下两个方面：

- 通过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。
- 通过资源控制策略实现对系统资源（接口、VLAN、VPN 实例）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，禁止用户操作接口 GigabitEthernet2/1/1。

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、特性组或者 XML 元素进行操作。

(1) 命令：控制用户权限的最小单元。RBAC 根据命令的作用，将命令分成以下三类：

- 读类型：本类型的命令仅能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**。
- 写类型：本类型的命令用于对系统进行配置，如使能信息中心功能的命令 **info-center enable**、配置调试信息开关的命令 **debugging**。
- 执行类型：本类型的命令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**。

(2) 特性：与一个功能相关的所有命令的集合，例如 OSPF 特性包含了所有 OSPF 的配置、显示及调试命令。系统中的所有特性及其包含的命令都是系统预定义的，不允许用户自定义。

(3) 特性组：一个或者多个特性的集合。其主要目的是为了方便管理员对用户权限进行配置。系统预定义了两个特性组 L2 和 L3。L2 中包含了所有的二层协议相关功能的命令，L3 中包含了所有三层协议相关功能的命令。管理员可以根据需要自定义特性组，但不能修改和删除系统预定义的特性组 L2 和 L3。各个特性组之间包含的特性允许重叠。

(4) XML 元素：XML 对于配置对象的组织也呈现树状结构，每一个 XML 元素代表 XML 配置中的一个 XML 节点。

根据权限控制范围的不同，可以将用户角色规则分为如下四类：

(1) 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。关于匹配的具体涵义，请参见 RBAC 配置命令。

(2) 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。因为特性中的每条命令都属于读类型、写类型或执行类型，所以在定义基于特性的规则时，可以精细地控制特性所包含的读、写或执行类型的命令能否被执行。

(3) 基于特性组的规则：此规则和基于特性的规则类似，区别是一条基于特性组的规则中可同时对多个特性包含的命令进行控制。

(4) 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。XML 元素也具有读，写或执行属性。

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三种类型的资源控制策略：接口策略、VLAN 策略以及 VPN 策略，它们分别定义了用户允许操作的接口、VLAN 以及 VPN 实例。对接口/VLAN/VPN 实例的操作是指创建并进入接口视图/VLAN 视图/VPN 实例视图视图、删除和应用接口/VLAN/VPN 实例（在 **display** 命令中指定接口/VLAN/VPN 实例参数并不属于应用接口/VLAN/VPN 实例）。

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。

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。

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

用户角色名	权限
network-operator	• 可执行系统所有功能和资源的相关 **display** 命令（除 **display history-command all** 命令，具体请通过 **display role name network-operator** 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 XML 元素
level-*n* (*n* = 0～15)	• 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

说明

- 只有具有 network-admin 或者 level-15 用户角色的用户登录设备后才可以执行 RBAC 特性的所有命令、修改用户线视图下的相关配置（包括 **user-role**、**authentication-mode**、**protocol inbound** 和 **set authentication password**）以及执行创建/修改/删除本地用户和本地用户组；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。
- 预定义的用户角色中，仅用户角色 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。需要注意的是，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。

1.1.2 角色与用户的关联

角色与用户的关联是通过为用户赋予角色建立的。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。

(1) 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。

(2) 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。

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。

说明

- 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”。
- 通过 publickey 或 password-publickey 认证登录服务器的 SSH 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。SSH 用户相关的介绍请参见“安全配置指导”中的“SSH”。

1.2 RBAC配置任务简介

表1-2 RBAC 配置任务简介

配置任务	说明	详细配置
创建用户角色	必选	1.3
为用户角色赋予权限	必选	1.4
为用户授权角色	可选	1.5
切换用户角色	可选	1.6

1.3 创建用户角色

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。

表1-3 创建用户角色

操作	命令	说明
进入系统视图	**system-view**	-
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）。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

操作	命令	说明
（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

1.4 为用户角色赋予权限

1.4.1 配置用户角色规则

用户角色规则分为以下四类，可根据权限控制需要配置一条或多条规则：

- 基于命令的规则：由允许/禁止（**permit**/**deny**）关键字及命令匹配字符串（*command-string*）定义是否允许执行一条命令或者与指定命令关键字相匹配的一组命令。
- 基于特性的规则：由允许/禁止（**permit**/**deny**）关键字、特性名称（*feature-name*）以及该特性中命令的类型（读/写/执行）定义是否允许执行一个或所有特性中包含的指定类型的命令。
- 基于特性组的规则：由允许/禁止（**permit**/**deny**）关键字、特性组名称（*feature-group-name*）以及该特性组中命令的类型（读/写/执行）定义是否允许执行一个特性组中的特性包含的指定类型的命令。
- 基于 XML 元素的规则：由允许/禁止（**permit**/**deny**）关键字、XML 元素名称（*feature-name*）以及该 XML 元素的类型（读/写/执行）定义是否允许执行一个或所有指定类型的 XML 元素。

关于用户角色规则，存在以下配置限制：

- 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。

表1-4 配置用户角色规则

操作	命令	说明
进入系统视图	**system-view**	-
进入用户角色视图	**role name** *role-name*	-
配置基于命令的规则	**rule** *number* { **deny** | **permit** } **command** *command-string*	至少选其一 缺省情况下，新创建的用户角色中未定义规则，即当前用户角色无任何权限 当多条规则中配置的权限出现冲突时，规则编号大的权限生效
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*	
配置基于XML元素的规则	**rule** *number* { **deny** | **permit** } { **execute** | **read** | **write** } * **xml-element** [*xml-string*]	
退回系统视图	**quit**	-
创建特性组，并进入特性组视图	**role feature-group name** *feature-group-name*	若要配置基于特性组的规则，则必选 缺省情况下，存在两个特性组，名称为L2和L3 除系统预定义的特性组L2和L3之外，系统中最多允许创建64个特性组

操作	命令	说明
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

1.4.2 配置资源控制策略

资源控制策略分为接口策略、VLAN 策略和 VPN 策略三类。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（接口/VLAN/VPN 实例）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。

需要注意的是，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。

表1-5 配置接口资源控制策略

操作	命令	说明
进入系统视图	**system-view**	-
进入用户角色视图	**role name** *role-name*	-
进入接口策略视图	**interface policy deny**	缺省情况下，用户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，则用户将没有操作任何接口的权限
（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

表1-6 配置 VLAN 资源控制策略

操作	命令	说明
进入系统视图	**system-view**	-
进入用户角色视图	**role name** *role-name*	-
并进入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
（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

表1-7 配置 VPN 资源控制策略

操作	命令	说明
进入系统视图	**system-view**	-
进入用户角色视图	**role name** *role-name*	-
进入VPN策略视图	**vpn-instance policy deny**	缺省情况下，用户具有操作任何VPN实例的权限 进入VPN策略视图后，如果不配置允许操作的VPN列表，则用户将没有操作任何VPN实例的权限
（可选）配置允许操作的VPN列表	**permit vpn-instance** *vpn-instance-name*&<1-10>	缺省情况下，未定义允许操作的VPN列表，用户没有操作任何VPN实例的权限 可以多次执行此命令向VPN列表中添加允许操作的VPN实例

1.5 为用户授权角色

说明

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。

1.5.1 使能缺省用户角色授权功能

对于通过 AAA 认证登录设备的用户，由 AAA 服务器（远程认证）或设备（本地认证）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。为此，系统提供了一个缺省用户角色授权功能。使能该功能后，用户在没有被授权任何角色的情况下，将具有一个缺省的用户角色 network-operator。

表1-8 使能缺省用户角色授权功能

操作	命令	说明
进入系统视图	**system-view**	-
使能缺省用户角色授权功能	**role default-role enable**	缺省情况下，缺省用户角色授权功能处于关闭状态 若本地用户的授权方案为**none**（即不授权），则必须使能缺省用户角色授权功能

1.5.2 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。

1.5.3 为本地AAA认证用户授权角色

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”。

需要注意的是：

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。

表1-9 为本地用户授权用户角色

操作	命令	说明
进入系统视图	**system-view**	-
创建本地用户，并进入本地用户视图	**local-user** *user-name* **class** { **manage** | **network** }	-
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 可通过多次执行本命令，为本地用户授权多个用户角色，最多可授权64个

1.5.4 为非AAA认证用户授权角色

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”。

表1-10 为非 AAA 认证用户授权用户角色

操作	命令	说明
进入系统视图	**system-view**	-
进入用户线视图	**line** { *first-num1* [*last-num1*] | { **aux** | **console** | **tty** | **vty** } *first-num2* [*last-num2*] }	二者选其一 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”
进入用户线类视图	**line class** { **aux** | **console** | **tty** | **vty** }	

操作	命令	说明
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Console/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 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

1.6 切换用户角色

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。因此，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。

2. 配置用户角色切换时的认证方式

为了保证切换操作的安全性，执行用户角色切换时，需要进行身份认证。设备支持如 表 1-11 所示的四种用户角色切换认证方式。

表1-11 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	设备验证用户输入的用户角色切换密码 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 对于Console/AUX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
scheme	通过HWTACACS或RADIUS进行远程AAA认证	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 使用该方式时，需要进行以下相关配置： • 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

认证方式	涵义	说明
local scheme	先本地密码认证，后远程AAA认证	先进行本地密码认证，若设备上没有设置本地用户角色切换密码，使用Console、TTY或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
scheme local	先远程AAA认证，后本地密码认证	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

目前，本地密码认证方式可支持任意用户角色之间的切换认证，但远程认证方式只能支持名称为 level-*n* 的用户角色之间的切换认证。

- 当使用 HWTACACS 方案进行用户角色切换认证时，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，每一个该类型的用户都能提供切换到低于或等于某最大级别的服务。例如，HWTACACS 服务器上存在一个用于角色切换认证的用户，它支持切换到的最高级别用户角色为 level-3，即表示用户可以使用该用户的用户名进行 level-0、level-1、level-2、level-3 之间的用户角色切换。无论用户希望切换到哪一个角色，系统均使用该用户名进行用户角色切换认证（是否携带域名由 **user-name-format** 命令决定）。
- 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相同形式的用户名。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。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“$enab3$@*domain-name*”或“$enab3$”形式的用户名进行用户角色切换认证（是否携带域名由 **user-name-format** 命令决定）。
- 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。

表1-12 配置用户角色切换时的认证方式

操作	命令	说明
进入系统视图	**system-view**	-
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
配置用户角色切换的密码	非FIPS模式下： **super password** [**role** *rolename*] [{ **hash** | **simple** } *password*] FIPS模式下： **super password** [**role** *rolename*]	如果采用**local**认证方式，则该步骤必选 缺省情况下，没有设置切换用户角色的密码 若不指定用户角色，则配置的是切换到network-admin用户角色的密码

3. 切换用户角色

表1-13 切换用户角色

操作	命令	说明
切换用户角色	**super** [*rolename*]	该命令在用户视图下执行 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 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

1.7 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1-14 RBAC 显示和维护

操作	命令
显示用户角色信息	**display role** [**name** *role-name*]
显示特性信息	**display role feature** [**name** *feature-name* | **verbose**]
显示特性组信息	**display role feature-group** [**name** *feature-group-name*] [**verbose**]

1.8 RBAC典型配置举例

1.8.1 Telnet用户的本地用户角色授权配置举例

1. 组网需求

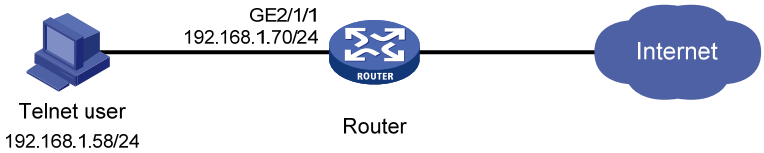
如 图 1-1 所示，Telnet用户主机与Router相连，需要实现Router对Telnet用户进行本地认证并授权用户角色。Telnet用户的登录用户名为user1@bbb，认证通过后被授权的用户角色为role1。

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 GigabitEthernet2/1/2～ GigabitEthernet2/1/4 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

配置接口 GigabitEthernet2/1/1 的 IP 地址，Telnet 用户将通过该地址连接 Router。

```
<Router> system-view
[Router] interface gigabitethernet 2/1/1
[Router-GigabitEthernet2/1/1] ip address 192.168.1.70 255.255.255.0
[Router-GigabitEthernet2/1/1] quit
```

开启 Router 的 Telnet 服务器功能。

```
[Router] telnet server enable
```

配置 Telnet 用户登录采用 AAA 认证方式。

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

配置 ISP 域 bbb 的 AAA 方法为本地认证和本地授权。

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

创建用户角色 role1。

```
[Router] 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。

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

配置用户角色规则 2，允许用户执行进入接口视图以及接口视图下的相关命令。

```
[Router-role-role1] rule 2 permit command system-view ; interface *
```

进入接口策略视图，允许用户具有操作接口 GigabitEthernet2/1/2～GigabitEthernet2/1/4 的权限。

```
[Router-role-role1] interface policy deny
[Router-role-role1-ifpolicy] permit interface gigabitethernet 2/1/2 to gigabitethernet
2/1/4
[Router-role-role1-ifpolicy] quit
[Router-role-role1] quit
```

创建设备管理类本地用户 user1。

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

配置用户的密码是明文的 aabbcc。

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

指定用户的服务类型是 Telnet。

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

指定用户 user1 的授权角色为 role1。

```
[Router-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。

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

4. 验证配置

用户向 Router 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 Router，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：

- 可操作接口 GigabitEthernet2/1/2～GigabitEthernet2/1/4。（以接口 GigabitEthernet2/1/1、GigabitEthernet2/1/2 为例）

进入接口 GigabitEthernet2/1/1 视图。

```
<Router> system-view
[Router] interface gigabitethernet 2/1/1
Permission denied.
```

配置接口 GigabitEthernet2/1/2 的 IPv4 地址。

```
[Router] interface gigabitethernet 2/1/2
[Router-GigabitEthernet2/1/2] ip address 6.6.6.6 24
[Router-GigabitEthernet2/1/2] quit
```

- 可执行所有特性中读类型的命令。（以 **display clock** 为例）

```
[Router] display clock
09:31:56 UTC Sat 01/01/2011
[Router] quit
```

- 不能执行特性中写类型和执行类型的命令。

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

1.8.2 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Router相连，Router与一台RADIUS服务器相连，需要实现RADIUS服务器对登录Router的Telnet用户进行认证和授权。

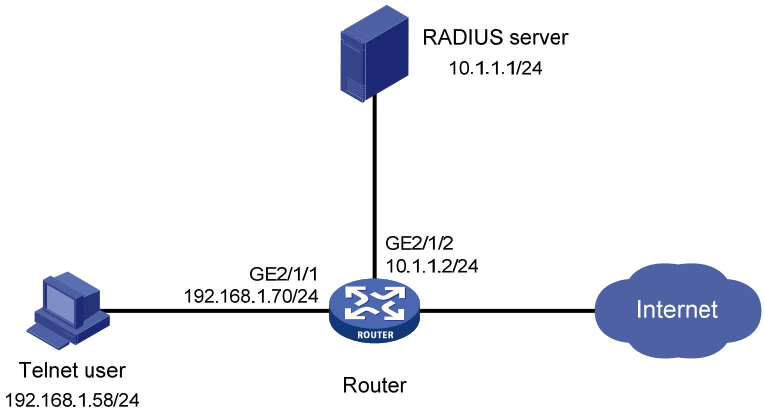
- 由一台 FreeRadius 服务器（IP 地址为 10.1.1.1/24）担当认证/授权 RADIUS 服务器的职责；
- Router 与 RADIUS 服务器交互报文时使用的共享密钥为 expert，认证端口号为 1812；
- Router 向 RADIUS 服务器发送的用户名携带域名；
- Telnet 用户登录 Router 时使用 RADIUS 服务器上配置的用户名 hello@bbb 以及密码进行认证，认证通过后被授权的用户角色为 role2。

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；
- 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 GigabitEthernet2/1/1～GigabitEthernet2/1/4 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) Router 上的配置

配置接口 GigabitEthernet2/1/1 的 IP 地址，Telnet 用户将通过该地址连接 Router。

```
<Router> system-view
[Router] interface gigabitethernet 2/1/1
[Router-GigabitEthernet2/1/1] ip address 192.168.1.70 255.255.255.0
[Router-GigabitEthernet2/1/1] quit
```

配置接口 GigabitEthernet2/1/2 的 IP 地址，Router 将通过该地址与服务器通信。

```
[Router] interface gigabitethernet 2/1/2
[Router-GigabitEthernet2/1/2] ip address 10.1.1.2 255.255.255.0
[Router-GigabitEthernet2/1/2] quit
```

开启 Router 的 Telnet 服务器功能。

```
[Router] telnet server enable
```

配置 Telnet 用户登录采用 AAA 认证方式。

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

创建 RADIUS 方案 rad。

```
[Router] 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。

```
[Router-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 expert。

```
[Router-radius-rad] key authentication expert
[Router-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。

```
[Router] domain bbb
[Router-isp-bbb] authentication login radius-scheme rad
[Router-isp-bbb] authorization login radius-scheme rad
[Router-isp-bbb] quit
```

创建特性组 fgroup1。

```
[Router] role feature-group name fgroup1
```

配置特性组 fgroup1 中包含特性 ARP 和 RADIUS。

```
[Router-featuregrp-fgroup1] feature arp
[Router-featuregrp-fgroup1] feature radius
[Router-featuregrp-fgroup1] quit
```

创建用户角色 role2。

```
[Router] 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。

```
[Router-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。

```
[Router-role-role2] rule 2 permit read write feature-group fgroup1
```

配置用户角色规则 3，允许用户执行创建 VLAN 以及进入 VLAN 视图后的相关命令。

```
[Router-role-role2] rule 3 permit command system-view ; vlan *
```

配置用户角色规则 4，允许用户执行进入接口视图以及接口视图下的相关命令。

```
[Router-role-role2] rule 4 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。

```
[Router-role-role2] vlan policy deny
[Router-role-role2-vlanpolicy] permit vlan 1 to 20
[Router-role-role2-vlanpolicy] quit
```

进入接口策略视图，允许用户具有操作接口 GigabitEthernet2/1/1～GigabitEthernet2/1/4 的权限。

```
[Router-role-role2] interface policy deny
[Router-role-role2-ifpolicy] permit interface gigabitethernet 2/1/1 to gigabitethernet
2/1/4
[Router-role-role2-ifpolicy] quit
[Router-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 Router 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 Router，并被授予用户角色 role2，具有相应的命令行执行权限。

可通过如下步骤验证用户的权限：

- 可执行 ISP 视图下所有的命令。

```
<Router> system-view
[Router] domain abc
[Router-isp-abc] authentication login radius-scheme abc
[Router-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）

```
[Router] radius scheme rad
[Router-radius-rad] primary authentication 2.2.2.2
```

```
[Router-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）

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

- 可操作接口 GigabitEthernet2/1/1～GigabitEthernet2/1/4。（以接口 GigabitEthernet2/1/2、GigabitEthernet2/1/5 为例）

```
[Router] vlan 10
```

将接口 GigabitEthernet2/1/2 加入到 VLAN 10。

```
[Router-vlan10] port gigabitethernet 2/1/2
```

将接口 GigabitEthernet2/1/5 加入到 VLAN 10。

```
[Router-vlan10] port gigabitethernet 2/1/5
Permission denied.
```

1.8.3 Telnet用户的HWTACACS用户角色切换认证配置

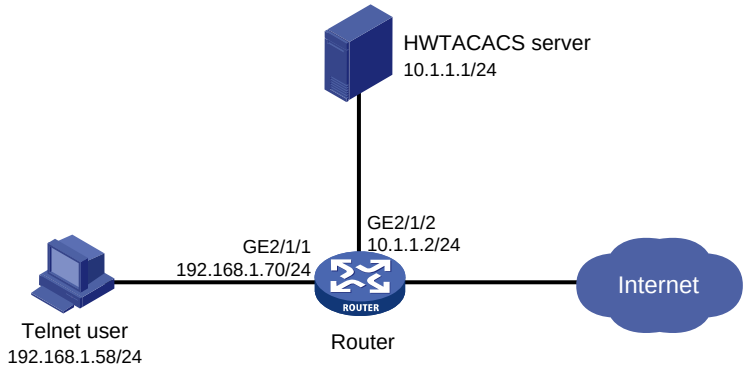
1. 组网需求

如 图 1-3 所示，Telnet用户主机与Router直接相连，Router与一台HWTACACS服务器相连，需要配置Router实现对登录Router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 Router 时进行本地认证，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 Router 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 中的本地认证。

- 创建 ISP 域 bbb，配置 Telnet 用户登录时采用的 **login** 认证和授权方法为 **local**。
- 创建本地用户，配置 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，Router 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 HWTACACS 方案 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 Router

配置 GE2/1/1 的 IP 地址，Telnet 客户端将通过该地址连接 Router。

```
<Router> system-view
[Router] interface GigabitEthernet 2/1/1
[Router-GigabitEthernet2/1/1] ip address 192.168.1.70 255.255.255.0
[Router-GigabitEthernet2/1/1] quit
```

配置 GE2/1/2 的 IP 地址，Router 将通过该地址与服务器通信。

```
[Switch] interface GigabitEthernet 2/1/2
[Router-GigabitEthernet2/1/2] ip address 10.1.1.2 255.255.255.0
[Router-GigabitEthernet2/1/2] quit
```

开启 Router 的 Telnet 服务器功能。

```
[Router] telnet server enable
```

配置 Telnet 用户登录采用 AAA 认证方式。

```
[Router] line vty 0 15
[Router-line-vty0-15] authentication-mode scheme
[Router-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）

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

创建 HWTACACS 方案 hwtac。

```
[Router] 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。

```
[Router-hwtacacs-hwtac] primary authentication 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。

```
[Router-hwtacacs-hwtac] key authentication simple expert
```

配置向 HWTACACS 服务器发送的用户名不携带域名。

```
[Router-hwtacacs-hwtac] user-name-format without-domain
[Router-hwtacacs-hwtac] quit
```

创建 ISP 域 bbb。

```
[Router] domain bbb
```

配置 Telnet 用户登录认证方法为本地认证。

```
[Router-isp-bbb] authentication login local
```

配置 Telnet 用户登录授权方法为本地授权。

```
[Router-isp-bbb] authorization login local
```
配置用户角色切换认证方法为 hwtac。
```
[Router-isp-bbb] authentication super hwtacacs-scheme hwtac
[Router-isp-bbb] quit
```
创建并配置设备管理类本地 Telnet 用户 test。
```
[Router] local-user test class manage
[Router-luser-manage-test] service-type telnet
[Router-luser-manage-test] password simple aabbcc
```
指定 Telnet 用户登录系统后被授予的用户角色为 level-0。
```
[Router-luser-manage-test] authorization-attribute user-role level-0
```
为保证 Telnet 用户仅使用授权的用户角色 level-0，删除用户 test 具有的缺省用户角色 network-operator。
```
[Router-luser-manage-test] undo authorization-attribute user-role network-operator
[Router-luser-manage-test] quit
```
配置用户级角色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。
```
[Router] super password role level-3 simple 654321
[Router] quit
```
(2) 配置 HWTACACS server

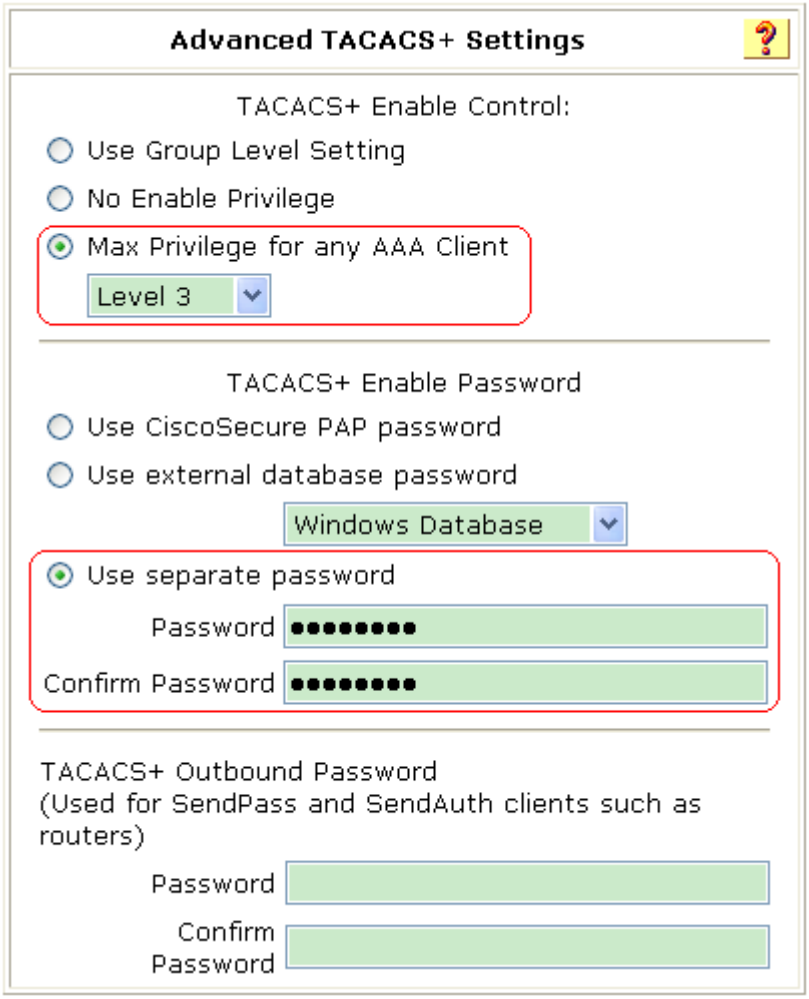

说明

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。

图1-4 设置 Telnet 用户的高级属性



5. 验证配置

(1) Telnet 用户建立与 Router 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 Router，且只能访问指定权限的命令。

```
<Router> telnet 192.168.1.70
Trying 192.168.1.70 ...
Press CTRL+K to abort
Connected to 192.168.1.59 ...
******************************************************************************
* Copyright (c) 2004-2012 Hangzhou H3C Tech. Co., Ltd. All rights reserved.  *
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************

login: test@bbb
Password:
<Router>?
```

```
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

<Router>
```

(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。

```
<Router> 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。

```
<Router> 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.
```

1.9 常见配置错误举例

1.9.1 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。

1.9.2 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

设备支持 CLI（Command Line Interface，命令行接口）和 SNMP（Simple Network Management Protocol，简单网络管理协议）两种登录方式：

- 通过 CLI 登录设备后，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、AUX 口（Auxiliary port，辅助端口）、Telnet、SSH 或 Modem 登录方式。
- 通过 SNMP 登录设备后，NMS 可以通过 Set 和 Get 等操作来配置和管理设备。关于 SNMP 的详细介绍请参见“网络管理与维护配置指导”中的“SNMP”。

用户首次登录设备时，只能通过Console口登录。登录时认证方式为none（不需要用户名和密码），用户角色为network-admin，详细登录过程请参见“缺省情况下如何通过Console口登录设备”。只有通过Console口登录到设备，进行相应的配置后，才能通过其它方式登录。各登录方式下需要的最小配置详见 表 1-1。

用户首次登录设备时，只能通过Console口登录。登录时认证方式为none（不需要用户名和密码），用户角色为network-admin，详细登录过程请参见“缺省情况下如何通过Console口登录设备”。只有通过Console口登录设备，进行相应的配置后，才能通过其它方式登录。各登录方式下需要的最小配置详见 表 1-1。

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”。

表1-1 各种登录设备方式的最小配置描述表

登录方式	最小配置描述
配置通过Console口/AUX口本地登录设备	缺省情况下，Console口登录时认证方式为none，存在安全隐患。用户在首次登录后，可以通过修改Console口登录的认证方式以及其它参数来增强设备的安全性 对于AUX口进行本地登录，至少需要进行如下配置： • 配置 password 认证方式的密码，或者更改认证方式并完成相关参数的设置（缺省情况下，AUX 用户采用 password 认证方式） • 配置 AUX 用户的用户角色（缺省情况下，VTY 用户的角色为 network-operator）
配置通过Telnet登录设备	• 开启设备的 Telnet 功能 • 配置 IP 地址，并确保设备与 Telnet 登录用户间路由可达（缺省情况下，设备没有配置 IP 地址） • 配置 password 认证方式的密码，或者更改认证方式并完成相关参数的设置（缺省情况下，VTY 用户采用 password 认证方式） • 配置 VTY 用户的用户角色（缺省情况下，VTY 用户的角色为 network-operator）
配置通过SSH登录设备	• 开启设备 SSH 功能并完成 SSH 属性的配置 • 配置 IP 地址，并确保设备与 SSH 登录用户间路由可达（缺省情况下，设备没有配置 IP 地址） • 配置 VTY 用户的认证方式为 scheme（缺省情况下，VTY 用户采用 password 认证方式） • 配置 VTY 用户的用户角色（缺省情况下，VTY 用户的角色为 network-operator）

登录方式	最小配置描述
配置通过Modem登录设备	• 配置 password 认证方式的密码，或者更改认证方式并完成相关参数的设置（缺省情况下，AUX 用户采用 password 认证方式） • 配置 VTY 用户的用户角色（缺省情况下，VTY 用户的角色为 network-operator）
配置通过SNMP登录设备	• 配置 IP 地址，并确保设备与 NMS 登录用户间路由可达（缺省情况下，设备没有配置 IP 地址） • 配置 SNMP 基本参数

2 缺省情况下如何通过Console口登录设备

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

通过 Console 口登录设备时，请按照以下步骤进行操作：

(1) 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，以免误插入其它接口。
- 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) 在PC机上运行终端仿真程序（如Windows XP/Windows 2000 的超级终端等，以下配置以Windows XP为例。PC上选择“开始>程序>附件>通讯>超级终端”），选择与设备相连的串口（PC上选择“我的电脑>管理>设备管理器>端口”来查看当前使用的串口），设置终端通信参数。这些参数的值必须和设备上的值一致，缺省情况下：传输速率为 9600bit/s、8 位数据位、1 位停止位、无校验和无流控，如 图 2-2 至 图 2-4 所示。

说明

如果 PC 使用的是 Windows Server 2003 操作系统，请在 Windows 组件中添加超级终端程序后，再按照本文介绍的方式登录和管理设备；如果 PC 使用的是 Windows Server 2008、Windows Vista、Windows 7 或其它操作系统，请准备第三方的终端控制软件，使用方法请参照软件的使用指导或联机帮助。

图2-2 新建连接

图2-3 连接端口设置

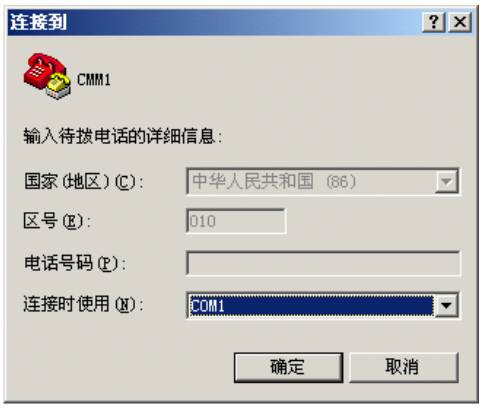
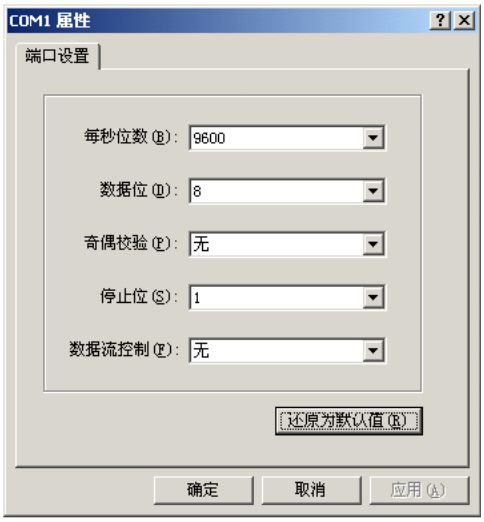
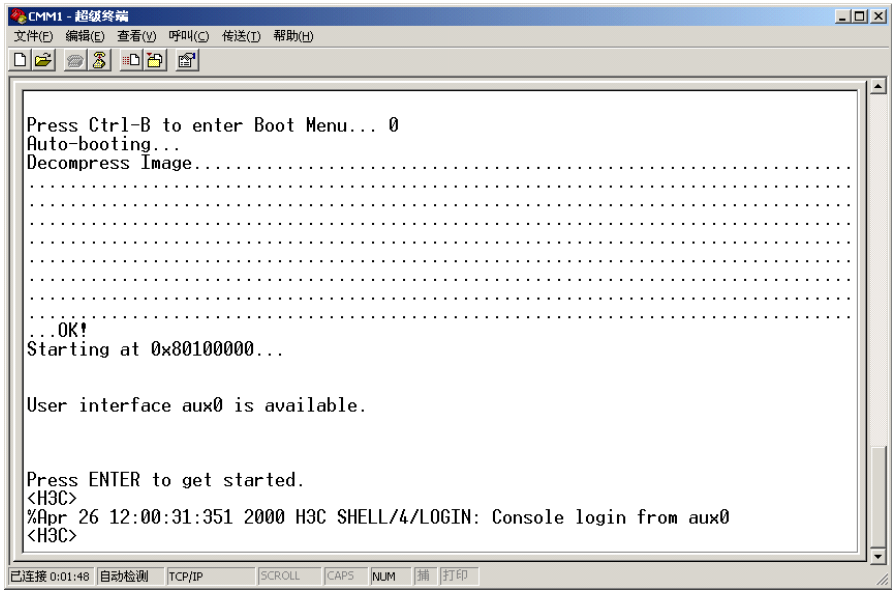


图2-4 端口通信参数设置



(5) 设备上电，终端上显示设备自检信息，自检结束后提示用户键入回车，用户键入回车后将出现命令行提示符（<H3C>），如 图 2-5 所示。

图2-5 设备配置界面



(6) 键入命令，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 配置通过CLI登录设备简介

说明

设备运行于 FIPS 模式时，不支持用户通过 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”。

通过 CLI 登录设备包括：通过 Console 口、Telnet、SSH、AUX 口或 Modem 登录方式。

- 缺省情况下，用户不需要任何认证即可通过 Console 口登录设备，这给设备带来许多安全隐患；
- 缺省情况下，用户不能通过 AUX 口、Telnet、SSH 以及 Modem 方式登录设备，这样不利于用户对设备进行远程管理和维护。

因此，用户需要对这些登录方式进行相应的配置，来增加设备的安全性及可管理性。

本文将分别介绍如何配置通过 Console 口、Telnet、SSH、AUX 口及 Modem 登录设备时的认证方式、用户角色及公共属性。

3.1.1 用户线简介

用户线用于管理、限制 CLI 登录用户的访问行为：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。当用户使用 Console 口、Telnet、SSH、AUX 口及 Modem 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。

1. 用户线概述

设备提供了四种类型的用户线：

- Console 用户线：用来管理和监控通过 Console 口登录的用户。
- AUX 用户线：用来管理和监控通过 AUX 口登录的用户。AUX 口通常用于通过 Modem 进行拨号访问。
- TTY（True Type Terminal，实体类型终端）用户线：用来管理和监控通过异步串口登录的用户。异步串口包括工作在异步方式的同/异步串口，即 Serial 接口，和专用异步串口，即 Async 接口。
- 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. 用户与用户线的关系

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 Console 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. 用户线的编号

用户线的编号有两种方式：绝对编号方式和相对编号方式。

(1) 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 Console 用户线编号，其次是所有 TTY 用户线，然后是所有 AUX 用户线，最后是所有 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。

(2) 相对编号方式

相对编号是每种类型用户线的内部编号。相对编号方式的形式是：“用户线类型 编号”，遵守如下规则：

- Console 口的编号：第一个为 CON 0。
- AUX 口的编号：第一个为 AUX 0。
- TTY 的编号：第一个为 TTY 1，第二个为 TTY 2，依次类推。
- VTY 的编号：第一个为 VTY 0，第二个为 VTY 1，依次类推。

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。非 FIPS 模式下，设备支持的认证方式有 none、password 和 scheme 三种；FIPS 模式下，设备仅支持 scheme 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。
- 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，请妥善保存密码。
- 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，请妥善保存用户名及密码。

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	说明
none	设置登录用户的认证方式为不认证	具体配置请见各登录方式下的相关章节
password	设置登录用户的认证方式为password认证	具体配置请见各登录方式下的相关章节
	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	具体配置请见各登录方式下的相关章节

认证方式	认证所需配置	说明
	在ISP域视图下为login用户配置认证方法	请参见“安全配置指导”中的“AAA”

3.1.3 用户角色简介

用户角色对登录用户至关重要，角色中定义了允许用户操作哪些系统功能以及资源对象，即用户登录后可以执行哪些命令。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”。

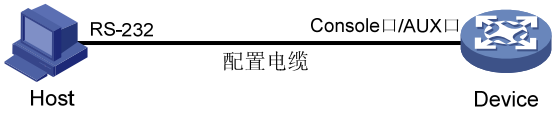
- 对于 none 和 password 认证方式，登录用户的角色由用户线下的用户角色配置决定。
- 对于 scheme 认证方式，且用户通过 SSH 的 publickey 或 password-publickey 方式登录设备时，登录用户将被授予同名的设备管理类本地用户视图下配置的授权用户角色。
- 对于 scheme 认证方式，非 SSH 登录以及用户通过 SSH 的 password 方式登录设备时，登录用户使用 AAA 认证用户的角色配置。尤其对于远程 AAA 认证用户，如果 AAA 服务器没有下发用户角色且缺省用户角色授权功能处于关闭状态时，用户将不能登录设备。

3.2 配置通过Console口/AUX口本地登录设备

通过Console口/AUX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 和 图 3-2 所示。

图3-1 通过 Console 口登录设备示意图

图3-2 通过 Console 口/AUX 口登录设备示意图



缺省情况下，用户可以直接通过 Console 口登录设备，登录时认证方式为 none（不需要用户名和密码），用户角色为 network-admin。用户可以修改认证方式、用户角色以及其它登录参数，来增加设备的安全性及可管理性。

缺省情况下，通过 AUX 口进行本地登录，使用 password 认证方式。需要先通过 Console 口或其它方式登录到设备上，配置 AUX 口 password 认证方式的密码，或者更改认证方式并完成相关参数的设置，才可以通过 AUX 口从本地登录设备。

3.2.1 通过Console口/AUX口登录设备配置任务简介

表3-2 通过 Console 口/AUX 口登录设备配置任务简介

配置任务		说明	详细配置
配置通过Console口/AUX口登录设备时的认证方式	配置通过Console口/AUX口登录设备时无需认证（none）	必选 请根据实际需要选择其中的一种认证方式 FIPS模式下，仅支持AAA认证（scheme）	3.2.2 1.
	配置通过Console口/AUX口登录设备时采用密码认证（password）		3.2.2 2.
	配置通过Console口/AUX口登录设备时采用AAA认证（scheme）		3.2.2 3.
配置Console口/AUX口登录方式的公共属性		可选	3.2.2 4.

说明

改变 Console 口/AUX 口登录的认证方式后，新认证方式对新登录的用户生效。

3.2.2 配置通过Console口/AUX口登录设备

1. 配置通过Console口/AUX口登录设备时无需认证（none）

用户已经成功登录到了设备上，并希望以后通过 Console 口/AUX 口登录设备时无需进行认证。

表3-3 配置用户通过 Console 口/AUX 口登录设备时无需认证

操作	命令	说明
进入系统视图	**system-view**	-
进入Console/AUX用户线视图	**line** { **aux** | **console** } *first-number* [*last-number*]	二者选其一 • 用户线视图下的配置优先于用户线类视图下的配置 • 用户线视图下的配置只对该用户线生效且立即生效 • 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 • 用户线视图下的属性配置为缺省值时，将采用用户线类视图下配置的值。如果用户线类视图下的属性配置也为缺省值时，则直接采用该属性的缺省值
进入Console/AUX用户线类视图	**line class** { **aux** | **console** }	
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，认证方式为none；用户通过AUX口登录，认证方式为password 如果设备上只有一个AUX口，而没有Console口（Console口与AUX口共用），则使用AUX用户线登录的用户不需要认证
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；通过AUX口登录设备的用户角色为network-operator

当用户下次通过Console口/AUX口登录设备时，无须提供用户名或密码，直接按回车键进入用户视图，如 图 3-3 和 图 3-4 所示。

图3-3 用户通过 Console 口登录设备时无需认证登录界面

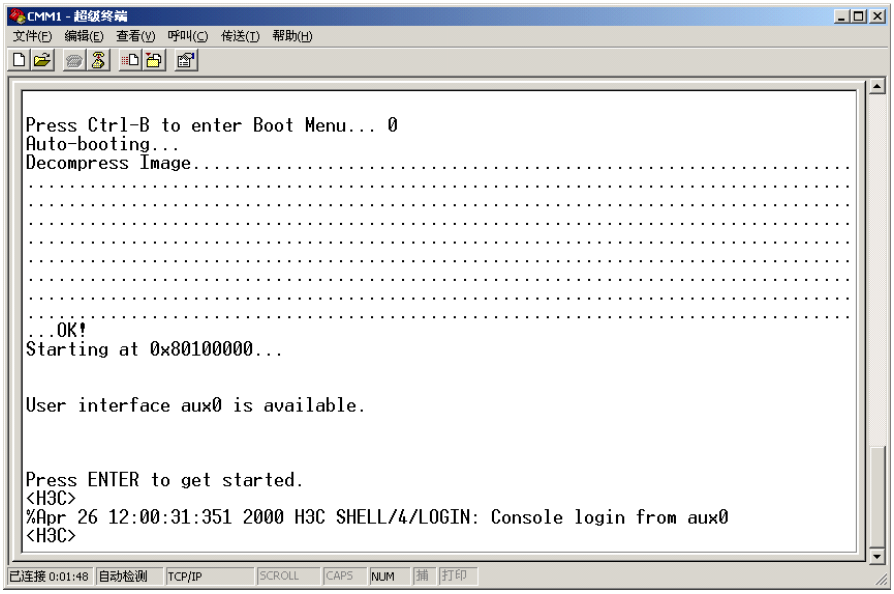
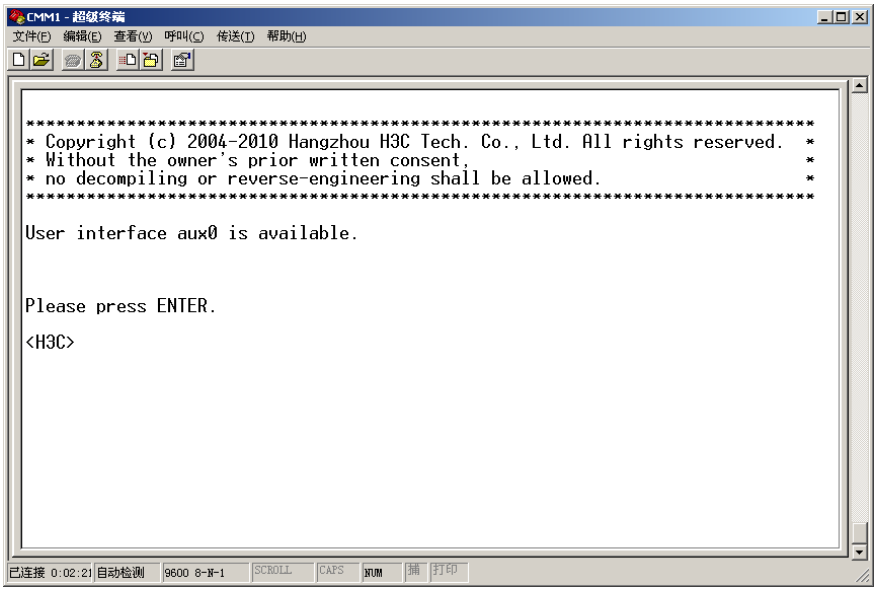


图3-4 用户通过 AUX 口登录设备时无需认证登录界面



2. 配置通过Console口/AUX口登录设备时采用密码认证（password）

用户已经成功登录到了设备上，并希望以后通过 Console 口/AUX 口登录设备时采用密码认证，以提高设备的安全性。

表3-4 配置用户通过 Console 口/AUX 口登录设备时采用密码认证

操作	命令	说明
进入系统视图	**system-view**	-
进入Console/AUX用户线视图	**line** { **aux** | **console** } *first-number* [*last-number*]	二者选其一 • 用户线视图下的配置优先于用户线类视图下的配置 • 用户线视图下的配置只对该用户线生效且立即生效 • 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 • 用户线视图下的属性配置为缺省值时，将采用用户线类视图下配置的值。如果用户线类视图下的属性配置也为缺省值时，则直接采用该属性的缺省值
进入Console/AUX用户线类视图	**line class** { **aux** | **console** }	
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，认证方式为none；用户通过AUX口登录，认证方式为password 如果设备上只有一个AUX口，而没有Console口（Console口与AUX口共用），则使用AUX用户线登录的用户不需要认证 用户线视图下，对**authentication-mode**和**protocol inbound**进行关联绑定，当两条命令中的任意一条配置了非缺省值，那么另外一条取缺省值
设置本地认证的密码	**set authentication password** { **hash** | **simple** } *password*	缺省情况下，没有设置本地认证的密码
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；通过AUX口登录设备的用户角色为network-operator

配置完成后，当用户再次通过Console口/AUX口登录设备，键入回车后，设备将要求用户输入登录密码。正确输入登录密码并回车，登录界面中出现命令行提示符（如<H3C>），如 图 3-5 和 图 3-6 所示。

图3-5 用户通过 Console 口登录设备时采用密码认证登录界面

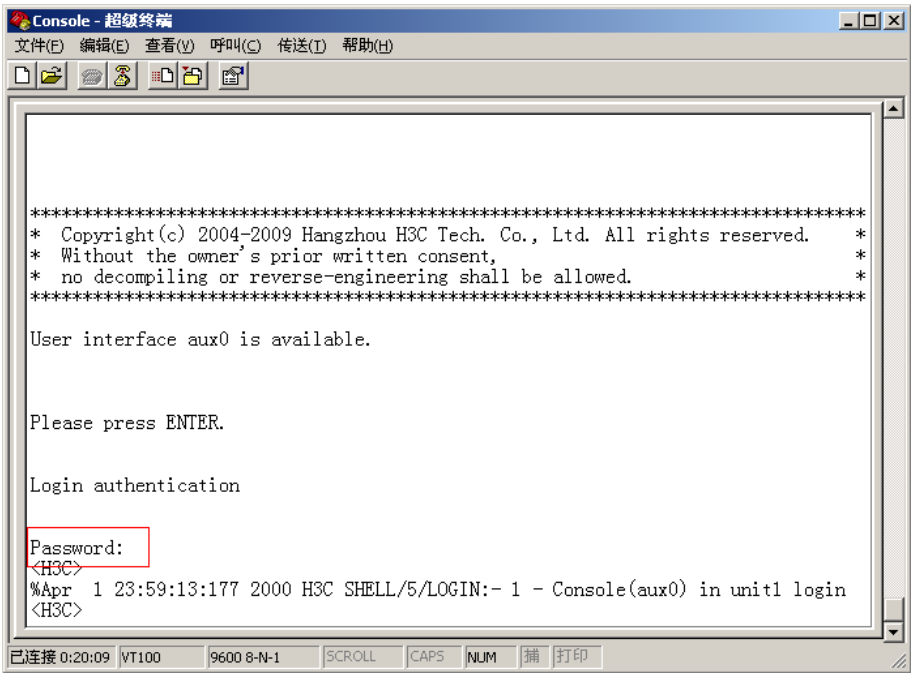
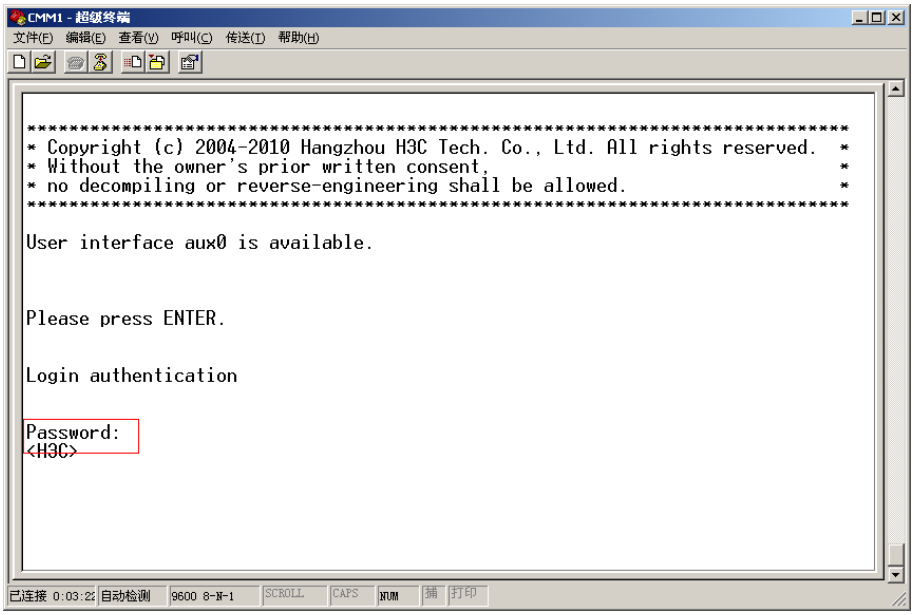


图3-6 用户通过 AUX 口登录设备时采用密码认证登录界面



3. 配置通过Console口/AUX口登录设备时采用AAA认证（scheme）

用户已经成功的登录到了设备上，并希望以后通过 Console 口/AUX 口登录设备时采用 AAA 认证，以提高设备的安全性。

要使配置的 AAA 认证方式生效，还需要在 ISP 域视图下配置 login 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。相关详细介绍请参见“安全配置指导”中的“AAA”。

表3-5 配置用户通过 Console 口/AUX 口登录设备时采用 AAA 认证

操作	命令	说明
进入系统视图	**system-view**	-
进入Console/AUX用户线视图	**line** { **aux** | **console** } *first-number* [*last-number*]	二者选其一 • 用户线视图下的配置优先于用户线类视图下的配置 • 用户线视图下的配置只对该用户线生效且立即生效 • 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 • 用户线视图下的属性配置为缺省值时，将采用用户线类视图下配置的值。如果用户线类视图下的属性配置也为缺省值时，则直接采用该属性的缺省值
进入Console/AUX用户线类视图	**line class** { **aux** | **console** }	
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，用户通过Console口登录，认证方式为none；用户通过AUX口登录，认证方式为password 如果设备上只有一个AUX口，而没有Console口（Console口与AUX口共用），则使用AUX用户线登录的用户不需要认证 用户线视图下，对**authentication-mode**和**protocol inbound**进行关联绑定，当两条命令中的任意一条配置了非缺省值，那么另外一条取缺省值

配置完成后，当用户再次通过Console口/AUX口登录设备，键入回车后，设备将要求用户输入登录用户名和密码。正确输入用户名（此处以用户为admin为例）和密码并回车，登录界面中出现命令行提示符（如<H3C>），如 图 3-7 和 图 3-8 所示。

图3-7 用户通过 Console 口登录设备时 AAA 认证登录界面

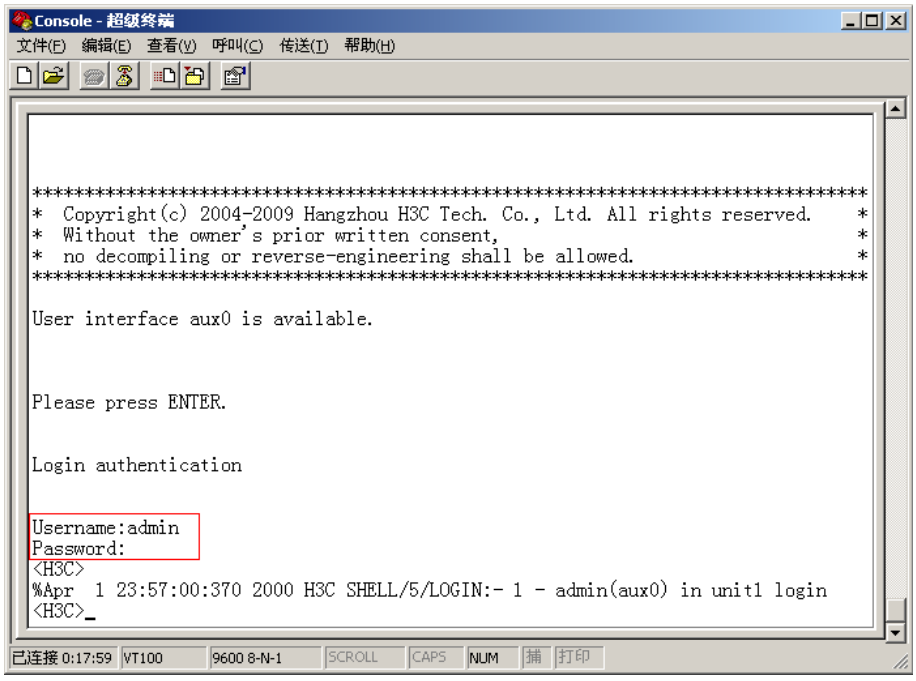
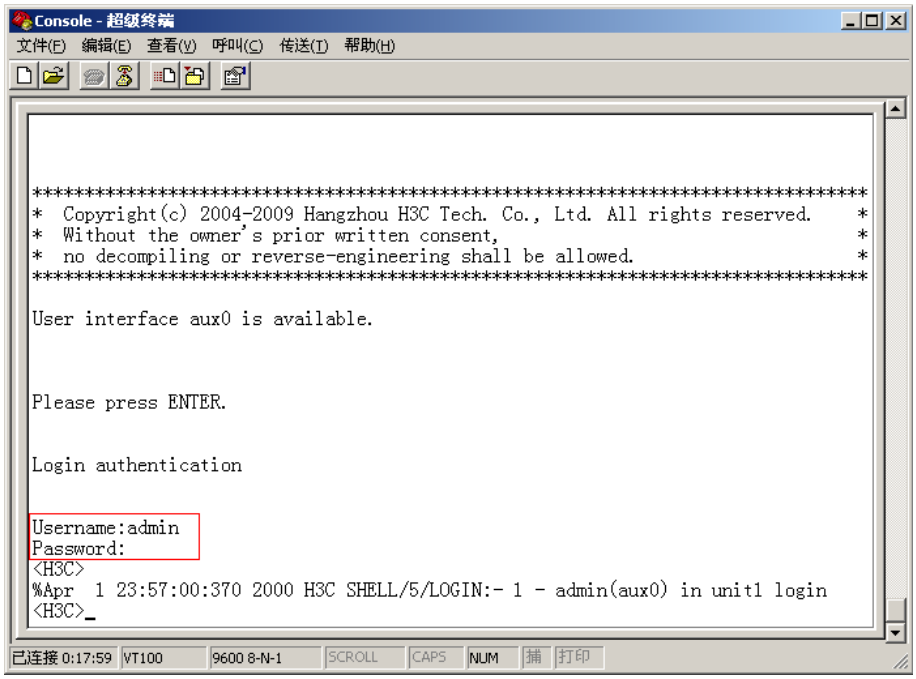


图3-8 用户通过 AUX 口登录设备时 AAA 认证登录界面



4. 配置Console口/AUX口登录方式的公共属性

提示

- 改变 Console 口/AUX 口属性后会立即生效，所以通过 Console 口/AUX 口登录来配置 Console 口/AUX 口属性可能在配置过程中发生连接中断，建议通过其它登录方式来配置 Console 口/AUX 口属性。
- 若用户需要通过 Console 口/AUX 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/AUX 口属性保持一致。否则，连接失败。

表3-6 配置 Console 口/AUX 口登录方式的公共属性

操作	命令	说明
进入系统视图	**system-view**	-
进入Console/AUX用户线视图	**line** { **aux** | **console** } *first-number* [*last-number*]	二者选其一

操作	命令	说明
进入Console/AUX用户线类视图	**line class** { **aux** | **console** }	• 用户线视图下的配置优先于用户线类视图下的配置 • 用户线视图下的配置只对该用户线生效且立即生效 • 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 • 用户线视图下的属性配置为缺省值时，将采用用户线类视图下配置的值。如果用户线类视图下的属性配置也为缺省值时，则直接采用该属性的缺省值
配置传输速率	**speed** *speed-value*	缺省情况下，Console口/AUX口使用的传输速率为9600bit/s 传输速率为设备与访问终端之间每秒钟传送的比特的个数 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，Console口/AUX口的校验方式为**none**，即不进行校验 用户线类视图下不支持该命令
配置停止位	**stopbits** { **1** | **1.5** | **2** }	缺省情况下，Console口/AUX口的停止位为1 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
配置数据位	**databits** { **5 | 6 | 7** | **8** }	缺省情况下，Console口/AUX口的数据位为8位 数据位的设置取决于需要传送的信息。比如，如果传送的是标准的ASCII码，则可以将数据位设置为7，如果传输的是扩展的ASCII码，则需要将数据位设置为8 用户线类视图下不支持该命令
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
检测停止位	**stopbit-error intolerance**	缺省情况下，不检测停止位 用户线类视图下不支持该命令
配置流量控制方式	**flow-control** { **hardware** | **none** | **software** } **flow-control hardware** *flow-control-type1* [**software** *flow-control-type2*] **flow-control software** *flow-control-type1* [**hardware** *flow-control-type2*]	用户线类视图下不支持该命令

操作	命令	说明
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 当设备的终端类型与客户端（如超级终端或者Telnet客户端等）的终端类型不一致，或者均设置为ANSI，并且当前编辑的命令行的总字符数超过80个字符时，客户端会出现光标错位、终端屏幕不能正常显示的现象。建议两端都设置为VT100类型
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 **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 **idle-timeout** 0表示永远不会超时
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 当配置自动执行的命令后，登录到终端线路，所配置的命令会自动执行*command*，然后退出当前连接 对于没有Console用户线，只有AUX用户线的设备，AUX用户线/AUX用户线类视图下不支持该命令 对于有Console用户线，又有AUX用户线的设备，Console用户线/Console用户线类视图下不支持该命令，AUX用户线/AUX用户线类视图下支持该命令
设置终端线路上禁止终端服务	**undo shell**	缺省情况下，在所有的终端线路上启动终端服务 对于没有Console用户线，只有AUX用户线的设备，AUX用户线视图下不支持该命令 对于有Console用户线，又有AUX用户线的设备，Console用户线视图下不支持该命令，AUX用户线视图下支持该命令

3.3 配置通过Telnet登录设备

设备可以作为Telnet服务器，以便用户能够Telnet登录到设备进行远程管理和监控。具体请参见“3.3.1 配置设备作为Telnet服务器”。

设备也可以作为Telnet客户端，Telnet到其它设备，对别的设备进行管理和监控。具体请参见“3.3.2 配置设备作为Telnet客户端登录其它设备”。

3.3.1 配置设备作为Telnet服务器

缺省情况下，设备的 Telnet 服务器功能处于关闭状态，通过 Telnet 方式登录设备的认证方式为password，但设备没有配置缺省的登录密码，即在缺省情况下用户不能通过 Telnet 登录到设备上。因此当使用 Telnet 方式登录设备前，首先需要通过 Console 口登录到设备上，开启 Telnet 服务器功能，然后对认证方式、用户角色及公共属性进行相应的配置，才能保证通过 Telnet 方式正常登录到设备。

1. 配置设备作为Telnet服务器的配置任务简介

表3-7 配置设备作为 Telnet 服务器的配置任务简介

配置任务		说明	详细配置
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）	必选 请根据实际需要选择其中的一种认证方式	3.3.1 2.
	配置Telnet登录设备时采用密码认证（password）		3.3.1 3.
	配置Telnet登录设备时采用AAA认证（scheme）		3.3.1 4.
配置Telnet登录同时在线的最大用户连接数		可选	3.3.1 5.
配置Telnet服务器发送报文的DSCP优先级		可选	3.3.1 6.
配置VTY用户线的公共属性		可选	3.3.1 7.

说明

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。

2. 配置Telnet登录设备时无需认证（none）

用户已经成功登录到了设备上，并希望以后通过 Telnet 登录设备时无需进行认证。

表3-8 认证方式为 none 的配置

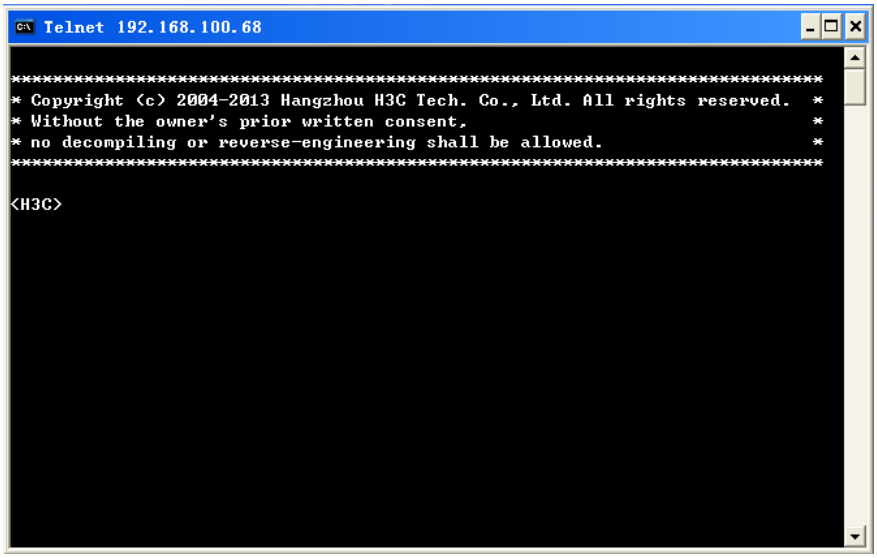
操作	命令	说明
进入系统视图	**system-view**	-
使能设备的Telnet服务	**telnet server enable**	缺省情况下，Telnet服务处于关闭状态
进入一个或多个VTY用户线视图	**line vty** *first-number* [*last-number*]	二者选其一 • 用户线视图下的配置优先于用户线类视图下的配置 • 用户线视图下的配置只对该用户线生效且立即生效 • 用户线类视图下的配置修改不会立即生效，当用户下次登录后所修改的配置值才会生效 • 用户线视图下的属性配置为缺省值时，将采用用户线类视图下配置的值。如果用户线类视图下的属性配置也为缺省值时，则直接采用该属性的缺省值
进入VTY用户线类视图	**line class vty**	
设置VTY登录用户的认证方式为不认证	**authentication-mode none**	缺省情况下，VTY用户线的认证方式为password 用户线视图下，对**authentication-mode**和**protocol inbound**进行关联绑定，当两条命令中的任意一条配置了非缺省值，那么另外一条取缺省值

操作	命令	说明
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

配置完成后，当用户再次通过 Telnet 登录设备时：

- 设备会显示如 图 3-9 所示的登录界面。
- 如果出现“All user interfaces are used, please try later!”的提示，表示当前 Telnet 到设备的用户过多，则请稍候再连接。

图3-9 用户通过 Telnet 登录设备时无需认证登录界面



3. 配置Telnet登录设备时采用密码认证（password）

用户已经成功登录到了设备上，并希望以后通过 Telnet 登录设备时需要进行密码认证。

表3-9 认证方式为 password 的配置

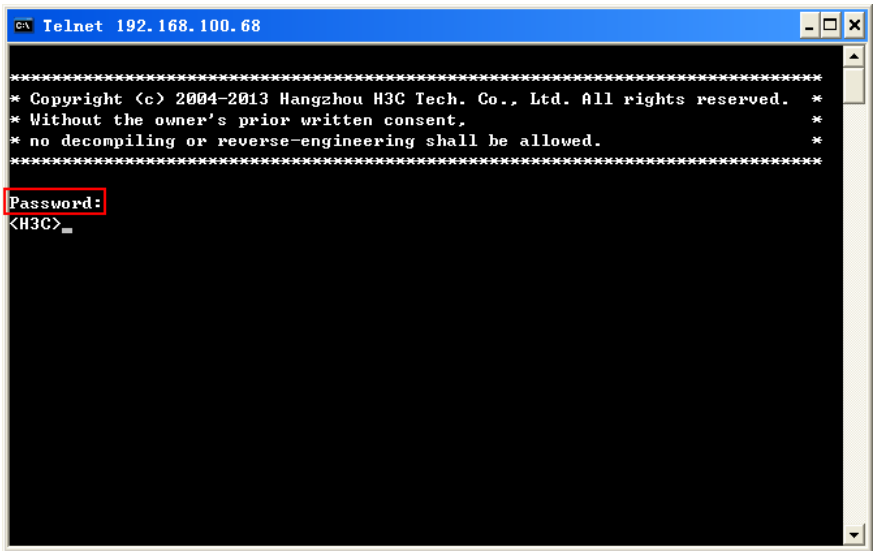
操作	命令	说明
进入系统视图	**system-view**	-
使能设备的Telnet服务	**telnet server enable**	缺省情况下，Telnet服务处于关闭状态
进入一个或多个VTY用户线视图	**line vty** *first-number* [*last-number*]	二者选其一

操作	命令	说明
进入VTY用户线类视图	**line class vty**	• 用户线视图下的配置优先于用户线类视图下的配置 • 用户线视图下的配置只对该用户线生效且立即生效 • 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 • 用户线视图下的属性配置为缺省值时，将采用用户线类视图下配置的值。如果用户线类视图下的属性配置也为缺省值时，则直接采用该属性的缺省值
设置登录用户的认证方式为密码认证	**authentication-mode password**	缺省情况下，VTY用户线的认证方式为password 用户线视图下，对**authentication-mode**和**protocol inbound**进行关联绑定，当两条命令中的任意一条配置了非缺省值，那么另外一条取缺省值
设置本地认证的密码	**set authentication password** { **hash** | **simple** } *password*	缺省情况下，没有设置本地认证的密码
（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

配置完成后，当用户再次通过 Telnet 登录设备时：

- 设备将要求用户输入登录密码，正确输入登录密码并回车，登录界面中出现命令行提示符（如<H3C>），如 图 3-10 所示。
- 如果出现“All user interfaces are used, please try later!”的提示，表示当前 Telnet 到设备的用户过多，则请稍候再连接。

图3-10 配置用户通过 Telnet 登录设备时采用密码认证登录界面



4. 配置Telnet登录设备时采用AAA认证（scheme）

用户已经成功登录到了设备上，并希望以后通过 Telnet 登录设备时需要进行 AAA 认证。

要使配置的 AAA 认证方式生效，还需要在 ISP 域视图下配置 login 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。相关详细介绍请参见“安全配置指导”中的“AAA”。

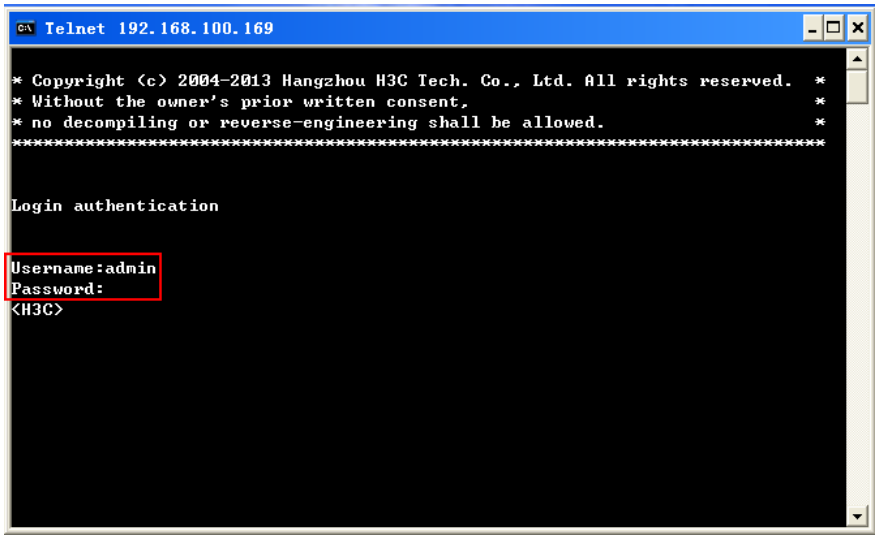
表3-10 配置用户通过 Telnet 登录设备时采用 AAA 认证

操作	命令	说明
进入系统视图	**system-view**	-
使能设备的Telnet服务	**telnet server enable**	缺省情况下，Telnet服务处于关闭状态
进入一个或多个VTY用户线视图	**line vty** *first-number* [*last-number*]	二者选其一 • 用户线视图下的配置优先于用户线类视图下的配置 • 用户线视图下的配置只对该用户线生效且立即生效 • 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 • 用户线视图下的属性配置为缺省值时，将采用用户线类视图下配置的值。如果用户线类视图下的属性配置也为缺省值时，则直接采用该属性的缺省值
进入VTY用户线类视图	**line class vty**	
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，VTY用户线的认证方式为password 用户线视图下，对**authentication-mode**和**protocol inbound**进行关联绑定，当两条命令中的任意一条配置了非缺省值，那么另外一条取缺省值

配置完成后，当用户再次通过 Telnet 登录设备时：

- 设备将要求用户输入登录用户名和密码，正确输入用户名（此处以用户为admin为例）和密码并回车，登录界面中出现命令行提示符（如<H3C>），如 图 3-11 所示。
- 如果出现“All lines are used, please try later!”的提示，表示当前 Telnet 到设备的用户过多，则请稍候再连接。

图3-11 用户通过 Telnet 登录设备时 AAA 认证登录界面



5. 配置Telnet登录同时在线的最大用户连接数

通过配置同时在线的最大用户连接数，可以限制采用 Telnet 登录同时接入设备的在线用户数。该配置对于通过任何一种认证方式（none、password 或者 sheme）接入设备的用户都生效。

表3-11 配置同时在线的最大用户连接数

操作	命令	说明
进入系统视图	**system-view**	-
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”

6. 配置Telnet服务器发送报文的DSCP优先级

DSCP 携带在 IP/IPv6 报文的 ToS/Trafic class 字段，用来体现报文自身的优先等级，决定报文传输的优先程度。

表3-12 配置 Telnet 服务器发送报文的 DSCP 优先级

操作	命令	说明
进入系统视图	**system-view**	-
配置Telnet服务器发送报文的DSCP优先级	**telnet server dscp** *dscp-value*	二者选其一 缺省情况下，Telnet/IPv6 Telnet服务器发送Telnet/IPv6 Telnet报文的DSCP优先级48
	telnet server ipv6 dscp *dscp-value*	

7. 配置VTY用户线的公共属性

提示

- 使用 **auto-execute command** 命令后，将导致用户通过该用户线登录后，不能对设备进行常规配置，需谨慎使用。
- 在配置 **auto-execute command** 命令并退出登录之前，要确保可以通过其它 VTY、AUX 用户登录进来更改配置，以便出现问题后，能删除该配置。

表3-13 配置 VTY 用户线的公共属性

操作	命令	说明
进入系统视图	**system-view**	-
进入一个或多个VTY用户线视图	**line vty** *first-number* [*last-number*]	二者选其一 • 用户线视图下的配置优先于用户线类视图下的配置 • 用户线视图下的配置只对该用户线生效且立即生效 • 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 • 用户线视图下的属性配置为缺省值时，将采用用户线类视图下配置的值。如果用户线类视图下的属性配置也为缺省值时，则直接采用该属性的缺省值
进入VTY用户线类视图	**line class vty**	
启动终端服务	**shell**	缺省情况下，在所有的用户线上启动终端服务
配置VTY用户线支持的协议	**protocol inbound** { **all** | **pad** | **ssh** | **telnet** }	缺省情况下，设备同时支持Telnet和SSH协议 使用该命令配置的协议将在用户下次使用该用户线登录时生效 用户线视图下，对**authentication-mode**和**protocol inbound**进行关联绑定，当两条命令中的任意一条配置了非缺省值，那么另外一条取缺省值
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 **screen-length** 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

操作	命令	说明
设置VTY用户线的超时时间	**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 **idle-timeout** 0表示永远不会超时
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，未设定自动执行命令 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。如果这条命令引发起了一个任务，系统会等这个任务执行完毕后再断开连接。该命令通常用来配置Telnet命令，使用户登录时自动连接到指定的主机

3.3.2 配置设备作为Telnet客户端登录其它设备

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 3-12 所示。

先给设备配置 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，请配置路由使得两台设备间路由可达。

图3-12 通过设备登录到其它设备

表3-14 设备作为 Telnet 客户端登录到 Telnet 服务器的配置

操作	命令	说明
进入系统视图	**system-view**	-
（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，没有指定发送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
退回到用户视图	**quit**	-
设备作为Telnet客户端登录到Telnet服务器	**telnet** *remote-host* [*service-port*] [**vpn-instance** *vpn-instance-name*] [**source** { **interface** *interface-type interface-number* | **ip** *ip-address* }] [**dscp** *dscp-value*]	二者选其一 此命令在用户视图下执行
	telnet ipv6 *remote-host* [**-i** *interface-type interface-number*] [*port-number*] [**vpn-instance** *vpn-instance-name*] [**dscp** *dscp-value*]	

3.4 配置通过SSH登录设备

3.4.1 通过SSH登录设备简介

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，以便用户能够使用SSH协议登录到设备进行远程管理和监控。具体请参见“3.4.2 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。具体请参见“3.4.3 配置设备作为SSH客户端登录其它设备”。

3.4.2 配置设备作为SSH服务器

缺省情况下，设备的 SSH Server 功能处于关闭状态，因此当使用 SSH 方式登录设备前，首先需要通过 Console 口登录到设备上，开启设备的 SSH 服务器功能、对认证方式及其它属性进行相应的配置，才能保证通过 SSH 方式正常登录到设备。

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”。

表3-15 设备作为 SSH 服务器时的配置

操作	命令	说明
进入系统视图	**system-view**	-
生成本地密钥对	**public-key local create** { **dsa** | **rsa** | **ecdsa** } [**name** *key-name*]	缺省情况下，没有生成密钥对
使能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
（可选）建立SSH用户，并指定SSH用户的认证方式	非FIPS模式下： **ssh user** *username* **service-type stelnet authentication-type** { **password** | { **any** | **password-publickey** | **publickey** } **assign publickey** *keyname* } FIPS模式下： **ssh user** *username* **service-type stelnet authentication-type** { **password** | **password-publickey** **assign publickey** *keyname* }	缺省情况下，不存在任何SSH用户
进入VTY用户线视图	**line vty** *first-number* [*last-number*]	二者选其一

操作	命令	说明
进入VTY用户线类视图	**line class vty**	• 用户线视图下的配置优先于用户线类视图下的配置 • 用户线视图下的配置只对该用户线生效且立即生效 • 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 • 用户线视图下的属性配置为缺省值时，将采用用户线类视图下配置的值。如果用户线类视图下的属性配置也为缺省值时，则直接采用该属性的缺省值
配置登录用户线的认证方式为**scheme**方式	**authentication-mode scheme**	非FIPS模式下：缺省情况下，VTY用户线认证为**password**方式 FIPS模式下：缺省情况下，VTY用户线认证为**scheme**方式 用户线视图下，对**authentication-mode**和**protocol inbound**进行关联绑定，当两条命令中的任意一条配置了非缺省值，那么另外一条取缺省值
（可选）配置VTY用户线支持的SSH协议	非FIPS模式下： **protocol inbound { all | pad | ssh | telnet }** FIPS模式下： **protocol inbound ssh**	非FIPS模式下：缺省情况下，设备同时支持Telnet和SSH协议 FIPS模式下：缺省情况下，设备支持SSH协议 使用该命令配置的协议将在用户下次使用该用户线登录时生效 用户线视图下，对**authentication-mode**和**protocol inbound**进行关联绑定，当两条命令中的任意一条配置了非缺省值，那么另外一条取缺省值
（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”
退回系统视图	**quit**	-
（可选）配置VTY用户线的公共属性	**-**	详细配置请参见“3.3.1 7. 配置VTY用户线的公共属性”

3.4.3 配置设备作为SSH客户端登录其它设备

用户已经成功登录到了设备上，并希望将当前设备作为SSH客户端登录到其它设备上进行操作，如图 3-12 所示。

先给设备配置 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。

图3-13 通过设备登录到其它设备

表3-16 设备作为 SSH 客户端登录到其它设备的配置

操作	命令	说明
设备作为SSH客户端登录到SSH IPv4服务器	**ssh2** *server*	此命令在用户视图下执行
设备作为SSH客户端登录到SSH IPv6服务器	**ssh2 ipv6** *server*	此命令在用户视图下执行

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它配置，具体请参见“安全配置指导”中的“SSH”。

3.5 配置通过Modem登录设备

网络管理员可以通过设备的 AUX 口，利用一对 Modem 和 PSTN（Public Switched Telephone Network，公共电话交换网）拨号登录到设备上，对远程设备进行管理和维护。这种登录方式一般适用于在网络中断的情况下，利用 PSTN 网络对设备进行远程管理、维护及故障定位。

通过AUX口利用Modem拨号进行远程登录时，使用的是AUX用户线。缺省情况下，通过Modem登录使用password认证方式。需要先通过Console口或其它方式登录到设备上，配置Modem登录password认证方式的密码，或者更改认证方式并完成相关参数的设置，才可以通过Modem登录设备。具体配置同“3.2 配置通过Console口/AUX口本地登录设备”，但需要注意的是：

- AUX 口（Console 口）波特率 Speed 要低于 Modem 的传输速率，否则可能会出现丢包现象。
- AUX 口（Console 口）的其它属性（AUX 口（Console 口）校验方式、AUX 口（Console 口）的停止位、AUX 的数据位）均采用缺省值。
- AUX 口连接 Modem 用于 Modem 登录时，在 AUX 用户线视图下，还可以配置一些 **modem** 命令来管理 Modem 登录用户，具体配置步骤请参见“二层技术－广域网接入”中的“Modem 管理”。

请参照以下步骤来建立 Modem 连接：

(1) 如 图 3-14 所示，建立远程配置环境，在PC机（或终端）的串口和设备的AUX口分别挂接Modem。

图3-14 搭建远程配置环境

(2) 获取远程设备端 AUX 口（Console 口）所连 Modem 上对应的电话号码。

(3) 在与设备直接相连的 Modem 上进行以下配置。

```
AT&F------------------------- Modem 恢复出厂配置
ATS0=1----------------------- 配置自动应答（振铃一声）
AT&D------------------------- 忽略 DTR 信号
AT&K0------------------------ 禁止流量控制
AT&R1------------------------ 忽略 RTS 信号
AT&S0------------------------ 强制 DSR 为高电平
ATEQ1&W---------------------- 禁止 modem 回送命令响应和执行结果并存储配置
```

在配置后为了查看 Modem 的配置是否正确，可以输入 AT&V 命令显示配置的结果。

说明

各种 Modem 配置命令及显示的结果有可能不一样，具体操作请参照 Modem 的说明书进行。

(4) 在PC机上运行终端仿真程序（如Windows XP/Windows 2000 的超级终端等，以下配置以Windows XP为例），新建一个拨号连接（所拨号码为与设备相连的Modem的电话号码），与设备建立连接，如 图 3-15 至 图 3-17 所示。

说明

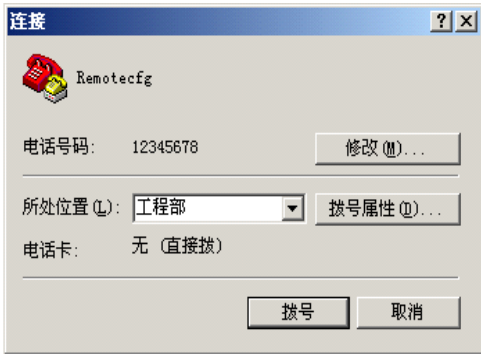
如果 PC 使用的是 Windows 2003 Server 操作系统，请在 Windows 组件中添加超级终端程序后，再按照本文介绍的方式登录和管理设备；如果 PC 使用的是 Windows 2008 Server、Windows 7 、Windows Vista 或其他操作系统，请您准备第三方的拨号控制软件，使用方法请参照软件的使用指导或联机帮助。

(5) 在远端通过终端仿真程序和 Modem 向设备拨号。

图3-15 新建连接

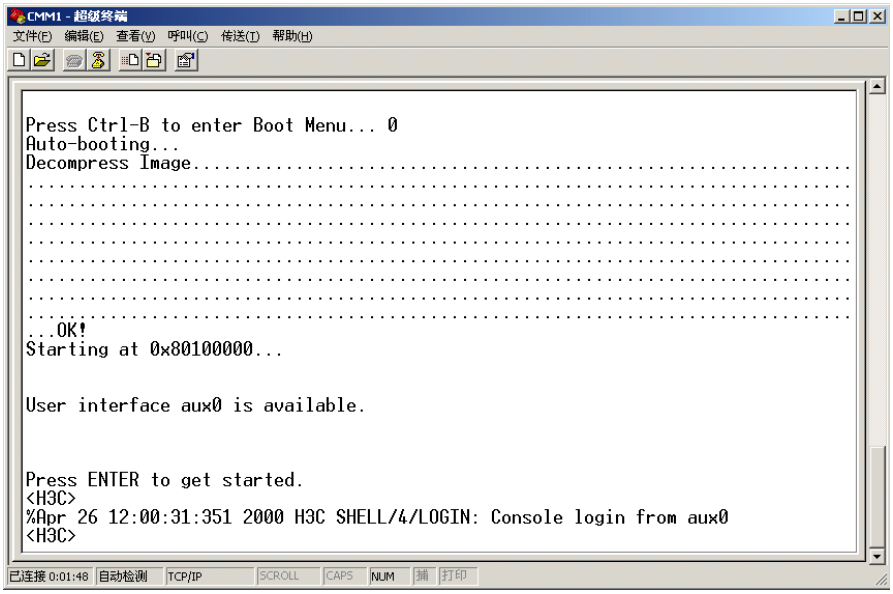
图3-16 拨号号码配置

图3-17 在远端 PC 机上拨号



(6) 当听到拨号音后，如果AUX用户线的认证方式为none，则在超级终端上键入回车键之后将出现命令行提示符（如<H3C>），如 图 3-18 所示。如果AUX用户线的认证方式为password或scheme，则在超级终端上需键入合法的用户名/密码之后才会出现命令行提示符。

图3-18 AUX 登录界面



说明

- 当您想断开 PC 与远端设备的连接时，首先在超级终端中用“ATH”命令断开 modem 间的连接。如果在超级终端窗口无法输入此命令，可输入“AT+++”并回车，待窗口显示“OK”提示后再输入“ATH”命令，屏幕再次显示“OK”提示，表示已断开本次连接。您也可以使用超级终端页面提供的挂断按扭  断开 PC 与远端设备的连接。
- 当您使用完超级终端仿真程序后，务必要先断开 PC 与远端设备的连接，不能直接关闭超级终端，否则有些型号的远程 modem 将一直在线，下次拨号连接时将无法拨号成功。

3.6 配置通过重定向服务器登录设备

用户能够通过Telnet方式登录到路由器，路由器通过异步串口连接到目的设备的Console口（AUX口）。当目的设备需要向用户提供Telnet服务，但又不方便告知用户自身的IP地址时，可以将路由器作为重定向服务器。在路由器的AUX/TTY用户线视图下使能Telnet重定向功能，用户执行“telnet 重定向服务器的IP地址 特定端口号”能够直接登录到目的设备，用户所看到的配置界面就是目的设备的，配置对目的设备生效。其典型组网图如 图 3-19 所示。

说明

- 异步接口包括专用异步串口（Async 接口）或者工作在异步模式下的同/异步串口（Serial 接口）。
- 目的设备通过 AUX 口与重定向服务器相连，则必须先通过 Console 口登录到设备后，将 AUX 用户线视图下的认证方式设置为无需认证，再重新连接。
- 仅支持一个用户终端通过重定向服务器登录目的设备。

图3-19 通过重定向服务器登录设备

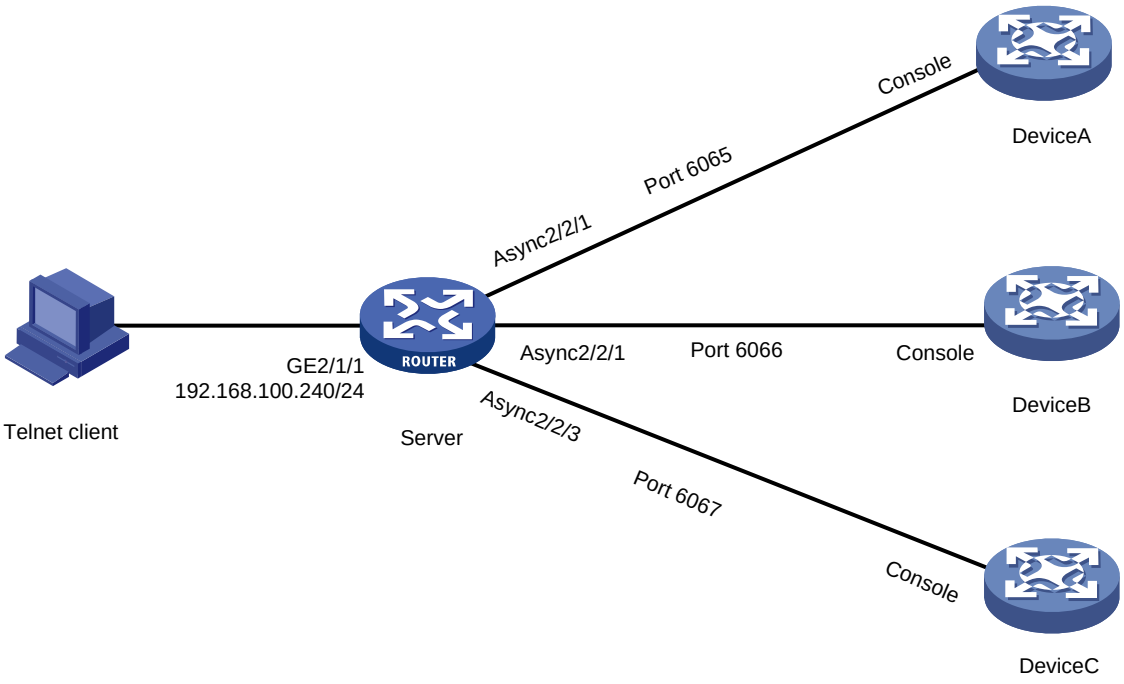


表3-17 路由器作为重定向服务器的配置

操作		命令	说明
进入系统视图		**system-view**	-
进入指定同/异步串口或者异步串口的视图	同/异步串口	**interface serial** *interface-number*	在使用同/异步串口时，需配置其工作在异步模式下，并使用转接器连接到目的设备
		physical-mode async	
	异步串口	**interface async** *interface-number*	
设置异步串口工作在流模式		**async-mode flow**	缺省情况下，异步串口工作在协议模式（**protocol**）
（可选）关闭电平检测功能		**undo detect dsr-dtr**	缺省情况下，电平检测功能处于开启状态 此命令是否需要配置，与对端设备有关，请以实际情况为准

操作	命令	说明
退出接口视图	**quit**	-
进入AUX/TTY用户线视图	**line** { *first-number1* [*last-number1*] | { **aux** | **tty** } *first-number2* [*last-number2*] }	-
设置终端线路上禁止终端服务	**undo shell**	缺省情况下，系统在所有的用户线上启动终端服务
（可选）设置用户线的传输速率	**speed** *speed-value*	缺省情况下，用户线的传输速率为9600bps 重定向服务器与目的设备相连端口对应的用户线的传输速率必须相同，否则重定向将失败
（可选）检测停止位	**stopbit-error intolerance**	缺省情况下，不检测停止位
（可选）设置停止位的个数	**stopbits** { **1** | **1.5** | **2** }	缺省情况下，停止位为1比特 重定向服务器与目的设备相连端口对应的用户线的停止位设置必须相同，否则重定向将失败。可以在重定向前，使用**stopbit-error intolerance**命令检测重定向设备与目的设备的停止位设置是否相同
使能Telnet重定向功能	**redirect enable**	缺省情况下，异步串口重定向功能处于关闭状态
（可选）设置Telnet重定向的监听端口	**redirect listen-port** *port-number*	缺省情况下，Telnet重定向的监听端口号为用户界面的绝对编号加2000
（可选）设置Telnet重定向时对数据不进行任何处理直接转发	**redirect passthrough**	缺省情况下，在建立Telnet重定向连接后，将对数据按照Telnet协议规定处理
（可选）设置Telnet重定向连接空闲超时时间	**redirect timeout** *time*	缺省情况下，设备Telnet重定向的空闲超时时间为360秒
（可选）设置在建立Telnet重定向连接时不进行Telnet选项协商	**redirect refuse-negotiation**	缺省情况下，在建立Telnet重定向连接时，将进行Telnet选项协商
（可选）强制断开已经建立的Telnet重定向连接	**redirect disconnect**	-
退回系统视图	**quit**	-
（可选）设置建立Telnet重定向监听端口与IP地址的对应关系	**ip alias** *ip-address port-number*	缺省情况下，Telnet重定向监听端口与IP地址没有对应关系

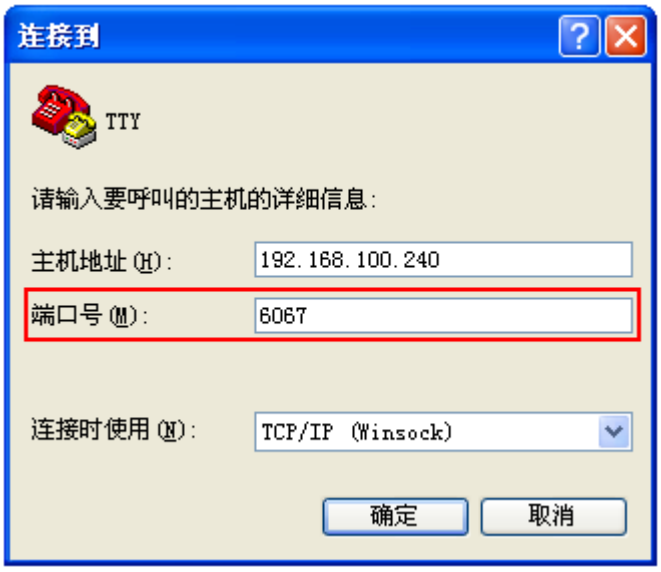
如 图 3-19 所示，当用户通过重定向服务器登录到Device C时，请按以下步骤操作：

(1) 在 PC 机上运行终端仿真程序（如 Windows XP/Windows 2000 的超级终端等，以下配置以 Windows XP 为例），新建一个连接。

图3-20 新建连接

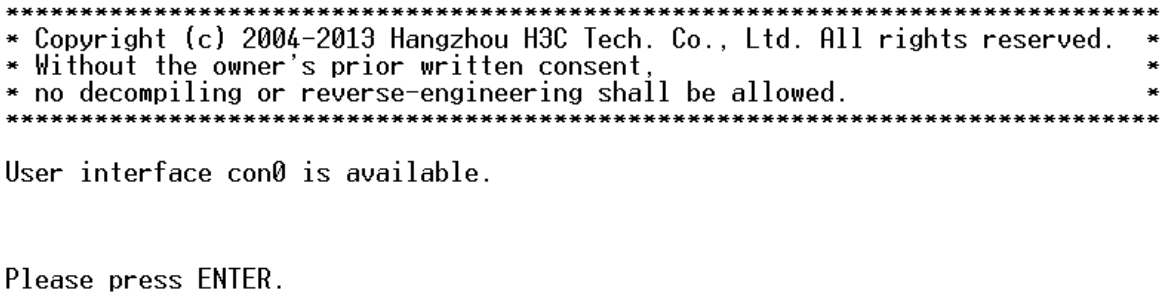
(2) 配置连接参数，串口服务器的地址 192.168.100.240，端口号要改成Telnet重定向监听的端口号 6067，连接时使用选择TCP/IP连接方式，和 图 3-21 所示，点击确定。

图3-21 配置连接参数



(3) 进入登录设备界面，按回车键之后将出现命令行提示符（如<H3C>）。

图3-22 用户通过重定向服务器登录设备界面



3.7 CLI登录显示和维护

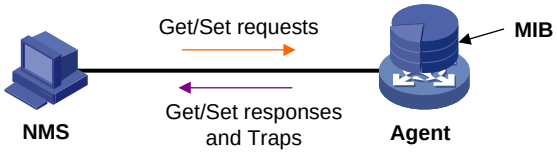
表3-18 CLI 显示和维护

操作	命令	说明
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
显示用户线的相关信息	**display line** [*num1* | { **aux** | **console** | **tty** | **vty** } *num2*] [**summary**]	在任意视图下执行 **console**参数仅MSR 5600支持
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
释放指定的用户线	**free line** { *num1* | { **aux** | **console** | **tty** | **vty** } *num2* }	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，其它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它用户干扰时，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 **console**参数仅MSR 5600支持
锁住当前用户线，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，系统不会自动锁住当前用户线 FIPS模式下，不支持此命令
向指定的用户线发送消息	**send** { **all** | *num1* | { **aux** | **console** | **tty** | **vty** } *num2* }	在用户视图下执行 **console**参数仅MSR 5600支持

4 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 4-1 所示。设备支持多种NMS软件，如iMC等。

图4-1 通过 SNMP 登录设备组网图



缺省情况下，用户不能通过NMS登录到设备上，如果要使用NMS登录设备，首先需要通过Console口登录到设备上，在设备上进行相关配置。设备支持SNMPv1、SNMPv2c和SNMPv3 三种版本，只有NMS和Agent使用的SNMP版本相同，NMS才能和Agent建立连接。请根据使用的SNMP版本选择对应的配置步骤，见 表 4-1 或 表 4-2。配置完成后，即可使用NMS网管的方式登录设备。关于SNMP的详细介绍及配置，请参见“网络管理和监控配置指导”中的“SNMP”。

表4-1 配置 SNMP 基本参数（SNMPv3 版本）

操作	命令	说明
进入系统视图	**system-view**	-
启动SNMP Agent服务	**snmp-agent**	缺省情况下，SNMP Agent服务处于关闭状态
启用SNMPv3版本	**snmp-agent sys-info version v3**	缺省情况下，系统启用的SNMP版本号为“SNMPv3”
（可选）创建MIB视图或更新MIB视图内容	**snmp-agent mib-view** { **excluded** | **included** } *view-name oid-tree* [**mask** *mask-value*]	缺省情况下，设备上已创建了四个视图，视图名均为ViewDefault： • 视图一包含 MIB 子树 iso • 视图二不包含子树 snmpUsmMIB • 视图三不包含子树 snmpVacmMIB • 视图四不包含子树 snmpModules.18
创建SNMPv3组	**snmp-agent group v3** *group-name* [**authentication** | **privacy**] [**read-view** *view-name*] [**write-view** *view-name*] [**notify-view** *view-name*] [**acl** *acl-number* | **acl ipv6** *ipv6-acl-number*] *	缺省情况下，设备上没有配置SNMP组

操作	命令	说明
创建SNMPv3用户	**snmp-agent usm-user v3** *user-name group-name* [**remote** { *ip-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*]] [{ **cipher** | **simple** } **authentication-mode** { **md5** | **sha** } *auth-password* [**privacy-mode** { **aes128** | **des56** } *priv-password*]] [**acl** *acl-number* | **acl ipv6** *ipv6-acl-number*] *	当设备需要向目的主机发送SNMPv3 Inform信息时，**remote** *ip-address*参数必选

表4-2 配置 SNMP 基本参数（SNMPv1 版本、SNMPv2c 版本）

操作			命令	说明
进入系统视图			**system-view**	-
启动SNMP Agent服务			**snmp-agent**	缺省情况下，SNMP Agent服务处于关闭状态
启用SNMPv1/v2c版本			**snmp-agent sys-info version** { **all** | { **v1** | **v2c** } *}	缺省情况下，系统启用的SNMP版本号为“SNMPv3”
（可选）创建MIB视图或更新MIB视图内容			**snmp-agent mib-view** { **excluded** | **included** } *view-name oid-tree* [**mask** *mask-value*]	缺省情况下，设备上已创建了四个视图，视图名均为ViewDefault： • 视图一包含 MIB 子树 iso • 视图二不包含子树 snmpUsmMIB • 视图三不包含子树 snmpVacmMIB • 视图四不包含子树 snmpModules.18
设置访问权限	直接设置	创建一个新的SNMP团体	**snmp-agent community** { **read** | **write** } *community-name* [**mib-view** *view-name*] [**acl** *acl-number* | **acl ipv6** *ipv6-acl-number*] *	二者选其一 直接设置是以SNMPv1和SNMPv2c版本的团体名进行设置 间接设置采用与SNMPv3版本一致的命令形式，添加的用户到指定的组，即相当于SNMPv1和SNMPv2c版本的团体名，在NMS上配置的团体名需要跟Agent上配置的用户名一致
	间接设置	设置一个SNMP组	**snmp-agent group** { **v1** | **v2c** } *group-name* [**read-view** *view-name*] [**write-view** *view-name*] [**notify-view** *view-name*] [**acl** *acl-number* | **acl ipv6** *ipv6-acl-number*] *	
		为一个SNMP组添加一个新用户	**snmp-agent usm-user** { **v1** | **v2c** } *user-name group-name* [**acl** *acl-number* | **acl ipv6** *ipv6-acl-number*] *	

5 对登录用户的控制

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，其它用户不允许访问设备，以免非法用户使用 Telnet/SSH 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。

5.1 配置对Telnet/SSH用户的控制

5.1.1 配置准备

确定了对 Telnet/SSH 的控制策略，包括对哪些源 IP、目的 IP、源 MAC 等参数进行控制，控制的动作是允许访问还是拒绝访问，即配置好 ACL。

5.1.2 配置对Telnet/SSH用户的控制

表5-1 配置对 Telnet 用户的控制

操作	命令	说明
进入系统视图	**system-view**	-
使用ACL限制哪些Telnet客户端可以访问设备	**telnet server acl** *acl-number*	请根据需要选择 缺省情况下，没有使用ACL限制Telnet客户端
	telnet server ipv6 acl [**ipv6**] *acl-number*	

表5-2 配置对 SSH 用户的控制

操作	命令	说明
进入系统视图	**system-view**	-
使用ACL限制哪些SSH客户端可以访问设备	**ssh server acl** *acl-number*	请根据需要选择 缺省情况下，没有使用ACL限制SSH客户端 **ssh server acl**和**ssh server ipv6 acl**命令的详细介绍请参见“安全命令参考”中的“SSH”
	ssh server ipv6 acl [**ipv6**] *acl-number*	

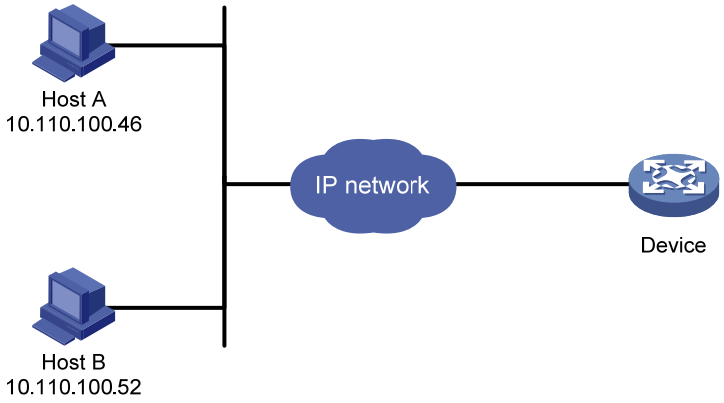
5.1.3 配置举例

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5-1 使用 ACL 对 Telnet 用户进行控制



3. 配置步骤

定义 ACL。

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

5.2 配置对NMS的控制

5.2.1 配置准备

确定了对 NMS 的控制策略，包括对哪些源 IP 进行控制，控制的动作是允许访问还是拒绝访问，即配置好 ACL。

5.2.2 配置对NMS的控制

表5-3 配置对 NMS 的控制

操作	命令	说明
进入系统视图	**system-view**	-
在配置SNMP团体名的命令中引用ACL	**snmp-agent community** { **read** | **write** } *community-name* [**mib-view** *view-name*] [**acl** *acl-number* | **acl ipv6** ipv6-*acl-number*] *	根据网管用户运行的SNMP版本及配置习惯，可以在团体名、组

操作	命令	说明
在配置SNMPv1/SNMPv2c组名的命令中引用ACL	**snmp-agent group** { **v1** | **v2c** } *group-name* [**read-view** *view-name*] [**write-view** *view-name*] [**notify-view** *view-name*] [**acl** *acl-number* | **acl ipv6** *ipv6-acl-number*] *	名或者用户名配置时引用访问控制列表，详细介绍请参见“网络管理和监控配置指导”中的“SNMP”
在配置SNMPv3组名的命令中引用ACL	**snmp-agent group v3** *group-name* [**authentication** | **privacy**] [**read-view** *view-name*] [**write-view** *view-name*] [**notify-view** *view-name*] [**acl** *acl-number* | **acl ipv6** *ipv6-acl-number*] *	
在配置SNMPv1/SNMPv2c用户名的命令中引用ACL	**snmp-agent usm-user** { **v1** | **v2c** } *user-name group-name* [**acl** *acl-number* | **acl ipv6** *ipv6-acl-number*] *	
在配置SNMPv3用户名的命令中引用ACL	**snmp-agent usm-user v3** *user-name group-name* [**remote** { *ip-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*]] [{ **cipher** | **simple** } **authentication-mode** { **md5** | **sha** } *auth-password* [**privacy-mode** { **aes128** | **des56** } *priv-password*]] [**acl** *acl-number* | **acl ipv6** *ipv6-acl-number*] *	

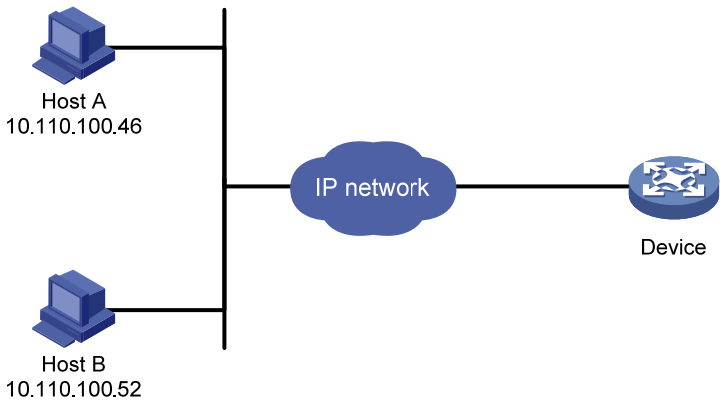
5.2.3 配置举例

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5-2 使用 ACL 对 NMS 进行控制



3. 配置步骤

定义基本 ACL。

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

5.3 配置命令行授权功能

5.3.1 配置步骤

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。

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”。

表5-4 配置命令行授权功能

操作	命令	说明
进入系统视图	**system-view**	-
进入用户线视图	**line** { *first-number1* [*last-number1*] | { **aux** | **console** | **tty** | **vty** } *first-number2* [*last-number2*] }	二者选其一 • 用户线视图下的配置优先于用户线类视图下的配置 • 用户线视图下的配置只对该用户线生效且立即生效 • 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 • 用户线视图下的属性配置为缺省值时，将采用用户线类视图下配置的值。如果用户线类视图下的属性配置也为缺省值时，则直接采用该属性的缺省值
进入用户线类视图	**line class** { **aux** | **console** | **tty** | **vty** }	
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，用户通过Console口登录，认证方式为none（即不需要进行认证）；用户通过AUX口登录，认证方式为password（即需要进行密码认证） 如果设备上只有一个AUX口，而没有Console口（Console口与AUX口共用），则使用AUX用户线登录的用户不需要认证 用户线视图下，对**authentication-mode**和**protocol inbound**进行关联绑定，当两条命令中的任意一条配置了非缺省值，那么另外一条取缺省值
使能命令行授权功能	**command authorization**	缺省情况下，没有使能命令行授权功能，即用户登录后执行命令行不需要授权 如果用户类视图下使能了命令行授权功能，则该类型用户线视图都使能命令行授权功能，并且在该类型用户线视图下将无法禁用命令行授权功能

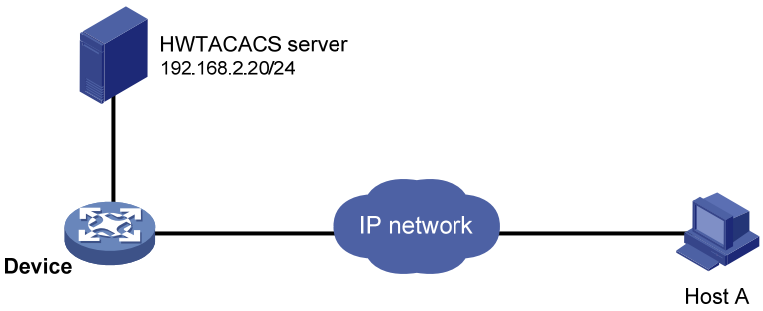
5.3.2 配置举例

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5-3 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，以便用户访问。

```
<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 63
[Device-line-vty0-63] authentication-mode scheme
```

使能命令行授权功能，限制用户只能使用授权成功的命令。

```
[Device-line-vty0-63] command authorization
[Device-line-vty0-63] 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 expert
[Device-hwtacacs-tac] key authorization 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 123，可使用的服务类型为 telnet，用户角色为 level-1。

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

5.4 配置命令行计费功能

5.4.1 配置步骤

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。

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”。

表5-5 配置命令行计费功能

操作	命令	说明
进入系统视图	**system-view**	-
进入用户线视图	**line** { *first-number1* [*last-number1*] | { **aux** | **console** | **tty** | **vty** } *first-number2* [*last-number2*] }	二者选其一 • 用户线视图下的配置优先于用户线类视图下的配置 • 用户线视图下的配置只对该用户线生效且立即生效
进入用户线类视图	**line class** { **aux** | **console** | **tty** | **vty** }	• 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 • 用户线视图下的属性配置为缺省值时，将采用用户线类视图下配置的值。如果用户线类视图下的属性配置也为缺省值时，则直接采用该属性的缺省值
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，用户通过Console口登录，认证方式为none（即不需要进行认证）；用户通过AUX口登录，认证方式为password（即需要进行密码认证） 如果设备上只有一个AUX口，而没有Console口（Console口与AUX口共用），则使用AUX用户线登录的用户不需要认证 用户线视图下，对**authentication-mode**和**protocol inbound**进行关联绑定，当两条命令中的任意一条配置了非缺省值，那么另外一条取缺省值
使能命令行计费功能	**command accounting**	缺省情况下，没有使能命令行计费功能，即计费服务器不会记录用户执行的命令行

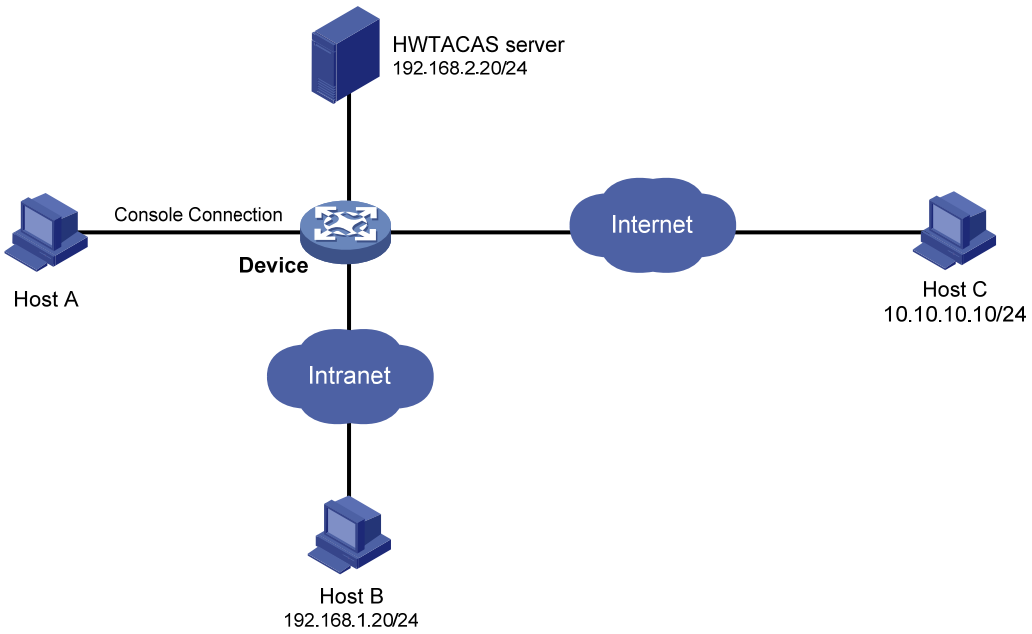
5.4.2 配置举例

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5-4 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，以便用户访问。

```
<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 console 0
[Device-line-console0] command accounting
[Device-line-console0] 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 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

说明

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

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。FTP 协议基本操作在 RFC 959 中进行了描述。

FTP 有两种文件传输模式：

- 二进制模式，用于传输程序文件（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）。

缺省情况下，FTP 服务器传输模式为 ASCII 码模式。

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。

设备可以作为 FTP 服务器，也可以作为 FTP 客户端。

图1-1 FTP 组网应用示意图

提示

在建立 FTP 连接前请确保 FTP 服务器与 FTP 客户端之间路由可达，否则，连接建立失败。

1.2 配置FTP服务器

当设备作为 FTP 服务器时，至少要开启 FTP 服务器功能，并配置 FTP 服务器的认证和授权，其它命令请根据需要选择配置。

1.2.1 FTP服务器的基本配置

表1-1 配置 FTP 服务器

操作	命令	说明
进入系统视图	**system-view**	-
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
（可选）使用ACL（Access Control List，访问控制列表）限制哪些FTP客户端可以访问设备	**ftp server acl** { *acl-number* | **ipv6** *acl-number6* }	缺省情况下，没有使用ACL限制FTP客户端
（可选）配置FTP服务与SSL服务器端策略关联	**ftp server ssl-server-policy** *policy-name*	缺省情况下，没有配置SSL服务器端策略与FTP服务关联
（可选）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
（可选）配置FTP服务器发送的FTP报文的DSCP优先级	**ftp server dscp** *dscp-value*	二者选其一 缺省情况下，FTP服务器发送的FTP报文的DSCP优先级为0，FTP服务器发送的IPv6 FTP报文的DSCP优先级为0
（可选）配置FTP服务器发送的IPv6 FTP报文的DSCP优先级	**ftp server ipv6 dscp** *dscp-value*	
（可选）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“安全配置指导”中的“AAA”

1.2.2 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。

在设备在对 FTP 客户端进行认证时，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。

在设备在对 FTP 客户端进行授权时，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”。

1.2.3 释放已建立的FTP连接

表1-2 释放已建立的 FTP 连接

操作	命令	说明
强制释放与指定用户之间的FTP连接	**free ftp user** *username*	二者必选其一
强制释放与指定IP地址的主机之间的FTP连接	**free ftp user-ip** [**ipv6**] *client-address* [**port** *port-num*]	

1.2.4 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1-3 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	**display ftp-server**
查看当前FTP登录用户的详细情况	**display ftp-user**

1.2.5 FTP服务器典型配置举例（MSR 2600/MSR 3600）

1. 组网需求

- Device 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 Device 的启动配置文件。
- 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1-2 FTP 服务器典型配置组网图

3. 配置步骤

配置前请确保Device和PC之间路由可达，IP地址如 图 1-2 所示，具体配置步骤略。

(1) 配置 Device（FTP server）

在 Device 上添加一个 FTP 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:/
[Sysname-luser-abc] service-type ftp
[Sysname-luser-abc] quit
```

启动 Device 的 FTP 服务功能。

```
[Sysname] ftp server enable
[Sysname] quit
```

删除 Device 中的多余文件，以保证剩余足够的空间，用于存储需要上传的文件。

```
<Sysname> dir
Directory of flash:
     0      -rw-           0  Sep 27 2010 14:43:34     kernel.bin
     1      -rw-           0  Sep 27 2010 14:43:34     base.bin
     2      drw-           -  Jun 29 2011 18:30:38     logfile
     3      drw-           -  Jun 21 2011 14:51:38     diagfile
     4      drw-           -  Jun 21 2011 14:51:38     seclog
     5      -rw-        2943  Jul 02 2011 08:03:08     startup.cfg
     6      -rw-       63901  Jul 02 2011 08:03:08     startup.mdb
     7      -rw-         716  Jun 21 2011 14:58:02     hostkey
     8      -rw-         572  Jun 21 2011 14:58:02     serverkey
     9      -rw-     6541264  Aug 04 2011 20:40:49     backup.bin

473664 KB total (467080 KB free)
<Sysname> delete /unreserved flash:/backup.bin
```

(2) 配置 PC（FTP client）

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 Device 的配置文件 startup.cfg 下载到 PC 本地进行备份。

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

将传输模式设置为 binary，并上传文件 temp.bin 到 Device。

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

退出 FTP。

```
ftp> bye
```

1.2.6 FTP服务器典型配置举例（MSR 5600）

1. 组网需求

- Device 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 Device 的启动配置文件。
- 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1-3 FTP 服务器典型配置组网图

3. 配置步骤

配置前请确保Device和PC之间路由可达，IP地址如 图 1-3 所示，具体配置步骤略。

(1) 配置 Device（FTP server）

在 Device 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

如果要直接访问备用主控板（所在槽位号为 1）Flash 的根目录，需要将“authorization-attribute work-directory flash:/”配置中的“flash:/”替换成“slot1#flash:/”。

```
[Sysname-luser-abc] service-type ftp
[Sysname-luser-abc] quit
```

启动 Device 的 FTP 服务功能。

```
[Sysname] ftp server enable
[Sysname] quit
```

删除 Device 中的多余文件，以保证剩余足够的空间，用于存储需要上传的文件。

```
<Sysname> dir
Directory of flash:
     0      -rw-           0  Sep 27 2010 14:43:34     kernel.bin
     1      -rw-           0  Sep 27 2010 14:43:34     base.bin
     2      drw-           -  Jun 29 2011 18:30:38     logfile
     3      drw-           -  Jun 21 2011 14:51:38     diagfile
     4      drw-           -  Jun 21 2011 14:51:38     seclog
     5      -rw-        2943  Jul 02 2011 08:03:08     startup.cfg
```

```
6       -rw-       63901  Jul 02 2011 08:03:08     startup.mdb
7       -rw-         716  Jun 21 2011 14:58:02     hostkey
8       -rw-         572  Jun 21 2011 14:58:02     serverkey
9       -rw-     6541264  Aug 04 2011 20:40:49     backup.bin

473664 KB total (467080 KB free)
<Sysname> delete /unreserved flash:/backup.bin
```

(2) 配置 PC（FTP client）

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 Device 的配置文件 startup.cfg 下载到 PC 本地进行备份。

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

将传输模式设置为 binary，并上传文件 temp.bin 到主用主控板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
```

1.3 配置FTP客户端

1.3.1 建立FTP连接

FTP 客户端要访问 FTP 服务器，必须先与 FTP 服务器建立连接。连接的建立方式有两种，一种是使用 **ftp** 命令直接建立连接；一种是在 FTP 客户端视图下使用 **open** 命令间接建立连接。

在使用 **ftp** 命令建立 FTP 连接时，还可以进行源地址绑定。源地址绑定可以通过指定源接口（建议使用 LoopBack 接口或 Dailer 接口）或源 IP 地址来实现。

表1-4 建立 FTP 连接（IPv4 组网环境）

操作	命令	说明
进入系统视图	**system-view**	-
（可选）在IPv4组网环境下配置FTP客户端发送的FTP报文的源地址	**ftp client source** { **interface** *interface-type interface-number* | **ip** *source-ip-address* }	缺省情况下，没有配置源地址，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
退回用户视图	**quit**	-

操作	命令	说明
在用户视图下直接登录FTP服务器	**ftp** *ftp-server* [*service-port*] [**vpn-instance** *vpn-instance-name*] [**dscp** *dscp-value* | **source** { **interface** { *interface-name* | *interface-type interface-number* } | **ip** *source-ip-address* }] *	二者必选其一 **ftp**命令直接在用户视图下执行；**open**命令在FTP客户端视图下执行
在FTP客户端视图下间接登录FTP服务器	**ftp**	
	open *server-address* [*service-port*]	

说明

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。

表1-5 建立 FTP 连接（IPv6 组网环境）

操作	命令	说明
进入系统视图	**system-view**	-
（可选）在IPv6组网环境下配置FTP客户端发送的FTP报文的源地址	**ftp client ipv6 source** { **interface** *interface-type interface-number* | **ipv6** *source-ipv6-address* }	缺省情况下，没有配置源地址，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
退回用户视图	**quit**	-
在用户视图下直接登录FTP服务器	**ftp ipv6** *ftp-server* [*service-port*] [**vpn-instance** vpn-instance-name] [**dscp** *dscp-value* | **source** { **interface** *interface-type interface-number* | **ipv6** *source-ipv6-address* }] * [**-i** *interface-type interface-number*]	二者必选其一 **ftp ipv6**命令直接在用户视图下执行；**open**命令在FTP客户端视图下执行
在FTP客户端视图下间接登录FTP服务器	**ftp ipv6**	
	open *server-address* [*service-port*]	

说明

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。

1.3.2 操作FTP服务器上的目录

当设备作为 FTP 客户端，与 FTP 服务器成功建立连接后，在 FTP 服务器的授权目录下，用户可以进行创建、删除文件夹等操作。

表1-6 操作 FTP 服务器上的目录

操作	命令	说明
查看FTP服务器上的目录/文件的详细信息	**dir** [*remotefile* [*localfile*]]	二者选其一
	ls [*remotefile* [*localfile*]]	
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**	-
显示当前用户正在访问的FTP服务器上的路径	**pwd**	-
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*	-

1.3.3 操作FTP服务器上的文件

当设备作为 FTP 客户端，与 FTP 服务器成功建立连接后，在 FTP 服务器的授权目录下，用户可以通过以下操作，向 FTP 服务器上传或从 FTP 服务器下载文件，推荐使用以下步骤：

(1) 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) 删除过时文件，以便有效利用存储空间。

(3) 设置传输模式。FTP 传输文件有两种模式：一种是 ASCII 码模式，用于传输文本文件；另一种是二进制模式，用于传输程序文件。

(4) 使用 **lcd** 命令显示或切换 FTP 客户端本地的工作路径。无论使用相对路径还是绝对路径进行上传/下载操作，上传的将是该路径下的文件，文件下载后也将保存到该路径下。

(5) 进行上传/下载操作。

表1-7 操作 FTP 服务器上的文件

操作	命令	说明
查看FTP服务器上的目录/文件的详细信息	**dir** [*remotefile* [*localfile*]]	二者选其一
	ls [*remotefile* [*localfile*]]	
彻底删除FTP服务器上的指定文件	**delete** *remotefile*	-
设置FTP文件传输的模式	**ascii**	二者选其一 缺省情况下，文件传输模式为ASCII模式
	binary	
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
显示或切换FTP客户端本地的工作路径	**lcd** [*directory* | */*]	-
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*]	-

操作	命令	说明
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*]	-
重命名文件	**rename** [*oldfilename* [*newfilename*]]	-

1.3.4 更改登录用户

当设备作为 FTP 客户端，与 FTP 服务器连接建立成功后，可以更改登录用户。

该功能通常用于不同权限用户之间的切换，用户的成功切换不会影响当前的 FTP 连接（即 FTP 控制连接、数据连接以及连接状态都不变）；如果输入的用户名/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。

表1-8 更改登录用户

操作	命令	说明
成功登录FTP服务器后，使用其他用户身份重新登录	**user** *username* [*password*]	-

1.3.5 FTP连接的维护与调试

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 连接过程中出现的问题。

表1-9 FTP 连接的维护与调试

操作	命令	说明
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**	-

1.3.6 断开FTP连接

当设备作为 FTP 客户端，与 FTP 服务器连接建立成功后，可以使用以下任意一条命令来断开 FTP 连接。

表1-10 断开 FTP 连接

操作	命令	说明
不退出FTP客户端视图的前提下，断开与FTP服务器的连接	**disconnect**	二者选其一 在FTP客户端视图下执行
	close	
断开与FTP服务器的连接，并退回到用户视图	**bye**	二者选其一 在FTP客户端视图下执行
	quit	

1.3.7 显示帮助信息

当设备作为 FTP 客户端，与 FTP 服务器连接建立成功后，可以使用以下任意一条命令显示命令或命令的帮助信息。

表1-11 显示帮助信息

操作	命令	说明
显示命令或命令的帮助信息	**help** [*command-name*]	二者选其一
	? [*command-name*]	

1.3.8 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1-12 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**

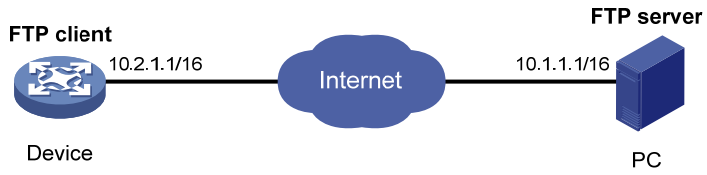
1.3.9 FTP客户端典型配置举例（MSR 2600/MSR 3600）

1. 组网需求

- Device 作为 FTP 客户端，PC 作为 FTP 服务器。
- Device 从 PC 上下载文件 temp.bin，并将启动配置文件上传到 PC 进行备份。
- PC 上已设置 Device 登录 FTP 服务器的用户名为 abc，密码为 123456。

2. 组网图

图1-4 FTP 客户端典型配置组网图



3. 配置步骤

提示

如果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 1-4 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 Device。

```
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 Device 的配置文件 startup.cfg 上传到 FTP 服务器进行备份。

```
ftp> ascii
200 TYPE is now ASCII
ftp> put startup.cfg back-startup.cfg
local: startup.cfg remote: back-startup.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>
```

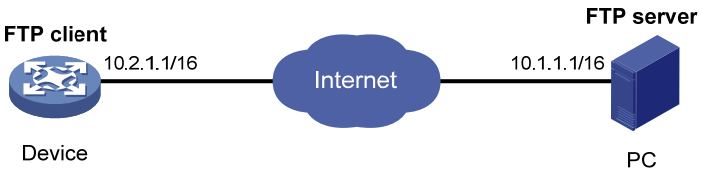
1.3.10 FTP客户端典型配置举例（MSR 5600）

1. 组网需求

- Device 作为 FTP 客户端，PC 作为 FTP 服务器。
- Device 从 PC 上下载文件 temp.bin，并将启动配置文件上传到 PC 进行备份。
- PC 上已设置 Device 登录 FTP 服务器的用户名为 abc，密码为 123456。

2. 组网图

图1-5 FTP 客户端典型配置组网图



3. 配置步骤

提示

如果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 1-5 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 Device。

- 将文件 temp.bin 从 FTP 服务器下载到主用主控板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 服务器下载到备用主控板（所在槽位号为 1）存储介质的根目录下。

```
ftp> get temp.bin slot1#flash:/temp.bin
```

将 Device 的启动配置文件 startup.cfg 上传到 FTP 服务器进行备份。

```
ftp> ascii
200 TYPE is now ASCII
ftp> put startup.cfg back-startup.cfg
local: startup.cfg remote: back-startup.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

说明

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

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器均很可靠的网络环境。

目前，设备只能作为 TFTP 客户端，不支持作为 TFTP 服务器。

图2-1 TFTP 组网示意图

2.2 配置TFTP客户端

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。

表2-1 配置 IPv4 TFTP 客户端

操作	命令	说明
进入系统视图	**system-view**	-
使用ACL限制设备可访问哪些TFTP服务器	**tftp-server acl** *acl-number*	可选 缺省情况下，没有使用ACL对设备可访问的TFTP服务器进行限制
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，没有配置源地址，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
退回用户视图	**quit**	-

操作	命令	说明
在IPv4网络，用TFTP上传/下载文件	**tftp** *tftp-server* { **get** | **put** | **sget** } *source-filename* [*destination-filename*] [**vpn-instance** *vpn-instance-name*] [**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 该命令在用户视图下执行

表2-2 配置 IPv6 TFTP 客户端

操作	命令	说明
进入系统视图	**system-view**	-
（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** *acl-number*	缺省情况下，没有使用ACL对设备可访问的TFTP服务器进行限制
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-ip-address* }	缺省情况下，没有配置源地址，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
退回用户视图	**quit**	-
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*] [**vpn-instance** *vpn-instance-name*] [**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 该命令在用户视图下执行

目 录

1 文件系统管理

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”。

MSR 系列路由器各款型对于本节所描述的特性的支持情况有所不同，详细差异信息如下：

型号	特性	描述
MSR 2600	支持的储存设备	支持FLASH
MSR 3600		• MSR3600-28/MSR3600-51 支持 FLASH • MSR 36-10/MSR 36-20/MSR 36-40/MSR 36-60 支持 CF 卡
MSR 5600		支持CF卡

1.1 文件系统

1.1.1 文件系统简介

设备运行过程中所需要的文件（如：主机软件、配置文件等）保存在设备的存储介质中，为了方便用户对存储介质进行有效的管理，设备以文件系统的方式对这些文件进行管理。

文件/文件夹分为隐藏的、非隐藏的。对于隐藏文件/文件夹，请不要修改或删除，以免影响对应功能；对于非隐藏的文件/文件夹，请完全了解它的作用后再执行文件/文件夹操作，以免误删重要文件/文件夹。

1.1.2 存储介质的命名

存储介质有多种类型，如 Flash、CF 卡、U 盘等。

存储介质的命名遵循以下规则：

如果设备上只支持一个同一类型的存储介质，则存储介质的名称就是存储介质类型名称。Flash 命名为 flash；CF 卡命名为 cfa0、cfb0 等，U 盘命名为 usba0、usbb0 等。

1.1.3 文件名参数输入规则

注意

在输入文件名参数时，请确保存储介质名（包括字符串 chassis 和 slot）为全小写，文件夹和纯文件名不区分大小写。否则，系统会提示错误信息“The file or directory doesn't exist.”。

在设备上执行文件系统操作时，文件名参数的输入需要遵循 表 1-1。

表1-1 文件名参数输入规则（MSR 2600/MSR 3600）

格式	说明	举例
file-name	纯文件名（只有文件名而没有路径），表示当前路径下的文件	a.cfg表示当前目录下的a.cfg文件
[*path/*]*file-name*	文件夹+纯文件名，表示当前路径指定文件夹下的指定文件。*path*表示文件夹的名称，*path*参数可以输入多次，表示多级文件夹下的文件	• test/a.cfg 表示当前路径下 test 文件夹下的 a.cfg 文件 • test/subtest/a.cfg 表示当前路径下 test 文件夹下 subtest 子文件夹下的 a.cfg 文件
drive:/[*path/*]*file-name*	存储介质+文件夹+纯文件名，表示设备上某块存储介质上的文件。*drive*表示存储介质的名称，通常为flash或者cfa0 如果设备上只有一个存储介质，可以不用给出存储介质的信息；如果设备上有多个存储介质，需要给出存储介质的信息以确定是哪块存储介质上的文件	flash:/test/a.cfg表示Flash根目录下test文件夹下的a.cfg文件

表1-2 设备文件名参数输入规则（MSR 5600）

格式	说明	举例
file-name	纯文件名（只有文件名而没有路径），表示当前工作路径下的文件	a.cfg表示当前目录下的a.cfg文件 • 如果当前工作路径在主用主控板，则 a.cfg 表示主用主控板上的 a.cfg 文件 • 如果当前工作路径在备用主控板，则 a.cfg 表示备用主控板上的 a.cfg 文件
[*path/*]*file-name*	文件夹+纯文件名，表示当前路径指定文件夹下的指定文件。*path*表示文件夹的名称，*path*参数可以输入多次，表示多级文件夹下的文件	• test/a.cfg 表示当前路径下 test 文件夹下的 a.cfg 文件 • test/subtest/a.cfg 表示当前路径下 test 文件夹下 subtest 子文件夹下的 a.cfg 文件
drive:/[*path/*]*file-name*	存储介质+文件夹+纯文件名，表示设备上某块存储介质上的文件。*drive*表示存储介质的名称，主用主控板上的存储介质表示为cfa0；备用主控板上的存储介质表示为slot*n*#cfa0，*n*为备用主控板所在的槽位号，如：slot1#cfa0。可以使用**display device**命令查看单板与槽位号的对应关系	• cfa0:/test/a.cfg 表示主用主控板上 CF 卡根目录下 test 文件夹下的 a.cfg 文件 • slot1#cfa0:/a.cfg 表示备用主控板（槽位号为 1）上 CF 卡根目录下的 a.cfg 文件

说明

给文件/文件夹命名时，首字母请不要使用“.”。因为系统会把名称首字母为“.”的文件/文件夹当成隐藏文件/文件夹。

1.2 文件操作

注意

在进行文件操作过程中禁止对存储介质进行插拔操作。否则，可能会引起文件系统的损坏。（MSR 2600/MSR 3600）

在进行文件操作过程中禁止对存储介质进行插拔或主备倒换操作。否则，可能会引起文件系统的损坏。（MSR 5600）

文件操作包括显示文件夹或文件信息、显示文件内容、重命名文件、拷贝文件、移动文件、删除文件、恢复删除的文件、彻底删除回收站中的文件、计算文件摘要。

创建文件可以通过拷贝、下载操作或 **save** 命令来辅助完成。下载操作的详细介绍请参见“基础配置指导”中的“FTP”和“TFTP”，**save** 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”。

当需要对U盘进行写文件操作，包括 重命名文件、拷贝文件、移动文件、压缩/解压缩文件、删除/恢复文件，请确保没有将U盘写保护。如果U盘写保护了，这些操作将执行失败。其它文件操作不受写保护开关影响。

1.2.1 显示文件信息

表1-3 显示文件信息

操作	命令	说明
显示文件夹或文件信息	**dir** [**/all**] [*file-url* | **/all-filesystems**]	该命令在用户视图下执行

1.2.2 显示文件内容

表1-4 显示文件内容

操作	命令	说明
显示文本文件的内容	**more** *file-url*	该命令在用户视图下执行

1.2.3 重命名文件

表1-5 重命名文件

操作	命令	说明
重命名文件	**rename** *fileurl-source fileurl-dest*	该命令在用户视图下执行

1.2.4 拷贝文件

表1-6 拷贝文件

操作	命令	说明
拷贝文件	非FIPS模式下： **copy** *fileurl-source fileurl-dest* [**vpn-instance** *vpn-instance-name*] [**source interface** *interface-type interface-number*] FIPS模式下： **copy** *fileurl-source fileurl-dest*	该命令在用户视图下执行

1.2.5 移动文件

表1-7 移动文件

操作	命令	说明
移动文件	**move** *fileurl-source fileurl-dest*	该命令在用户视图下执行

1.2.6 压缩/解压缩文件

表1-8 压缩/解压缩文件

操作	命令	说明
压缩指定的文件	**gzip** *filename*	该命令在用户视图下执行
解压缩指定的文件	**gunzip** *filename*	该命令在用户视图下执行

1.2.7 删除/恢复文件

注意

请不要对回收站中的文件执行 **delete** 命令，以免影响回收站功能。若要删除回收站中的文件，请使用 **reset recycle-bin** 命令。

用户可以永久删除或者暂时删除一个文件，永久删除的文件不能恢复，暂时删除的文件被系统自动放入了回收站，可以恢复。

表1-9 删除/恢复文件

操作	命令	说明
删除文件并将文件放入回收站	**delete** *file-url*	该命令在用户视图下执行

操作	命令	说明
恢复回收站中的文件	**undelete** *file-url*	该命令在用户视图下执行
永久删除文件	**delete /unreserved** *file-url*	该命令在用户视图下执行

说明

使用 **delete** *file-url* 命令删除的文件，被保存在回收站中，仍会占用存储空间。如果用户经常使用该命令删除文件，则可能导致设备的存储空间不足，请用户查看回收站中是否有废弃文件。如果要彻底删除回收站中的废弃文件，必须执行 **reset recycle-bin** 命令，才可以回收存储空间。

1.2.8 彻底删除回收站中的文件

表1-10 彻底删除回收站中的文件

操作	命令	说明
彻底删除回收站中的文件	**reset recycle-bin** [**/force**]	该命令在用户视图下执行

1.2.9 计算文件摘要

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，防止文件内容被篡改。

表1-11 计算文件摘要

操作	命令	说明
使用SHA-256摘要算法计算文件的摘要值	**sha256sum** *file-url*	该命令在用户视图下执行
使用MD5摘要算法计算文件的摘要值	**md5sum** *file-url*	该命令在用户视图下执行

1.3 文件夹操作

当需要执行存储介质操作时，有以下注意事项：

- 在进行文件夹操作过程中禁止对存储介质进行插拔操作。否则，可能会引起文件系统的损坏。（MSR 2600/MSR 3600）
- 在进行文件夹操作过程中禁止对存储介质进行插拔或主备倒换操作。否则，可能会引起文件系统的损坏。（MSR 5600）
- 当需要对U盘进行写文件夹操作，包括 创建文件夹、删除文件夹，请确保没有将U盘写保护。如果U盘写保护了，这些操作将执行失败。其它文件夹操作不受写保护开关影响。

1.3.1 显示文件夹信息

表1-12 显示文件夹信息

操作	命令	说明
显示文件夹或文件信息	**dir** [**/all**] [*file-url* | **/all-filesystems**]	该命令在用户视图下执行

1.3.2 显示当前的工作路径

表1-13 显示当前的工作路径

操作	命令	说明
显示当前的工作路径	**pwd**	该命令在用户视图下执行

1.3.3 修改当前的工作路径

表1-14 修改当前的工作路径

操作	命令	说明
修改当前的工作路径	**cd** { *directory* | **..** }	该命令在用户视图下执行

1.3.4 创建文件夹

表1-15 创建文件夹

操作	命令	说明
创建文件夹	**mkdir** *directory*	该命令在用户视图下执行

1.3.5 删除文件夹

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。如果文件只是暂时删除，那么执行 **rmdir** 会将这些文件从回收站中彻底删除。

表1-16 删除文件夹

操作	命令	说明
删除文件夹	**rmdir** *directory*	该命令在用户视图下执行

1.4 存储介质操作

当需要执行存储介质操作时，有以下注意事项：

- 在执行存储介质操作过程中，禁止对存储介质进行插拔操作。否则，可能会引起文件系统的损坏。（MSR 2600/MSR 3600）
- 在执行存储介质操作过程中，禁止对单板或存储介质进行插拔或主备倒换操作。否则，可能会引起文件系统的损坏。（MSR 5600）
- 当用户占用可插拔存储介质的资源（如用户正在访问某个目录或正在打开文件等）时，存储介质被强制拔出。此时，请先释放占用的存储介质的资源（如切换目录、关闭打开的文件等），再插入存储介质。否则，存储介质被插入后可能不能被识别。
- 当需要对U盘进行写存储介质操作，包括 恢复存储介质的空间、格式化存储介质，请确保没有将U盘写保护。如果U盘写保护了，这些操作将执行失败。其它存储介质操作不受写保护开关影响。

1.4.1 恢复存储介质的空间

由于异常操作等原因，存储介质的某些空间可能不可用，用户可以通过 **fixdisk** 命令来恢复存储介质的空间。

用户对存储介质执行 **fixdisk** 操作时，如果同时还有其他用户在访问该存储介质，系统会提示 **fixdisk** 操作失败。

表1-17 恢复存储介质的空间

操作	命令	说明
恢复存储介质的空间	**fixdisk** *medium-name*	该命令在用户视图下执行

1.4.2 格式化存储介质

注意

格式化操作将导致存储介质上的所有文件丢失，并且不可恢复，请谨慎使用。

用户对存储介质执行格式化操作时，如果同时还有其他用户在访问该存储介质，系统会提示格式化操作失败。

表1-18 格式化存储介质

操作	命令	说明
格式化存储介质	**format** *medium-name*	该命令在用户视图下执行

1.4.3 存储介质的挂载/卸载

注意

- 刚插入 USB 接口的 U 盘，不允许立刻拔出，需要等待 U 盘被识别（即 U 盘上的指示灯不再闪烁），然后使用命令 **umount** 卸载 U 盘再拔出。否则，可能会造成 USB 接口或 U 盘无法使用。
- 用户对存储介质执行 **umount** 操作时，如果同时还有其他用户在访问该存储介质，系统会提示 **umount** 操作失败。

支持热插拔的存储介质（如 CF 卡等），可以在用户视图下，使用 **mount** 和 **umount** 命令挂载和卸载该存储介质。

- 缺省情况下，存储介质连接到设备后，自动被挂载，可以直接使用。如果系统未能自动识别插入的存储设备，则必须手动进行挂载操作后，才能对该存储介质执行读写操作。
- 卸载存储介质是逻辑上让存储介质处于非连接状态，此时，用户可以安全的拔出存储介质。如果不卸载直接拔出存储介质，则可能引起文件损坏甚至存储介质损坏、不可用。
- 被卸载的存储介质需重新挂载方可使用。

表1-19 存储介质的挂载/卸载

操作	命令	说明
挂载存储介质	**mount** *medium-name*	缺省情况下，存储介质连接到设备后，自动被挂载，处于挂载状态，可以直接使用 该命令在用户视图下执行
卸载存储介质	**umount** *medium-name*	缺省情况下，存储介质连接到设备后，自动被挂载，处于挂载状态，可以直接使用 该命令在用户视图下执行

1.5 设置文件和文件夹操作时是否提示

用户可以通过命令行来设置执行文件和文件夹操作时是否提示：

- 当设置为 **alert**，并且用户对文件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。

表1-20 设置文件和文件夹操作时是否提示

操作	命令	说明
进入系统视图	**system-view**	-
设置文件和文件夹操作时是否提示	**file prompt { alert | quiet }**	缺省情况下，用户对文件进行有危险性的操作时，系统会要求用户进行交互确认

目 录

1 配置文件管理

说明

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

1.1 配置文件简介

配置文件是用来保存配置的文件。配置文件主要用于：

- 将当前配置保存到配置文件，以便设备重启后，这些配置能够继续生效。
- 使用配置文件，用户可以非常方便地查阅配置信息。
- 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. 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。

2. 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。
- 使用 **display startup** 命令查看本次启动使用的配置文件，再使用 **more** 命令查看该配置文件的内容。（**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”）

3. 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

配置文件是用来保存配置的文件，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。为了安全起见，用户可以配置两个下次启动配置文件，一个为主用，一个为备用。

系统启动时，配置文件的选择遵循以下规则：

(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，再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。

1.1.3 配置文件的保存格式

用户执行 **save** 命令保存配置时，系统会自动生成一个字符串类型的配置文件和一个二进制类型的配置文件。

- 字符串类型的配置文件是一个文本文件，文件名后缀为“.cfg”，可以通过 **more** 命令查看该文件的内容。
- 二进制类型的配置文件是字符串类型的配置文件的二进制格式，文件名后缀为“.mdb”。在设备启动和运行时，系统软件能够解析该类配置文件，而用户却不能读取和编辑文件内容。

两个文件保存的配置相同，但格式不同。设备启动的时候，会优先使用二进制类型的配置文件，以便提高加载配置的速度。如果没有找到合适的二进制类型的配置文件，才使用字符串类型的配置文件。

设备启动的时候，会先根据配置查找指定名称的字符串类型的配置文件是否存在，如果存在，再查找对应的二进制类型的配置文件是否存在，如果存在，再判断两个文件的内容是否一致，一致才使用二进制类型的配置文件启动设备，不一致，还是使用字符串类型的配置文件启动设备。因此，二进制类型的配置文件不能单独存在，必须有对应的字符串类型的配置文件才有意义。字符串类型的配置文件可以没有对应的二进制类型的配置文件而单独存在。

如无特殊说明，下文描述的配置文件均指字符串类型的配置文件。

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，请尽量使用设备自动生成的配置文件。如果要手工修改配置文件，请遵循配置文件的内容与格式规则。

配置文件的内容与格式规则如下：

- 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，节与节之间用注释行隔开（以“#”开始的为注释行）。
- 以 **return** 结束。

下面摘录了配置文件的部分内容。

```
#
local-user root
 password simple admin
 service-type ssh telnet terminal
 authorization-attribute user-role network-admin
#
interface GigabitEthernet2/1/1
 port link-mode route
 ip address 1.1.1.1 255.255.255.0
#
```

1.2 保存当前配置

1.2.1 使能配置文件加密功能

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。加密后的文件只能被运行 Comware V7 平台软件的 H3C 设备识别和解析，运行其它平台软件的设备不能识别和解析。

表1-1 使能配置文件加密功能

操作	命令	说明
进入系统视图	**system-view**	-
使能配置文件加密功能	**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

1.2.2 保存当前配置

用户通过命令行可以修改设备的当前配置，而这些配置是暂时的，如果要使当前配置在系统下次启动时仍然有效，需要在重启设备前，将当前配置保存到下次启动配置文件中。

提示

执行 **save** [**backup** | **main**] [**force**]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。

表1-2 保存当前配置（MSR 2600/MSR 3600）

操作	命令	说明
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*	二者选其一 为了安全起见，在需要将当前配置保存到下次启动配置文件的时候，建议选用**safely**参数 两命令均可在任意视图下执行
将当前配置保存到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**]	

表1-3 保存当前配置（MSR 5600）

操作	命令	说明
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*]	二者选其一 为了安全起见，在需要将当前配置保存到下次启动配置文件的时候，建议选用**safely**参数 两命令均可在任意视图下执行
将当前配置保存到主用主控板和备用主控板存储介质的根目录，并将该文件设置为下次启动配置文件	**save** [**safely**] [**backup** | **main**] [**force**]	

1.3 配置回滚

1.3.1 配置回滚简介

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。该配置文件必须是有效的.cfg文件，它可以使用手工/自动备份功能或者**save**命令生成，也可以是别的设备的可兼容配置文件，推荐使用手工/自动备份功能生成。（如何使用手工/自动备份功能生成配置文件请参见“1.3.2 备份当前配置”）

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。

说明

为了方便描述，定义如下：

- 手工/自动备份功能生成的配置文件称为备份配置文件。
- “将当前配置回滚到指定配置文件中的配置状态”中的“指定配置文件”称为回滚配置文件。

1.3.2 备份当前配置

1. 设置备份参数

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。设置这些参数后，备份当前配置时，系统会将当前的配置以指定的文件名（格式为前缀_序号.cfg，比如 archive_1.cfg）保存到指定的路径，方便管理员管理。备份序号由设备自动生成，从 1 开始编号，依次加 1，累加至 1000 后又重新从 1 开始。修改备份文件的保存路径、文件名前缀，备份序号也会从 1 开始重新自动编号。

系统内能够保存的备份文件的数目有一定限制。当备份文件数目到达上限，又需要保存新的备份文件时，系统会删除保存时间最早的备份文件，以保存新的备份文件。

表1-4 设置备份参数

操作	命令	说明
进入系统视图	**system-view**	-
设置备份配置文件的保存路径和文件名前缀	**archive configuration location** *directory* **filename-prefix** *filename-prefix*	缺省情况下，系统没有配置备份配置文件的保存路径和文件名前缀
（可选）系统允许保存的备份配置文件的最大数	**archive configuration max** *file-number*	缺省情况下，系统最多允许保存5个备份配置文件 *file-number*的具体数值应根据系统的空余存储空间大小来决定。对于存储空间较小的设备，建议将该参数设为较小值

说明

执行 **undo archive configuration location** 命令后，用户将不能手工备份当前配置，系统也不再自动备份当前配置，**archive configuration interval** 和 **archive configuration max** 的配置也会恢复到缺省情况，**display archive configuration** 的显示信息也会被清除。

2. 自动/手工备份当前配置

系统提供了自动备份和手工备份两种灵活的备份方式。用户可以使用自动备份方式，让系统按照一定的时间间隔自动备份当前配置。如果备份时间没有到达，而用户需要立即备份当前配置，可以使用手工备份。备份的配置文件的名称和时间可以通过 **display archive configuration** 命令查看，以便用户可以将当前配置回退到某一历史时刻的配置状态。

- 当需要对设备进行步骤复杂的配置时，可以在修改配置前手工备份当前配置。以便配置过程中出现失败时，可以使用已备份的配置直接将当前配置回滚至配置改变前的状态。
- 对于不会频繁修改配置的设备，建议按需手工备份当前配置。
- 对于使用低速存储介质（如 Flash）的设备，建议不进行自动备份配置，或设置备份时间间隔大于 1440 分钟（24 小时）。
- 对于使用高速存储介质（如 CF 卡），且配置经常修改的设备，可以设置较小的备份时间间隔。

表1-5 自动备份当前配置

操作	命令	说明
进入系统视图	**system-view**	-
使能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** *minutes*	缺省情况下，系统不会自动备份当前配置

表1-6 手工备份当前配置

操作	命令	说明
手工备份当前配置	**archive configuration**	该命令在用户视图下执行

1.3.3 执行配置回滚

提示

配置回滚期间（即系统在执行 **configuration replace file** 命令时）不能进行单板热拔插操作，否则可能会造成配置回滚终止。（MSR 5600）

执行配置回滚，设备会将当前配置回滚到指定配置文件中的配置状态。配置回滚时，系统会比较、处理当前配置和回滚配置文件中配置的差异：

- 对于当前配置与回滚配置文件中的相同命令，不做处理。

- 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。

命令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。

表1-7 执行配置回滚

操作	命令	说明
进入系统视图	**system-view**	-
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

1.4 管理下次启动配置文件

1.4.1 设置下次启动配置文件

执行以下操作前，请确保指定文件（*cfgfile*）为设备存储介质根目录下的合法配置文件，否则，操作失败。（MSR 2600/MSR 3600）

主用主控板和备用主控板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主用主控板和备用主控板存储介质的根目录下，否则，操作失败。（MSR 5600）

使用该命令设置配置文件时：

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

表1-8 设置下次启动配置文件

操作	命令	说明
配置下次启动时的配置文件	**startup saved-configuration** *cfgfile* [**backup** | **main**]	该命令在用户视图下执行 该命令执行成功后，用户可以在任意视图下使用**display startup**命令以及**display saved-configuration**命令验证配置效果

执行**save** [**safely**] [**backup** | **main**] [**force**]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“1.2.2 保存当前配置”。

1.4.2 备份/恢复主用下次启动配置文件

设备运行于 FIPS 模式时，不支持备份/恢复主用下次启动配置文件。

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. 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** 命令查看一下设备是否已经设置了下次启动配置文件。如果没有下次启动配置文件，或者所设置的配置文件不存在，备份操作将会失败。

2. 备份/恢复主用下次启动配置文件

表1-9 备份/恢复主用下次启动配置文件

操作	命令	说明
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** *tftp-server* [*dest-filename*]	该命令在用户视图下执行
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** *tftp-server src-filename*	该命令在用户视图下执行 该命令执行成功后，用户可以在任意视图下使用**display startup**命令以及**display saved-configuration**命令验证配置效果

1.4.3 删除下次启动配置文件

注意

本特性会将下次启动配置文件从设备上彻底删除，请谨慎使用。

出现以下情况时，用户可能需要删除设备中的下次启动配置文件：

- 设备软件升级之后，系统软件和配置文件不匹配。
- 设备中的配置文件被破坏（常见原因是加载了错误的配置文件）。

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。如果当前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（假设指定了 **backup** 参数），系统只会将相应的下次启动配置文件设置为 NULL，不会删除该文件，需要再执行一次删除操作（指定 **main** 参数），才能将这个配置文件彻底删除。

下次启动配置文件被删除后，设备重启时，系统将采用出厂配置进行初始化。

表1-10 删除设备中的下次启动配置文件

操作	命令	说明
删除设备中的下次启动配置文件	**reset saved-configuration** [**backup** | **main**]	该命令在用户视图下执行 不指定**banckup**和**main**参数时，缺省使用**main**

1.5 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1-11 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**
显示当前配置	**display current-configuration** [**configuration** [*module-name*] | **interface** [*interface-type* [*interface-number*]]]
显示出厂配置	**display default-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 设备软件简介

设备软件包括 Boot ROM 程序和启动软件包，它是设备启动、运行的必备软件，为整个设备提供支撑、管理以及丰富的业务。

1.1.1 Boot ROM程序

设备开机最先运行的程序是 Boot ROM 程序，它能够引导硬件启动、引导启动软件包运行、提供 Boot ROM 菜单功能。

Boot ROM 程序存储在设备的 Boot ROM（芯片）中。完整的 Boot ROM 程序包含 Boot ROM 基本段和 Boot ROM 扩展段。基本段提供 Boot ROM 菜单的基本操作项，扩展段提供更多的 Boot ROM 菜单操作项。整个 Boot ROM 程序通过 Boot 包（*.bin）发布，产品会将需要升级的单板的 Boot ROM 程序集成到 Boot 包中统一发布，以降低版本维护成本。

1.1.2 启动软件包

1. 启动软件包的分类

启动软件包是用于引导设备启动的程序文件，按其功能可以分为以下几类：

- Boot 软件包（简称 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、应急 Shell 等功能。
- System 软件包（简称 System 包）：包含 Comware 内核和基本功能模块的程序，比如设备管理、接口管理、配置管理和路由模块等。
- Feature 软件包（简称 Feature 包）：用于业务定制的程序，能够提供更丰富的业务。一个 Feature 包可能包含一种或多种业务。
- Patch 软件包（简称补丁包）：用来修复设备软件缺陷的程序文件。补丁包与软件版本一一对应，补丁包只能修复与其对应的启动软件包的缺陷，不涉及功能的添加和删除。

设备必须具有 Boot 包和 System 包才能正常运行，Feature 包可以根据用户需要选择安装，补丁包只在需要修复设备软件缺陷时安装。

2. 启动软件包的发布形式

启动软件包有以下两种发布形式：

- BIN 文件：后缀为.bin 的文件。一个 BIN 文件就是一个启动软件包。要升级的 BIN 文件之间版本必须兼容才能升级成功。
- IPE（Image Package Envelope，复合软件包套件）文件：后缀为.ipe 的文件。它是多个软件包的集合，产品通常会将同一个版本需要升级的所有类型的软件包都压缩到一个 IPE 文件中发布。用户将该 IPE 文件加载到设备后，设备会自动将它解压缩成一个个 BIN 文件。用户再使用这些 BIN 文件升级设备即可，从而能够减少启动软件包之间的版本管理问题。

3. 主/备用下次启动软件包以及软件包列表

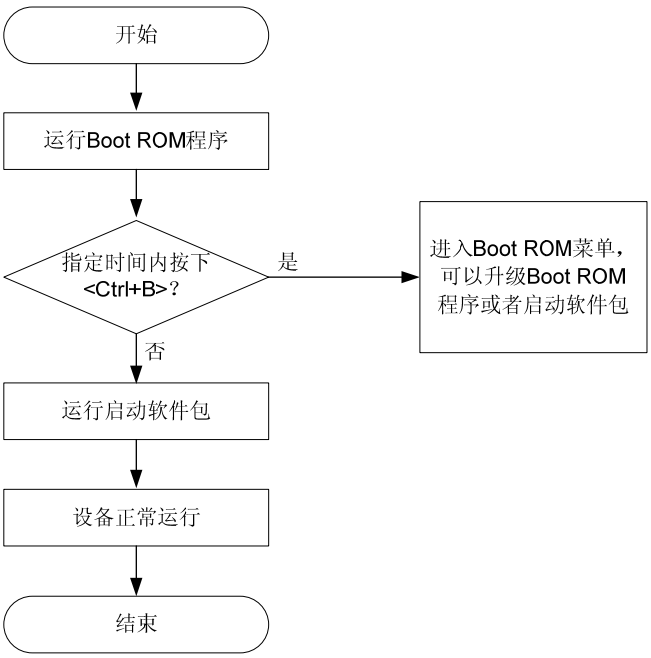
设备下次启动时使用的软件包称为下次启动软件包。用户可通过命令行将本设备存储介质上的某个软件包指定为设备的下次启动软件包，并指定软件包的属性为主用或者备用。被指定为主用属性的软件包称为主用下次启动软件包，被指定为备用属性的软件包称为备用下次启动软件包。

- 设备会将所有具有主用属性的软件包的名称存储在主用启动软件包列表中，将所有具有备用属性的软件包的名称存储在备用启动软件包列表中。
- 当设备启动时，优先使用主用启动软件包列表中的软件包，如果主用启动软件包列表中软件包不存在或者不可用，再使用备用启动软件包列表中的软件包。

1.1.3 设备启动过程

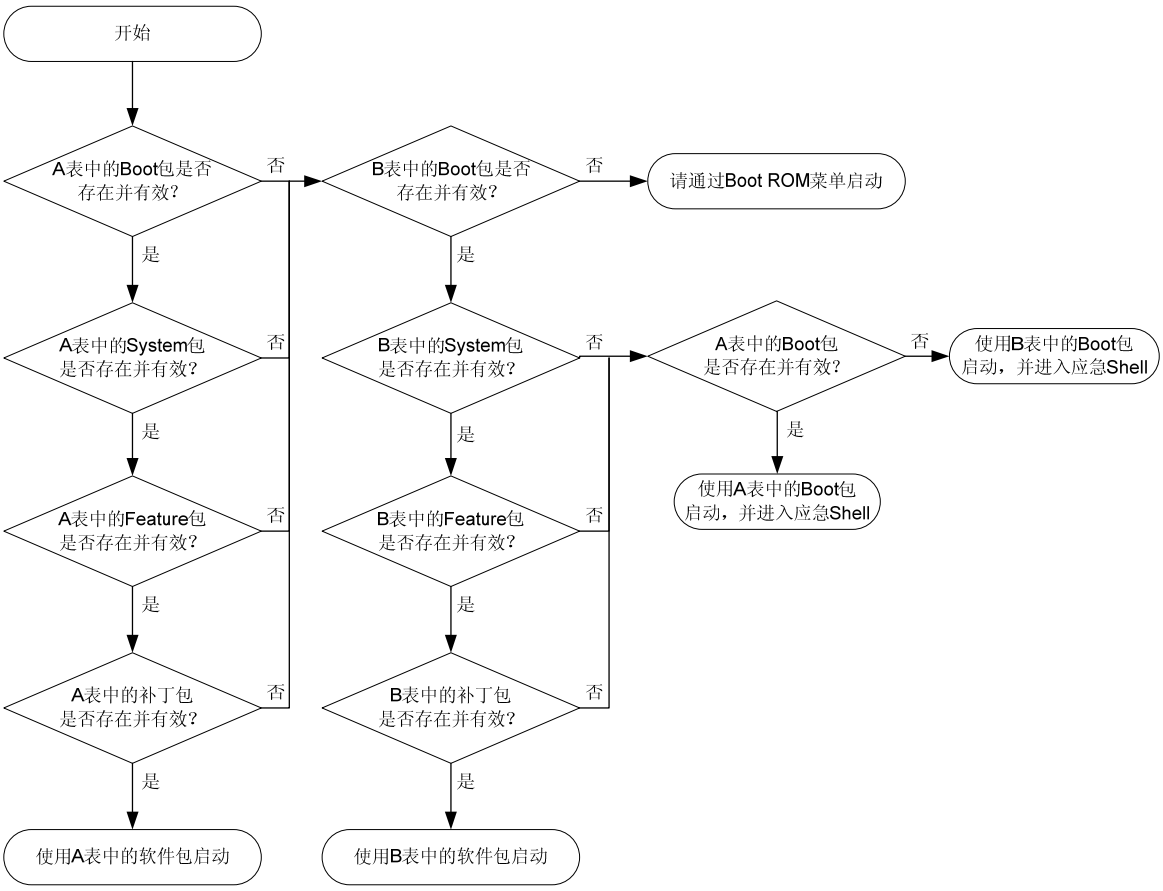
设备上电后，先运行Boot ROM文件，初始化硬件并显示设备的硬件参数，然后运行启动软件包，如 图 1-1 所示。图中“指定时间”为 4s。

图1-1 设备启动过程示意图



在运行启动软件包时，因为涉及到多个软件包，系统会做一系列处理，如 图 1-2 所示。

图1-2 启动软件包运行流程示意图



说明：流程图中A表示主用启动软件包列表，B表示备用启动软件包列表

- 系统会根据启动软件包列表自动判断相应的软件包是否存在，如果存在是否有效。如果启动软件包列表中没有 Feature 包/补丁包，则跳过 Feature 包/补丁包的判断流程。
- 当主用和备用启动软件包列表中的 Boot 包均不存在或不可用时，请使用 Console 口连接到设备，断电重启设备。启动过程中根据提示按<Ctrl+B>进入 Boot ROM 菜单，通过 Boot ROM 来重新加载 Boot 包，具体操作请参见产品随软件发布的版本说明书。
- 当设备进入应急 Shell 环境时，请使用 Console 口连接到设备，在应急 Shell 环境下，手工重新加载 System 包，才能进入 Comware 系统。具体操作请参见“基础配置指导”中的“应急 Shell”。

1.2 软件升级方式简介

设备出厂时，已经安装了软件，下次启动会延用本次启动使用的软件。如果要对软件进行升级，用户可以选择如下方式，详见 表 1-1。

表1-1 软件升级方式描述表

升级方式		升级对象	升级说明
通过命令行进行软件升级	通过整机重启方式升级	Boot ROM程序 启动软件包（该方式不能升级补丁包）	需要重启设备来实现设备软件的升级 使用该方式升级设备软件时会导致当前业务中断
	ISSU方式升级	启动软件包	ISSU是一种高可靠性升级设备启动软件的方式，推荐使用该方式升级设备 关于该方式的详细描述请参见“基础配置指导”中的“ISSU”
通过Boot ROM菜单进行软件升级		Boot ROM程序 启动软件包	可在设备无法正常启动时升级设备软件 具体操作请参见随版本发布的产品版本说明书

1.3 通过整机重启方式升级设备软件

1.3.1 升级步骤

请参照以下步骤来升级设备软件：

(1) 使用 **display version** 命令查看设备当前运行的 Boot ROM 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 Boot ROM 程序、启动软件的兼容性。

(3) 通过版本发布说明书了解将安装的软件包是否需要 License。如果需要，查看设备上是否有对应的有效的 License。如果没有，请先安装 License。否则，会导致软件包安装失败。

(4) 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，以免升级失败。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”。（MSR 2600/MSR 3600）

(5) 使用 **dir** 命令分别查看主用主控板和备用主板存储介质是否有足够的空间存储新的软件，以免升级失败。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”。（MSR 5600）

(6) 使用 FTP、TFTP 方式将新软件下载到存储介质的根目录下。FTP 及 TFTP 具体配置请参见“基础配置指导”中的“FTP 和 TFTP”。

(7) （可选）加载Boot ROM程序。当新软件和当前Boot ROM程序不兼容时，需要升级Boot ROM程序。虽然用户可以直接执行下一步操作，在升级Boot包的时候同步升级Boot ROM程序，但推荐用使用该功能升级Boot ROM程序。因为使用该功能能缩短Boot包的升级时间，以及减小升级过程中断电引入的问题。

(8) 指定下次启动软件包并完成升级。

1.3.2 加载Boot ROM程序

由于不同设备主控板和接口板的 Boot ROM 程序各不相同，用户容易混淆，从而导致 Boot ROM 程序升级错误。因此，请开启 Boot ROM 升级时的合法性检查功能，设备就能够对 Boot ROM 文件是否有效以及是否和硬件匹配等进行严格的检查，以确保升级成功。（MSR 5600）

表1-2 加载 Boot ROM 程序（MSR 2600/MSR 3600）

操作	命令	说明
加载新的Boot ROM程序	**bootrom update file** *file-url* [**slot** *slot-number-list*]	执行该命令，系统会将Flash中的Boot ROM程序加载到Boot ROM的Normal区

表1-3 加载 Boot ROM 程序（MSR 5600）

操作	命令	说明
加载新的Boot ROM程序	**bootrom update file** *file-url* **slot** *slot-number-list* [**subslot** *subslot-number-list*]	执行该命令，系统会将Flash中的Boot ROM程序加载到Boot ROM的Normal区

1.3.3 指定下次启动软件包并完成升级

1. MSR 2600/MSR 3600

- 当指定下次启动软件包/IPE 文件时，命令中指定的软件包（IPE 文件）必须放在设备存储介质的根目录下且后缀名为.bin（.ipe），文件名中必须包含存储介质的名称，形如 flash:/xx.bin（flash:/xx.ipe）。
- 配置 **boot-loader file** *ipe-filename* { **backup** | **main** }命令后，系统会自动将 IPE 文件中包含的所有软件包提取出来，并设置为下次启动软件包。

表1-4 指定下次启动软件包并完成升级

操作	命令	说明
指定设备下次启动时使用的软件包/IPE文件	**boot-loader file** *ipe-filename* { **backup**	**main** }	二者选其一 命令在用户视图下执行
	boot-loader file boot *boot-package* **system** *system-package* [**feature** *feature-package*&<1-30>] { **backup**	**main** }	
保存当前配置	**save**	保存当前配置，以便当前配置在设备重启后继续生效 该命令在用户视图下执行
重启设备	**reboot**	设备重启时，会运行新的启动软件包，从而完成升级 该命令在用户视图下执行

2. MSR 5600

- 当指定下次启动软件包/IPE 文件时，命令中指定的软件包（IPE 文件）必须放在主用主控板存储介质的根目录下且后缀名为.bin（.ipe），文件名中必须且只能包含存储介质的名称，不能包含 slot 的信息，形如 cfa0:/xx.bin（cfa0:/xx.ipe）。
- 为备用主控板指定下次启动软件包/IPE 文件时，系统会自动检查存储在主用主控板上的下次启动软件包/IPE 文件是否已拷贝到备用主控板的 Flash 根目录下。如果还未拷贝，则自动从主用主控板上拷贝一份并设置为备用主控板的主用下次启动软件包/IPE 文件。
- 配置 **boot-loader file** *ipe-filename* **slot** *slot-number* { **backup** | **main** }命令后，系统会自动将 IPE 文件中包含的、该主控板对应的软件包提取出来，并设置为该主控板的下次启动软件包。

通过命令 **boot-loader update slot** *slot-number* 指定备用主控板的下次启动软件包时，系统会进行如下处理：

- 如果主用主控板当前是使用主用启动软件包列表启动的，则将其主用下次启动软件包列表中的软件包拷贝到备用主控板的对应目录下，并设置为备用主控板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。
- 如果主用主控板当前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备用主控板的对应目录下，并设置为备用主控板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。

表1-5 指定新的下次启动软件包并完成升级

操作	命令	说明
指定主用主控板下次启动时使用的软件包/IPE 文件	**boot-loader file** *ipe-filename* { **all** | **slot** *slot-number* } { **backup** | **main** }	二者选其一 命令在用户视图下执行
	boot-loader file boot *boot-package* **system** *system-package* [**feature** *feature-package*&<1-30>] **slot** *slot-number* { **backup** | **main** }	
指定备用主控板下次启动时使用的软件包/IPE 文件	**boot-loader file** *ipe-filename* { **all** | **slot** *slot-number* } { **backup** | **main** }	三者选其一 命令在用户视图下执行
	boot-loader file boot *boot-package* **system** *system-package* [**feature** *feature-package*&<1-30>] **slot** *slot-number* { **backup** | **main** }	
	boot-loader update slot *slot-number*	
保存当前配置	**save**	保存当前配置，以便当前配置在设备重启后继续生效 该命令在用户视图下执行
重启设备	**reboot**	设备重启时，会运行新的启动软件包，从而完成升级 该命令在用户视图下执行

1.4 使能备用主控板启动软件包自动加载功能

注意

加载启动软件包需要一定时间，在加载期间，请不要插拔主控板或者手工重启备用主控板，否则，会导致备用主控板加载启动软件包失败而不能启动。用户可打开日志信息显示开关，并根据日志信息的内容来判断加载过程是否开始以及是否结束。

当设备上同时存在两块主控板时，建议用户不要忽略对启动软件包版本的一致性检查。因为：

- 如果忽略对备用主控板进行启动软件包版本一致性检查，当备用主控板和主用主控板启动软件包版本不一致时，备用主控板仍然使用不一致的版本启动，可能会造成设备功能问题。
- 如果使能对备用主控板进行启动软件包版本一致性检查，当备用主控板和主用主控板启动软件包版本不一致时，备用主控板会停留在启动阶段，不能正常启动。

配置 **undo version check ignore** 和 **version auto-update enable** 命令后，在设备启动过程中，当备用主控板发现自己当前启动软件包版本和主用主控板的当前启动软件包版本不一致时，会自动拷贝主用主控板的当前启动软件包列表中的所有软件包，设置为自己的主用下次启动软件包，并自动重启。这样，能够使得备用主控板启动后，和主用主控板启动软件包的版本一致。

表1-6 使能备用主控板启动软件包自动加载功能

操作	命令	说明
进入系统视图	**system-view**	-
使能对备用主控板进行启动软件包版本一致性检查	**undo version check ignore**	缺省情况下，备用主控板启动软件包版本一致性检查功能处于使能状态
使能备用主控板自动加载主用主控板当前启动软件包的功能	**version auto-update enable**	缺省情况下，当启动过程中，当备用主控板发现自己版本和主用主控板版本不一致时，会自动加载主用主控板的当前启动软件包

MSR 系列路由器各款型对于本节所描述的特性的支持情况有所不同，详细差异信息如下：

型号	特性	描述
MSR 2600	使能备用主控板启动软件包自动加载功能	不支持
MSR 3600		不支持
MSR 5600		支持

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1-7 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（MSR 2600/MSR 3600）	**display boot-loader**
显示本次启动和下次启动所采用的启动软件包的名称（MSR 5600）	**display boot-loader** [**slot** *slot-number* [**cpu** *cpu-number*]]

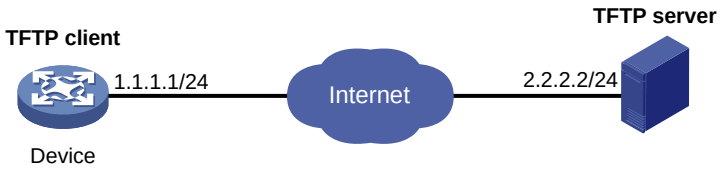
1.6 通过重启方式升级启动软件包配置举例（MSR 2600/MSR 3600）

1. 配置需求

使用最新软件版本文件 startup-a2105.ipe，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1-3 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

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 Device 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
```

将待升级的 IPE 文件 startup-a2105.ipe 从 TFTP server 下载到设备 Flash 的根目录下。

```
<Sysname> tftp 2.2.2.2 get startup-a2105.ipe
```

将 startup-a2105.ipe 备份为 startup-a2105-backup.ipe。

```
<Sysname> copy startup-a2105.ipe startup-a2105_backup.ipe
```

指定设备下次启动时使用 startup-a2105.ipe 作为主用 IPE 文件。

```
<Sysname> boot-loader file cfa0:/startup-a2105.ipe main
```

指定设备下次启动时使用 startup-a2105-backup.ipe 作为备用 IPE 文件。

```
<Sysname> boot-loader file cfa0:/startup-a2105-backup.ipe backup
```

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，查看设备使用的启动软件包的版本。

```
<Sysname> display version
```

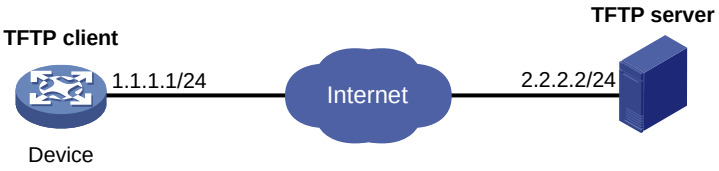
1.7 通过重启方式升级启动软件包配置举例（MSR 5600）

1. 配置需求

- Device 上有两块主控板：主用主控板所在槽位号为 0，备用主控板所在槽位号为 1。
- 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1-4 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

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，再设置为备用下次启动软件包/IPE 文件。如果设备上存储空间有限，可以不备份。

配置 IP 地址以及路由，确保 Device 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
```

将待升级的 IPE 文件 startup-a2105.ipe 从 TFTP server 下载到设备 Flash 的根目录下。

```
<Sysname> tftp 2.2.2.2 get startup-a2105.ipe
```

将 startup-a2105.ipe 备份为 startup-a2105-backup.ipe。

```
<Sysname> copy startup-a2105.ipe startup-a2105-backup.ipe
```

指定主用主控板和备用主控板下次启动时使用 startup-a2105.ipe 作为主用 IPE 文件。

```
<Sysname> boot-loader file cfa0:/startup-a2105.ipe slot 0 main
<Sysname> boot-loader file cfa0:/startup-a2105.ipe slot 1 main
```

指定主用主控板和备用主控板下次启动时使用 startup-a2105-backup.ipe 作为备用 IPE 文件。

```
<Sysname> boot-loader file cfa0:/startup-a2105-backup.ipe slot 0 backup
<Sysname> boot-loader file cfa0:/startup-a2105-backup.ipe slot 1 backup
```

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，查看设备使用的启动软件包的版本。

```
<Sysname> display version
```

目 录

1 应急Shell

1.1 应急Shell简介

设备的启动软件包分为 Boot 包、System 包、Feature 包和补丁包。其中，设备必须具有 Boot 包和 System 包才能正常运行，Feature 包可以根据用户需要选择安装，补丁包只在需要修复设备软件缺陷时安装。当设备启动，如果 Boot 包存在并有效，但当前启动软件包列表中的 System 包/Feature 包/补丁包中的某个包不存在或不可用，设备便会进入应急 Shell 环境（Emergency Shell）。

设备进入应急 Shell 环境后，普通的业务口将不可用，请使用 Console 口重新登录设备，您将看到设备的命令行提示符变成了<boot>，而不是正常运行情况下的<*设备名*>。请使用应急 Shell 下提供的一系列的命令，重新加载 System 软件包，才能进入 Comware 系统。此时的设备只运行了 Boot 包和 System 包，如需运行 Feature 包和补丁包，须重新下载、安装。

关于软件包的介绍以及具体配置步骤请参见“基础配置指导”中的“软件升级”。本文描述是应急 Shell 下支持的操作。

1.2 配置限制和指导

本文描述的操作均是在故障主控板上执行，且只能对本板进行操作。比如，主用主控板上 System 包不存在或者异常，进入应急 Shell 环境了，请使用主用主控板的 Console 口登录，执行本文中描述的操作给主用主控板加载 System 包；备用主控板缺乏 System 包，进入应急 Shell 环境了，请使用备用主控板的 Console 口登录，执行本文中描述的操作给备用主控板加载 System 包。（MSR 5600）

1.3 文件系统操作

应急 Shell 提供了基本的文件系统操作，以方便用户对存储介质上的文件进行管理。需要注意的是：

- 执行 **delete** 操作后，设备会彻底删除指定文件，并且不可恢复，请谨慎使用。
- 执行 **format** 操作后，存储介质上的所有文件将丢失，并且不可恢复，请谨慎使用。

表1-1 文件系统操作命令

操作	命令	说明
显示目录或文件信息	**dir** [**/all**] [*file-url*]	该命令在用户视图下执行
在存储介质的指定路径下创建目录	**mkdir** *directory*	如果创建的文件夹与指定路径下的其它文件或目录重名，则创建操作失败 在使用该命令创建目录之前，指定的路径必须已经存在。比如：创建文件夹flash:/test/mytest，这时，test目录必须已经存在，否则，创建失败 该命令在用户视图下执行
显示当前工作路径	**pwd**	该命令在用户视图下执行
复制文件	**copy** *fileurl-source fileurl-dest*	该命令在用户视图下执行

操作	命令	说明
移动文件	**move** *fileurl-source fileurl-dest*	目标目录必须空间足够，否则，移动操作失败 该命令在用户视图下执行
显示指定文件的内容	**more** *file-url*	该命令在用户视图下执行
彻底删除指定文件	**delete** *file-url*	该命令在用户视图下执行
删除已有目录	**rmdir** *directory*	被删除的目录必须为空目录，即删除目录前，必须先删除该目录下的所有文件及子目录 该命令在用户视图下执行
格式化存储介质	**format** *device*	该命令在用户视图下执行

1.4 获取System包

设备进入应急 Shell 环境后，只有 Console 口、AUX 口和管理以太网接口可用，请在管理以太网接口下配置网络参数，通过 FTP 和 TFTP 协议从远程服务器上获取 System 包。

在获取 System 包前，请使用 **display version** 命令查看 Boot 包的版本信息，并根据 System 包的版本发布说明，获取和 Boot 包版本相同的 System 包。

1.4.1 配置管理以太网接口

应急 Shell 下要使用 FTP、TFTP、SSH、Telnet 等网络功能，首先必须正确配置网络参数，包括给管理以太网接口配置 IP 地址，如果需要跨网段访问，则还需要给管理以太网接口配置网关。

表1-2 配置管理以太网接口（IPv4 网络）

操作	命令	说明
进入系统视图	**system-view**	-
进入管理以太网接口视图	**interface m-eth0**	-
配置接口的IPv4地址	**ip address** *ip-address* { *mask-length* | *mask* }	缺省情况下，管理以太网接口下没有配置IPv4地址
配置接口的IPv4网关地址	**ip gateway** *ip-address*	缺省情况下，管理以太网接口下没有配置IPv4网关地址
激活管理以太网接口	**undo shutdown**	缺省情况下，管理以太网接口处于激活状态
从当前视图退回到上一级视图	**quit**	-

表1-3 配置管理以太网接口（IPv6 网络）

操作	命令	说明
进入系统视图	**system-view**	-
进入管理以太网接口视图	**interface m-eth0**	-

操作	命令	说明
配置接口的IPv6地址	**ipv6 address** *ipv6-address prefix-length*	缺省情况下，管理以太网接口下没有配置IPv6地址
配置接口的IPv6网关地址	**ipv6 gateway** ipv6-address	缺省情况下，管理以太网接口下没有配置IPv6网关地址
激活管理以太网接口	**undo shutdown**	缺省情况下，管理以太网接口处于激活状态
从当前视图退回到上一级视图	**quit**	-

1.4.2 Ping功能

网络参数配置完成后，可使用 **ping** 命令测试网络是否可达。

表1-4 检查指定目的端是否可达（IPv4 网络）

操作	命令	说明
检查指定IPv4地址是否可达	**ping** [**-c** *count* | **-s** *size*] * *ip-address*	该命令在任意视图下执行

表1-5 检查指定目的端是否可达（IPv6 网络）

操作	命令	说明
检查指定IPv6地址是否可达	**ping ipv6** [**-c** *count* | **-s** *size*] * *ipv6-address*	该命令在任意视图下执行

1.4.3 访问远程服务器

应急 Shell 环境下，设备可以作为 FTP、TFTP 客户端，从远程文件服务器上下载软件包来启动设备，或者将设备上的文件上传至远程服务器进行备份。在进行 FTP/TFTP 操作前，可以先使用 **telnet/ssh2** 命令远程登录到 FTP/TFTP 服务器，进行一些基本的 FTP/TFTP 参数配置，比如，使能 FTP/TFTP 功能，配置 FTP 登录用户名和密码等。

表1-6 访问远程服务器（IPv4 网络）

操作	命令	说明
（可选）Telnet登录到IPv4远程服务器	**telnet** *server-ipv4-address*	该命令在用户视图下执行
（可选）SSH登录到IPv4远程服务器	**ssh2** *server-ipv4-address*	该命令在用户视图下执行 如果因为服务器公钥变更，导致设备再次SSH登录该服务器失败时，请执行**reset ssh public-key**命令清除原公钥后，再执行**ssh2**命令重新登录
在IPv4网络中，下载/上传指定文件到FTP服务器	**ftp** *server-ipv4-address* **user** *username* **password** *password* { **get** *remote-file local-file* | **put** *local-file remote-file* }	该命令在用户视图下执行

操作	命令	说明
在IPv4网络中，下载/上传指定文件到TFTP服务器	**tftp** *server-ipv4-address* { **get** *remote-file local-file* | **put** *local-file remote-file* }	该命令在用户视图下执行

表1-7 访问远程服务器（IPv6 网络）

操作	命令	说明
（可选）Telnet登录到IPv6远程服务器	**telnet ipv6** *server-ipv6-address*	该命令在用户视图下执行
（可选）SSH登录到IPv6远程服务器	**ssh2 ipv6** *server-ipv6-address*	该命令在用户视图下执行 如果因为服务器公钥变更，导致设备再次SSH登录该服务器失败时，请执行**reset ssh public-key**命令清除原公钥后，再执行**ssh2**命令重新登录
在IPv6网络中，下载/上传指定文件到FTP服务器	**ftp ipv6** *server-ipv6-address* **user** *username* **password** *password* { **get** *remote-file local-file* | **put** *local-file remote-file* }	该命令在用户视图下执行
在IPv6网络中，下载/上传指定文件到TFTP服务器	**tftp ipv6** *server-ipv6-address* { **get** *remote-file local-file* | **put** *local-file remote-file* }	该命令在用户视图下执行

1.5 加载System包

获取 System 包后，需要加载 System 包，以便引导设备进入 Comware 系统。需要注意的是：

- 加载前，请使用 **display version** 和 **display install package** 命令查看 Boot 包和 System 包的版本信息，确认两软件包版本完全相同后，再执行加载操作。
- 加载时，系统会同步刷新主用下次启动软件包列表，新列表中只包含 Boot 包和 System 包，以保证设备下次能够正常启动。

表1-8 加载 System 包

操作	命令	说明
加载System包	**install load** *system-package*	该命令在用户视图下执行

1.6 重启

表1-9 重启

操作	命令	说明
重启设备（MSR 2600/MSR 3600） 重启当前登录的主控板（MSR 5600）	**reboot**	该命令在用户视图下执行

1.7 应急Shell显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示应急 Shell 下的相关配置信息，通过查看显示信息验证配置的效果。

表1-10 应急 Shell 显示和维护

操作	命令
显示版权信息	**display copyright**
查看指定软件包的信息	**display install package** *package*
显示管理以太网接口M-Eth0的信息	**display interface m-eth0**
显示IPv4路由信息表	**display ip routing-table**
显示IPv6路由信息表	**display ipv6 routing-table**
显示Boot包版本信息	**display version**

1.8 应急Shell配置举例

1. 配置需求

Device 作为 TFTP 客户端，PC 作为 TFTP 服务器。IP 地址如组网图所示，Device 和 PC 之间路由可达。

系统只有 boot.bin 包，Device 需要通过 TFTP 协议从 PC 上下载对应版本的 system.bin 包，启动设备。

2. 配置组网

图1-1 应急 Shell 配置举例组网图

3. 配置步骤

查看存储介质上存在哪些文件以及存储介质上的使用情况。

```
<boot> dir
Directory of flash:
   0   drw-      5954  Apr 26 2007 21:06:29   logfile
   1   -rw-      1842  Apr 27 2007 04:37:17   boot.bin
   2   -rw-      1518  Apr 26 2007 12:05:38   startup.cfg
   3   -rw-      2045  May 04 2007 15:50:01   backcfg.cfg

524288 KB total (513248 KB free)
```

以上信息表明，当前只有 boot.bin 包，没有 system.bin 包，存储介质上的空闲内存大小为 513248KB，有足够的空间存放 System 包。

查看系统版本信息。

```
<boot> display version
H3C Comware Software
Copyright (c) 2004-2013 Hangzhou H3C Tech. Co., Ltd. All rights reserved.
H3C uptime is 0 weeks, 0 days, 0 hours, 2 minutes

Boot image: flash:/boot.bin
Boot image version: 7.1.049P01

CPU ID: 0x2
2G bytes DDR3 SDRAM Memory
8M bytes flash Memory
PCB               Version:  2.0
CPLD              Version:  2.0
Basic    BootWare Version:  1.20
Extended BootWare Version:  1.20
```

给管理以太网接口配置 IP 地址和网关。

```
<boot> system-view
[boot] interface m-eth0
[boot-m-eth0] ip address 1.1.1.1 16
[boot-m-eth0] ip gateway 1.1.1.2
```

测试和 TFTP 服务器之间是否可达。

```
<boot> ping 1.2.1.1
PING 1.2.1.1 (1.2.1.1): 56 data bytes
56 bytes from 1.2.1.1: seq=0 ttl=128 time=2.243 ms
56 bytes from 1.2.1.1: seq=1 ttl=128 time=0.717 ms
56 bytes from 1.2.1.1: seq=2 ttl=128 time=0.891 ms
56 bytes from 1.2.1.1: seq=3 ttl=128 time=0.745 ms
56 bytes from 1.2.1.1: seq=4 ttl=128 time=0.911 ms

--- 1.2.1.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.717/1.101/2.243 ms
```

从 TFTP 服务器上下载文件 system.bin。

```
<boot> tftp 1.2.1.1 get system.bin flash:/system.bin
```

查看 system.bin 的相关信息，确认是否和当前的 boot.bin 版本一致。

```
<boot> display install package flash:/system.bin
  flash:/system.bin
  [Package]
  Vendor: H3C
  Product: xxxx
  Service name: system
  Platform version: 7.1.049P01
  Product version: ESS 010203
  Supported board: mpu
```

```
  [Component]
  Component: system
  Description: system package
```

加载 System 包，引导设备进入 Comware 系统。

```
<boot> install load flash:/system.bin
Check package flash:/system.bin ...
Extracting package ...

Loading...
Line aux0 is available.


Press ENTER to get started.
```

按 ENTER 键可进入 Comware 系统，系统会提示如下信息：

```
<System>
<System>%Sep 23 18:29:59:777 2012 System SHELL/5/SHELL_LOGIN: TTY logged in from
 aux0.
```

目 录

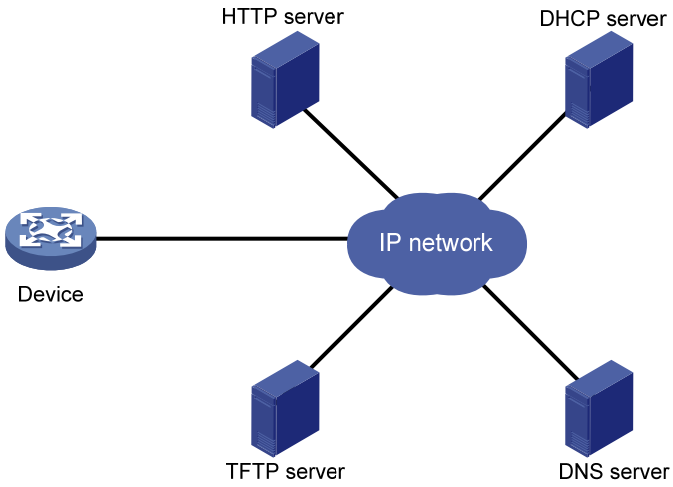
1 自动配置

1.1 自动配置简介

自动配置功能是指没有配置文件的设备在启动时自动获取并执行配置文件。

目前，网络规模较大时面临着设备分布广、维护人员少的问题，网络管理员在每一台设备上进行手工配置的工作量很大。利用自动配置功能，网络管理员只需将配置文件保存在指定的服务器上，设备在空配置启动时可以自动从服务器上获取并执行配置文件，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。

图1-1 自动配置典型组网图



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、TFTP服务器和DNS服务器的配合下，实现自动配置：

- DHCP 服务器：用来为执行自动配置的设备分配 IP 地址、配置文件名、TFTP 服务器参数和 DNS 服务器 IP 地址等信息。DHCP 服务器的详细介绍，请参见“三层技术-IP 业务配置指导”中的“DHCP 服务器”。
- TFTP服务器：用来保存自动配置过程中设备需要的文件，如保存主机IP地址和主机名映射关系的主机名文件和设备的配置文件等。TFTP服务器的详细介绍，请参见“基础配置指导”中的“TFTP”。配置文件和主机名文件的详细介绍，请参见“1.2.2 2. 获取配置文件”。
- DNS 服务器：用来提供 IP 地址和主机名的对应关系。执行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 服务器获取名为“主机名.cfg”的配置文件；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。DNS 服务器的详细介绍，请参见“三层技术-IP 业务配置指导”中的“域名解析”。

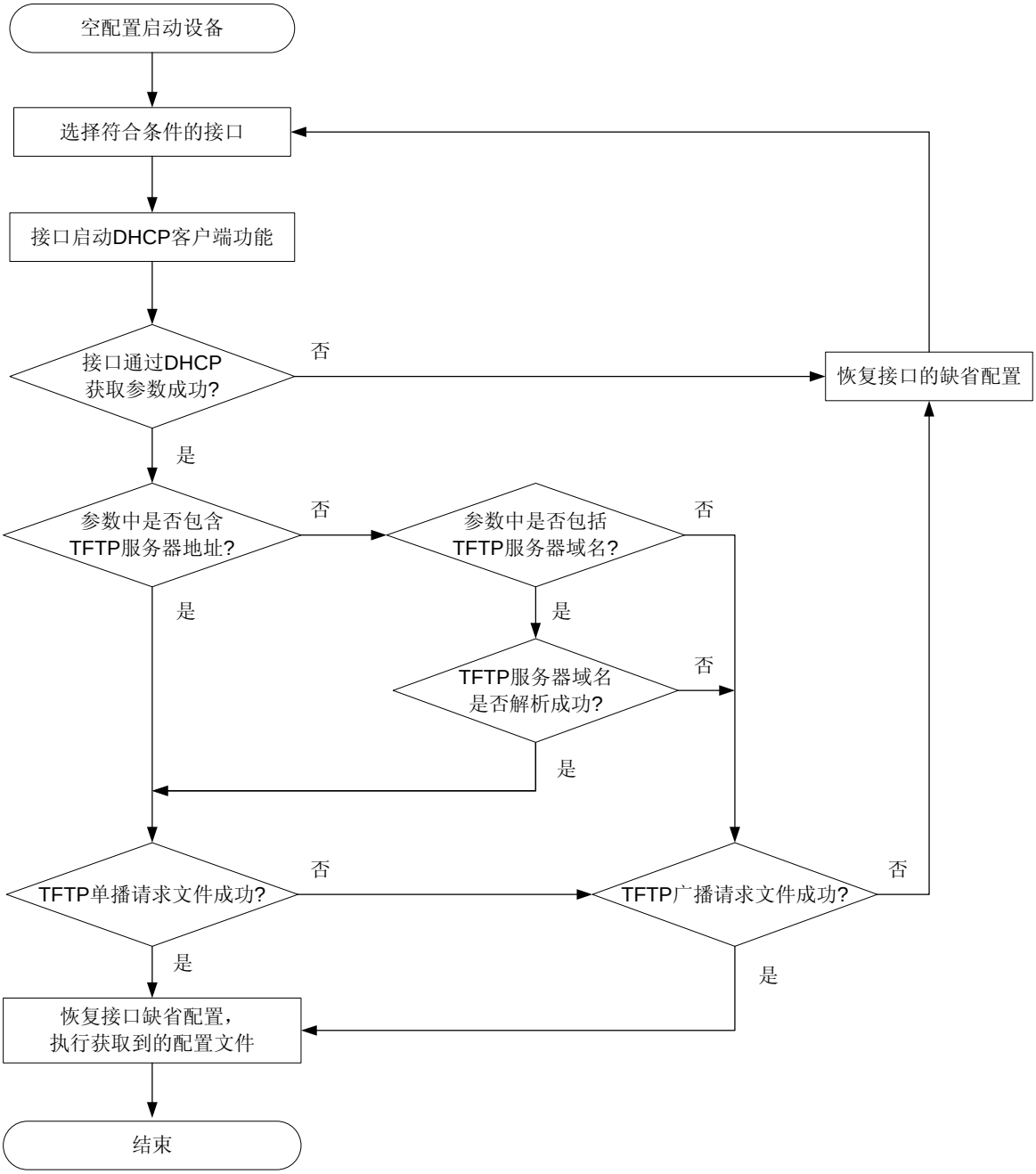
如果 DHCP 服务器、TFTP 服务器和 DNS 服务器与执行自动配置的设备不在同一个网段，自动配置的设备需要增加网关，并且网关得配置 DHCP 中继功能，并配置路由协议，使得各个服务器和设备之间路由可达。

以广播方式向 TFTP 服务器发送请求消息时，由于广播报文只能在本网段内传播，如果执行自动配置的设备与 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，将广播报文转换为单播报文，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 自动配置的工作过程

自动配置的流程如 图 1-2 所示。

图1-2 自动配置流程图



自动配置的基本工作过程如下：

(1) 设备在空配置启动时，系统按照如下规则选取符合条件的接口：

a. 若有处于链路状态 UP 的管理以太网接口，则优先选取管理以太网接口；

b. 若没有处于链路状态 UP 的管理以太网接口，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；

c. 若没有处于链路状态 UP 的二层以太网接口，则按照接口类型字典序、接口编号从小到大的顺序依次选择处于链路状态 UP 的三层以太网接口。

(2) 系统获取到符合条件的第一个接口后，系统配置该接口通过 DHCP 方式获取如下信息：配置文件名、TFTP 服务器域名、TFTP 服务器 IP 地址和 DNS 服务器地址等信息。

(3) 设备成功地从 DHCP 服务器获取到该接口的 IP 地址及后续获取配置文件所需要的信息后，根据上述信息获取配置文件名，，并从 TFTP 服务器下载该配置文件。如果下载配置文件成功，执行配置文件，自动配置过程结束；否则按照步骤(1)的规则开始获取下一个符合条件的接口，重复步骤(2)和(3)。

(4) 当获取配置文件失败时，设备会不断重复自动配置过程，直到成功获取配置文件为止。如果获取配置文件失败，则在 30 秒后开始下次自动配置过程，或用户通过<CTRL+D>手工终止自动配置操作。

(5) 成功获得配置文件后，执行获取到的配置文件。在自动配置过程中，不论通过当前接口下载配置文件成功与否，自动配置都会恢复该接口的缺省配置。

说明

- 如需使用自动配置功能，建议在设备开启前，只将自动配置时需要使用的接口连入网络，以便加快自动配置速度。
- 通过自动配置获取到的配置文件执行完成后，该文件将被删除，不会在设备上保存。建议配置文件执行完成后，在设备上通过 **save** 命令保存配置，否则，设备重启后还需重新执行自动配置功能。**save** 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”。

1.2.1 通过DHCP获取IP地址及相关信息

1. IP地址及相关信息的获取过程

DHCP 请求报文除获取 IP 地址以外，报文中的 Option 55 选项指明设备需要从 DHCP 服务器获得哪些信息（如配置文件名、TFTP 服务器域名、TFTP 服务器 IP 地址和 DNS 服务器 IP 地址等信息）。

通过 DHCP 成功获取到 IP 地址后，设备将解析 DHCP 服务器应答报文中的如下字段：

- Option 67 或 file 字段：用来获取配置文件名。设备首先解析 Option 67，如果该选项包括配置文件名信息，则不再解析 file 字段；否则，继续解析 file 字段。
- Option 66：用来获取 TFTP 服务器域名。
- Option 150：用来获取 TFTP 服务器 IP 地址。
- Option 6：用来获取 DNS 服务器 IP 地址。

DHCP 的详细工作过程请参见“三层技术-IP 业务配置指导”中的“DHCP 概述”。

2. 配置DHCP服务器上地址管理方式

用户可以根据自动配置功能的需要，在 DHCP 服务器上选择相应类型的地址管理方式：

- 不同设备的配置文件都相同时，可以在 DHCP 服务器上配置动态选择 IP 地址的方式，通过地址池为设备动态分配 IP 地址的同时，还为这些设备分配一样的网络配置参数（如配置文件名）。如果采用这种方式，则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采用其他方式完成。例如，通过自动配置获取的配置文件中指定在所有设备上开启 Telnet 服务，并创建本地用户，以便管理员通过 Telnet 方式登录这些设备，完成对每个设备特有的配置（如配置各个接口的 IP 地址）。
- 每个设备的配置文件都不相同时，需要在 DHCP 服务器上配置静态绑定 IP 地址的方式，以保证为特定的客户端分配固定的 IP 地址和其他网络配置参数。通过这种方式可以为每个设备指定不同的配置文件，实现对设备的完全配置，无需再通过其他方式配置设备。

说明

设备作为 DHCP 客户端时，采用客户端 ID 作为标识，在 DHCP 服务器上配置静态绑定 IP 地址时，需要指定静态绑定的客户端 ID。客户端 ID 的获取方法为：启动执行自动配置的设备，使执行自动配置的接口通过 DHCP 获取 IP 地址，IP 地址获取成功后，在 DHCP 服务器上通过 **display dhcp server ip-in-use** 命令显示地址绑定信息，从中可以获取设备的客户端 ID。

1.2.2 从TFTP服务器上获取配置文件

1. TFTP请求消息发送方式

设备根据对DHCP应答报文中TFTP服务器域名和TFTP服务器IP地址信息的解析结果，选择TFTP请求消息的发送方式：

(1) 如果应答报文中包括 TFTP 服务器 IP 地址信息，且 IP 地址值合法，设备将以单播方式向 TFTP 服务器发送请求消息，并不再解析 TFTP 服务器的域名信息。否则，继续解析应答报文中的 TFTP 服务器域名信息。

(2) 如果应答报文中包括 TFTP 服务器的域名信息，且域名合法，则通过 DNS 服务器解析 TFTP 服务器的 IP 地址。IP 地址解析成功后，以单播方式向 TFTP 服务器发送请求消息。如果 IP 地址解析不成功，则以广播方式向 TFTP 服务器发送请求消息。

(3) 如果应答报文中不包括 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。

以广播方式向 TFTP 服务器发送请求消息时，设备只会从第一个响应的 TFTP 服务器获取配置文件。

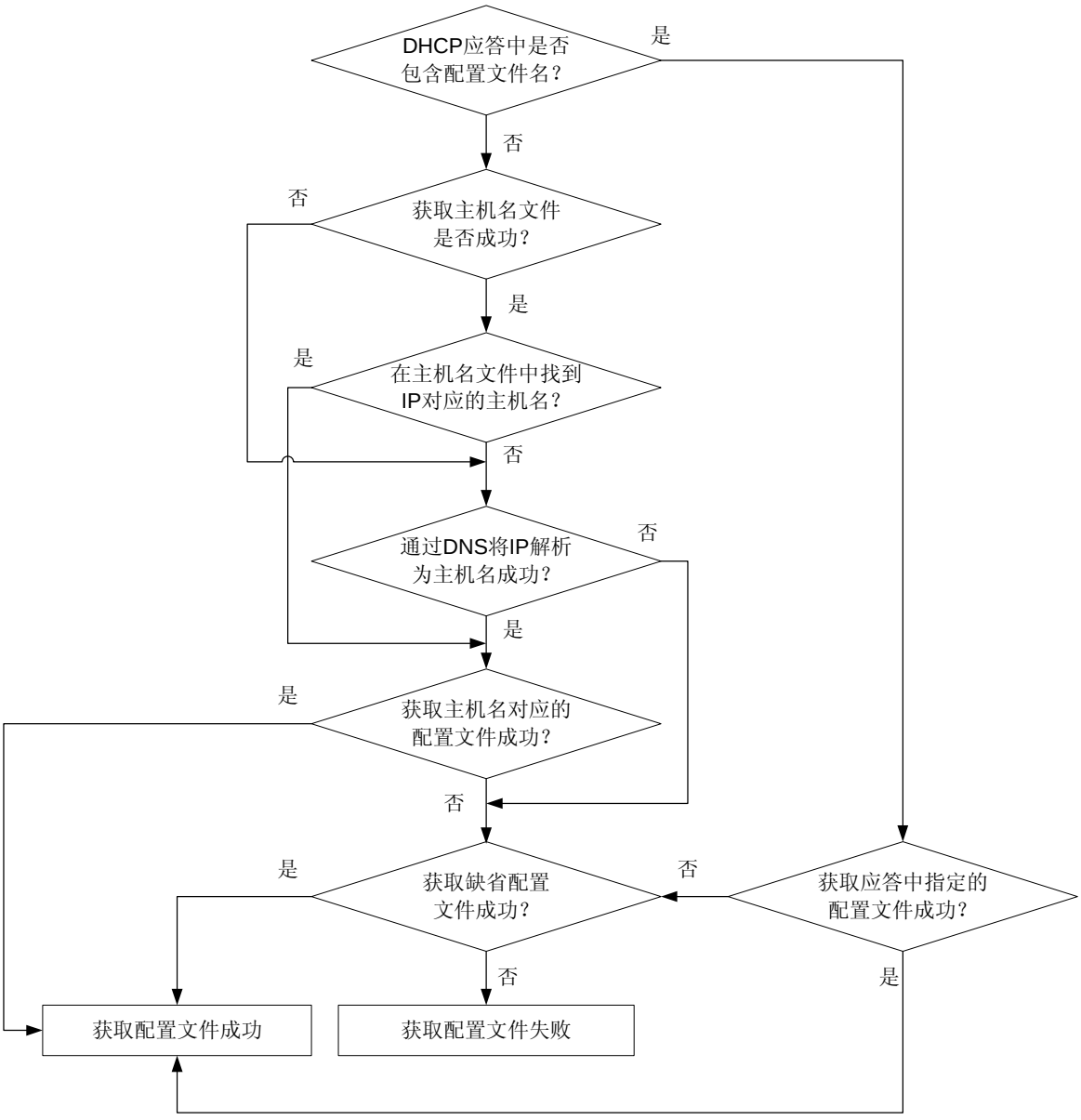
2. 获取配置文件

表1-1 文件类型

文件名	说明
配置文件	包含指定设备启动的配置信息，保存在TFTP服务器上，由DHCP应答报文中Option 67或file字段指定
主机名文件（network.cfg）	保存IP地址与主机名称的映射关系，文件由管理员设定，上传到TFTP服务器

文件名	说明
缺省配置文件	包含一般设备启动的公用配置信息，保存在TFTP服务器上

图1-3 配置文件获取过程



如 图 1-3 所示，设备根据对DHCP应答报文中配置文件名信息的解析结果，确定从TFTP服务器上获取哪个配置文件：

(1) 如果应答报文中包括配置文件名信息，则向 TFTP 服务器请求指定的配置文件。

(2) 如果应答报文中不包括配置文件名信息，则需要先获得设备的主机名，再向 TFTP 服务器请求与主机名对应的配置文件。设备通过如下几种方式获得主机名：

- 从 TFTP 服务器上获取主机名文件，在主机名文件中查找设备的 IP 地址对应的主机名；

- 如果在主机名文件中没有找到设备的主机名，则以单播方式向 DNS 服务器发送请求消息，以获取设备 IP 地址对应的主机名，如果单播方式失败，则以广播方式查询。

如果上述过程失败，则向 TFTP 服务器请求缺省配置文件。

1.3 通过U盘自动配置

1.3.1 通过U盘自动配置的工作过程

(1) 将 U 盘插入设备的 USB 接口，然后上电启动设备。

(2) 设备启动后检查全局主用板第一个 U 盘的根目录下是否存在配置文件，文件名为“设备序列号.cfg”如果没有该文件，继续查找固定配置文件名“autodeploy.cfg”，如果两个文件都没有则不进行 U 盘自动配置。

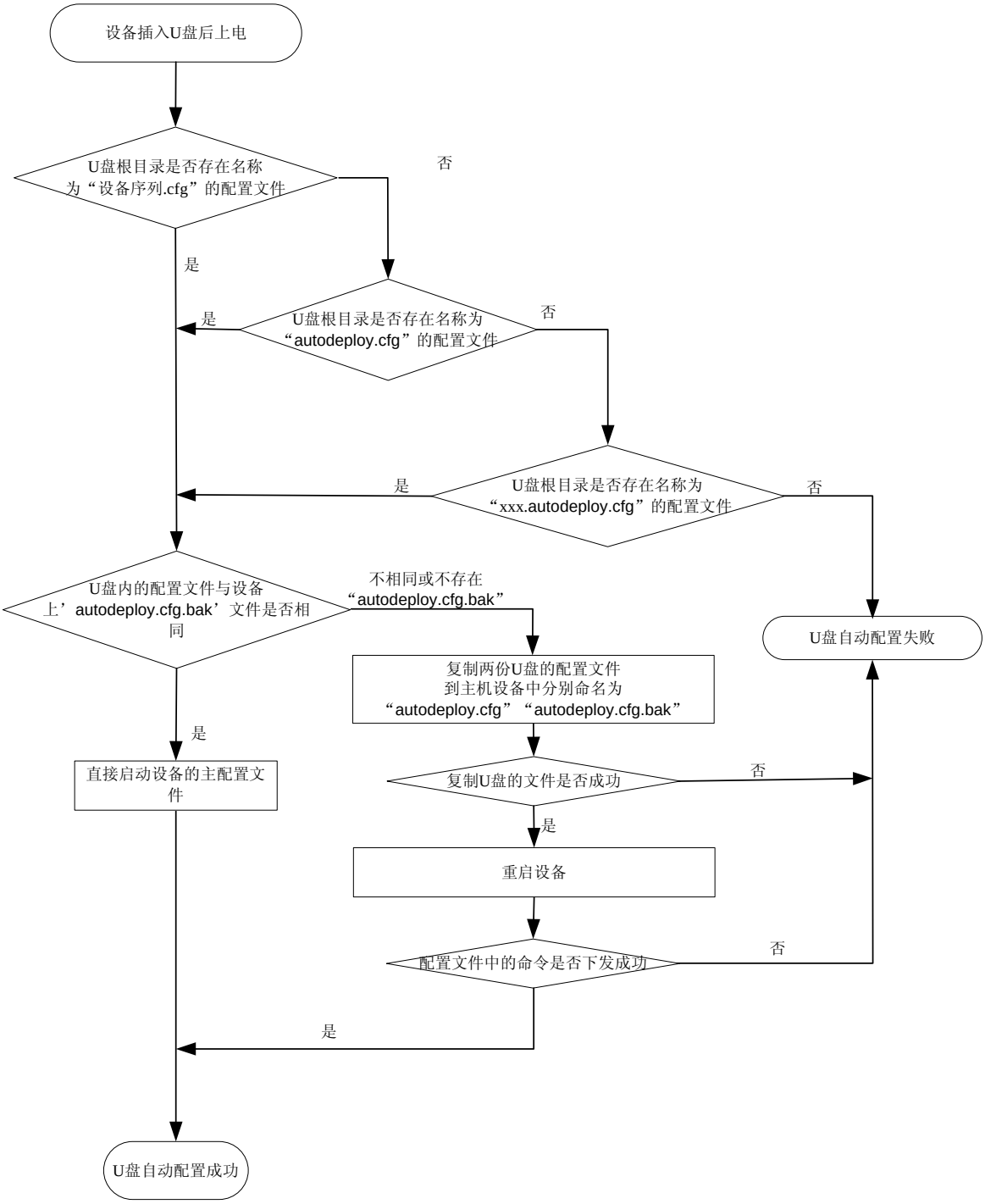
(3) 如果存在配置文件“设备序列号.cfg”或“autodeploy.cfg”（优先使用以设备序列号命名的配置文件），则比较 U 盘中的配置文件与设备上的当前主配置文件是否相同：

- 如果相同，则直接启动设备的主配置文件，完成 U 盘自动配置。
- 如果不相同，则把 U 盘中的配置文件复制到设备中，并设置为下次启动的配置文件。如果拷贝文件失败，则认为自动配置失败。
- 如果设备有预读配置的模块设备将重启。
- 如果自动配置失败，则把失败的 log 写到 U 盘根目录下，log 文件名为“配置文件全名.log”。

说明

- 配置文件必须保存在 U 盘的根目录下，文件名必须是“设备序列号.cfg”或“autodeploy.cfg”
- 把 U 盘中的配置文件复制到设备中时，如果与设备上下次启动文件同名则备份设备上原配置文件为”原名”+”_bak.cfg”。如果设备上有同名文件但不是下次启动配置文件则直接覆盖。
- 如果执行过程中有失败，生成的 log 文件名为“配置文件全名.log”。
- 只支持单主控 U 盘配置恢复。配置恢复完成后需拔出 U 盘。
- 必须在启动设备前插入 U 盘，设备正常运行过程中插入 U 盘不会执行 U 盘自动配置功能。
- 如果插入两个 U 盘，只检查第一个 U 盘，即 usba0:。
- U 盘自动配置成功时，系统（SYS）指示灯绿色快速闪烁 5 秒；U 盘自动配置失败时，系统（SYS）指示灯黄色快速闪烁 10 秒。

图1-4 U 盘自动配置流程图



1.3.2 开启U盘自动配置功能

表1-2 开启 U 盘自动配置功能

操作	命令	说明

操作	命令	说明
开启U盘自动配置功能	**autodeploy udisk enable**	必选 该操作在系统视图下执行 缺省情况下，设备的U盘自动配置功能处于开启状态

目 录

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。

目前的设备管理主要提供配置设备名称、配置系统时间、重启设备和配置单板的温度告警门限等功能，本文将分别详细介绍。

1.1 设备管理配置任务简介

配置任务	说明	详细配置
配置设备名称	必选	1.2
配置系统时间	必选	1.3
使能版权信息显示功能	可选	1.4
配置欢迎信息	可选	1.5
配置设备重启	可选	1.6
配置定时执行任务功能	可选	1.7
配置密码恢复功能	可选	1.9
电源管理	必选	1.10
配置端口状态检测定时器	可选	1.11
监控CPU利用率	可选	1.12
配置内存告警门限	必选	1.13
关闭USB接口	可选	1.14
配置接口卡的工作模式	必选	1.15
可插拔接口模块的识别与诊断	必选	1.16
恢复出厂状态	可选	1.17

1.2 配置设备名称

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>。

表1-1 配置设备名称

操作	命令	说明
进入系统视图	**system-view**	-
设置设备名称	**sysname** *sysname*	缺省设备名称为H3C

1.3 配置系统时间

1.3.1 配置时间协议

设备的系统时间有以下几种获取方式：

- **none**：表示通过本地时钟源获取系统时间。配置该参数后，用户可通过命令行修改系统时间。
- **ntp**：表示通过 NTP（Network Time Protocol，网络时间协议）协议获取系统时间。配置该参数后，用户不能通过命令行修改系统时间，需要配置 NTP 相关参数才能获取到时钟。关于 NTP 的详细介绍和配置，请参见“网络管理和监控配置指导”中的“NTP”。

表1-2 配置系统时间的获取方式

操作	命令	说明
进入系统视图	**system-view**	-
配置系统时间的获取方式	**clock protocol** { **none** | **ntp** }	多次使用该命令配置不同的系统时间获取方式时，新配置将覆盖旧配置

1.3.2 通过命令行修改系统时间

当配置系统时间的获取方式为 **none** 时，系统时间由 UTC（Coordinated Universal Time，国际协调时间）时间、本地时区和夏令时运算得出，通过 **display clock** 命令可以查看。为了保证与其它设备协调工作，用户需要将系统时间配置准确。

配置系统时间后，设备内的时钟能够从配置时间开始自动计时。但如果重启设备，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。

表1-3 配置系统时间

操作	命令	说明
设置UTC时间	**clock datetime** *time date*	该命令在用户视图下执行
进入系统视图	**system-view**	-
配置系统所在的时区	**clock timezone** *zone-name* { **add** | **minus** } *zone-offset*	缺省情况下，本地时区采用UTC时区
设置夏令时	**clock summer-time** *name start-time start-date end-time end-date add-time*	缺省情况下，没有配置夏令时

1.4 使能版权信息显示功能

- 使能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、AUX 口或 Modem 方式登录设备再退出用户视图时会显示版权信息，其它情况不显示版权信息。显示的版权信息形如：

```
******************************************************************************
* Copyright (c) 2004-2013 Hangzhou H3C Tech. Co., Ltd. All rights reserved.  *
```

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

- 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。

表1-4 使能版权信息显示功能

操作	命令	说明
进入系统视图	**system-view**	-
使能版权信息显示功能	**copyright-info enable**	缺省情况下，版权信息显示功能处于使能状态

1.5 配置欢迎信息

1.5.1 欢迎信息简介

欢迎信息是用户在连接到设备后、进入 CLI 配置界面前系统显示的一段提示信息。管理员可以根据需要，设置相应的欢迎信息。

按照同时配置时，显示顺序的先后，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。
- incoming 欢迎信息或者 shell 欢迎信息。Modem 拨号用户登录时显示 incoming 欢迎信息，其它方式登录的用户显示 shell 欢迎信息。

1.5.2 输入欢迎信息

输入欢迎信息时，信息内容支持单行输入和多行输入两种方式：

(1) 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，并且不会出现在欢迎信息的内容中。此时包括命令关键字、起始符和结束符在内，一共可以输入 510 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，设置 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.%
```

(2) 多行输入

该方式下，通过回车键将欢迎信息分多行输入，此时包括命令关键字、起始符和结束符在内，一共可以输入 2000 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设置，“%”不属于欢迎信息的内容。例如，设置的欢迎信息为“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，以结束符结束设置。起始符和结束符不属于欢迎信息的内容。例如，设置的欢迎信息为“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，以结束符结束设置。起始符和结束符不属于欢迎信息的内容。例如，设置的欢迎信息为“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

- 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。

1.5.3 配置欢迎信息

表1-5 配置欢迎信息

操作	命令	说明
进入系统视图	**system-view**	-
配置legal欢迎信息	**header legal** *text*	可选
配置MOTD欢迎信息	**header motd** *text*	可选
配置login欢迎信息	**header login** *text*	可选
配置incoming欢迎信息	**header incoming** *text*	可选
配置shell欢迎信息	**header shell** *text*	可选

1.6 配置设备重启

提示

重新启动会导致业务中断，请谨慎使用。

1. 简介

重启设备的方式有三种：

- 通过断电后重新上电来重启设备（该方式又称为硬件重启或者冷启动）。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。
- 通过命令行立即重启设备。
- 通过命令行定时重启设备。该方式下，用户可以设置一个时间点，让设备在该时间点自动重启，或者设置一个时延，让设备经过指定时间后自动重启。

后两种方式都属于命令行重启。命令行重启又称为热启动，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。

2. 配置准备

- 重启前请使用 **save** 命令保存当前配置，以免重启后配置丢失。（**save** 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”）
- 重启前请使用 **display startup** 和 **display boot-loader** 命令分别确认是否设置了合适的下次启动配置文件和下次启动文件。如果主用启动文件损坏或者不存在，则不能通过 **reboot** 命令重启设备。此时，可以通过指定新的主用启动文件再重启。**display startup** 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”，**display boot-loader** 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. 配置步骤

当多次使用 **scheduler reboot at** 或者 **scheduler reboot delay** 命令配置重启时间时，最新的配置生效。

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。

表1-6 通过命令行立即重启设备

操作	命令	说明
立即重启设备或者指定子卡（MSR 2600/MSR 3600）	**reboot** [**slot** *slot-number*] [**force**]	该命令在用户视图下执行
立即重启指定单板、指定子卡或整台设备（MSR 5600）	**reboot** [**slot** *slot-number* [**subslot** *subslot-number*]] [**force**]	该命令在用户视图下执行

表1-7 通过命令行定时重启设备

操作	命令	说明
指定设备重启的具体时间和日期	**scheduler reboot at** *time* [*date*]	二者选其一 缺省情况下，没有配置重启设备的时间 使用该方式配置定时重启后，如果发生主备倒换，则定时重启配置将自动取消（MSR 5600） 两命令均在用户视图下执行
配置重启设备的延迟时间	**scheduler reboot delay** *time*	

1.7 配置定时执行任务功能

1.7.1 定时执行任务功能简介

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。

1.7.2 配置定时执行任务

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。

设置的时间点到达时，系统将在后台执行指定命令，不显示任何输出信息（log、trap、debug 等系统信息除外）。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。

配置时需要注意的是：

- 通过 **command** 指定的命令行必须是设备上可成功执行的命令行，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。
- 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”。

表1-8 配置定时执行任务（一次性执行）

操作	命令	说明
进入系统视图	**system-view**	-
创建Job	**scheduler job** *job-name*	缺省情况下，没有创建Job
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
创建Schedule	**scheduler schedule** *schedule-name*	缺省情况下，没有创建Schedule

操作	命令	说明
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
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。同一个Schedule最多可以配置64个用户角色
配置在指定时刻执行Schedule	**time at** *time date*	三者选其一 缺省情况下，没有为Schedule配置执行时间 使用该方式配置定时执行功能后，即便执行**clock datetime**、**clock summer-time**或**clock timezone**命令调整了系统时间，也不会影响该任务的配置
为Schedule配置执行时间	**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*	

表1-9 配置定时执行任务（循环执行）

操作	命令	说明
进入系统视图	**system-view**	-
创建Job	**scheduler job** *job-name*	缺省情况下，没有创建Job
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
创建Schedule	**scheduler schedule** *schedule-name*	缺省情况下，没有创建Schedule
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。多个Job在Schedule指定的时间同时执行，没有先后顺序
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。同一个Schedule最多可以配置64个用户角色
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>]	二者选其一 缺省情况下，没有为Schedule配置执行时间 使用该方式配置定时执行功能后，即便执行**clock datetime**、**clock summer-time**或**clock timezone**命令调整了系统时间，也不会影响该任务的配置
为Schedule配置循环执行周期	**time repeating** [**at** *time* [*date*]] **interval** *interval-time*	

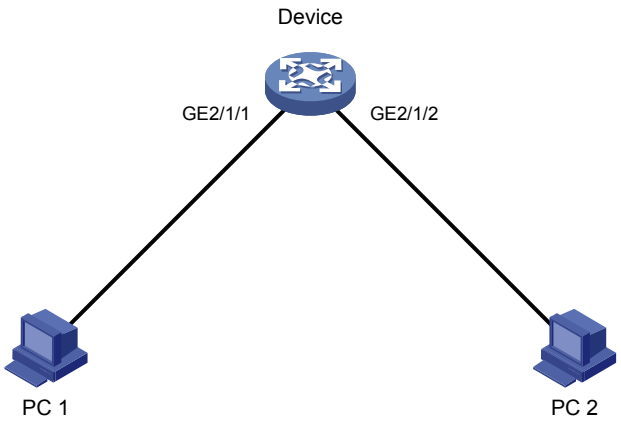
1.7.3 定时执行任务典型配置举例

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 GigabitEthernet2/1/1 和 GigabitEthernet2/1/2，其它时间关闭端口，以便起到有效节能的作用。

2. 组网图

图1-1 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 GigabitEthernet2/1/1 的 Job。

```
[Sysname] scheduler job shutdown-GigabitEthernet2/1/1
[Sysname-job-shutdown-GigabitEthernet2/1/1] command 1 system-view
[Sysname-job-shutdown-GigabitEthernet2/1/1] command 2 interface gigabitethernet 2/1/1
[Sysname-job-shutdown-GigabitEthernet2/1/1] command 3 shutdown
[Sysname-job-shutdown-GigabitEthernet2/1/1] quit
```

创建开启 GigabitEthernet2/1/1 的 Job。

```
[Sysname] scheduler job start-GigabitEthernet2/1/1
[Sysname-job-start-GigabitEthernet2/1/1] command 1 system-view
[Sysname-job-start-GigabitEthernet2/1/1] command 2 interface gigabitethernet 2/1/1
[Sysname-job-start-GigabitEthernet2/1/1] command 3 undo shutdown
[Sysname-job-start-GigabitEthernet2/1/1] quit
```

创建关闭 GigabitEthernet2/1/2 的 Job。

```
[Sysname] scheduler job shutdown-GigabitEthernet2/1/2
[Sysname-job-shutdown-GigabitEthernet2/1/2] command 1 system-view
[Sysname-job-shutdown-GigabitEthernet2/1/2] command 2 interface gigabitethernet 2/1/2
[Sysname-job-shutdown-GigabitEthernet2/1/2] command 3 shutdown
[Sysname-job-shutdown-GigabitEthernet2/1/2] quit
```

创建开启 GigabitEthernet2/1/2 的 Job。

```
[Sysname] scheduler job start-GigabitEthernet2/1/2
[Sysname-job-start-GigabitEthernet2/1/2] command 1 system-view
```

```
[Sysname-job-start-GigabitEthernet2/1/2] command 2 interface gigabitethernet 2/1/2
[Sysname-job-start-GigabitEthernet2/1/2] command 3 undo shutdown
[Sysname-job-start-GigabitEthernet2/1/2] 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-GigabitEthernet2/1/1
[Sysname-schedule-START-pc1/pc2] job start-GigabitEthernet2/1/2
[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-GigabitEthernet2/1/1
[Sysname-schedule- STOP-pc1/pc2] job shutdown-GigabitEthernet2/1/2
[Sysname-schedule- STOP-pc1/pc2] time repeating at 18:00 week-day mon tue wed thu fri
[Sysname-schedule- STOP-pc1/pc2] quit
```

4. 结果验证

显示 Job 的配置信息。

```
[Sysname] display scheduler job
Job name: shutdown-GigabitEthernet2/1/1
 system-view
 interface gigabitethernet 2/1/1
 shutdown

Job name: shutdown-GigabitEthernet2/1/2
 system-view
 interface gigabitethernet 2/1/2
 shutdown

Job name: start-GigabitEthernet2/1/1
 system-view
 interface GigabitEthernet 2/1/1
 undo shutdown

Job name: start-GigabitEthernet2/1/2
 system-view
 interface gigabitethernet 2/1/2
 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 2013
Last execution time  : Wed Sep 28 08:00:00 2013
Last completion time : Wed Sep 28 08:00:03 2013
Execution counts     : 1
----------------------------------------------------------------------
Job name                                        Last execution status
```

```
start-GigabitEthernet2/1/1                                  Successful
start-GigabitEthernet2/1/2                                  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 2013
Last execution time  : Wed Sep 28 18:00:00 2013
Last completion time : Wed Sep 28 18:00:01 2013
Execution counts     : 1
-------------------------------------------------------------------
Job name                                        Last execution status
shutdown-GigabitEthernet2/1/1                           Successful
shutdown-GigabitEthernet2/1/2                           Successful
```

显示 Job 运行的输出信息。

```
[Sysname] display scheduler logfile
Job name        : start-GigabitEthernet2/1/1
Schedule name   : START-pc1/pc2
Execution time  : Wed Sep 28 08:00:00 2013
Completion time : Wed Sep 28 08:00:02 2013
--------------------------------- Job output ---------------------------------
<Sysname>system-view
System View: return to User View with Ctrl+Z.
[Sysname]interface gigabitethernet 2/1/1
[Sysname-GigabitEthernet2/1/1]undo shutdown

Job name        : start-GigabitEthernet2/1/2
Schedule name   : START-pc1/pc2
Execution time  : Wed Sep 28 08:00:00 2013
Completion time : Wed Sep 28 08:00:02 2013
--------------------------------- Job output ---------------------------------
<Sysname>system-view
System View: return to User View with Ctrl+Z.
[Sysname]interface gigabitethernet 2/1/2.
[Sysname-GigabitEthernet2/1/2]undo shutdown

Job name        : shutdown-GigabitEthernet2/1/1
Schedule name   : STOP-pc1/pc2
Execution time  : Wed Sep 28 18:00:00 2013
Completion time : Wed Sep 28 18:00:01 2013
--------------------------------- Job output ---------------------------------
<Sysname>system-view
System View: return to User View with Ctrl+Z.
[Sysname]interface gigabitethernet 2/1/1
[Sysname-GigabitEthernet2/1/1]shutdown

Job name        : shutdown-GigabitEthernet2/1/2
Schedule name   : STOP-pc1/pc2
Execution time  : Wed Sep 28 18:00:00 2013
```

```
Completion time : Wed Sep 28 18:00:01 2013
------------------------------- Job output ---------------------------------
<Sysname>system-view
System View: return to User View with Ctrl+Z.
[Sysname]interface gigabitethernet 2/1/2
[Sysname-GigabitEthernet2/1/2]shutdown
```

1.8 配置HMIM接口模块的热插拔

将 HMIM 接口模块直接插入插槽中即可完成该接口模块的安装。

HMIM 接口模块在设备运行的过程中，可以通过以下命令卸载该接口模块。

表1-1 卸载 HMIM 接口模块

操作	命令	说明
卸载HMIM接口模块	**remove hmimslot** *slot-number*	必选 该命令在用户视图下执行

注意

该命令会使某单板不可用，从而导致业务中断，请谨慎使用。

MSR 系列路由器各款型对于本节所描述的特性的支持情况有所不同，详细差异信息如下：

型号	特性	描述
MSR 2600	卸载HMIM接口模块	不支持
MSR 3600		支持
MSR 5600		支持

1.9 配置密码恢复功能

配置密码恢复功能后，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Boot ROM菜单，再选择对应的Boot ROM菜单选项来修复这个问题。用户可选用的修复选项和密码恢复功能是否使能有关，详见 图 1-2。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Boot ROM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。

除了修复选项，Boot ROM 菜单中支持配置的其它选项也与密码恢复功能的使能状态有关，详见产品的相关手册。

图1-2 Console 口登录认证失败后的解决方法

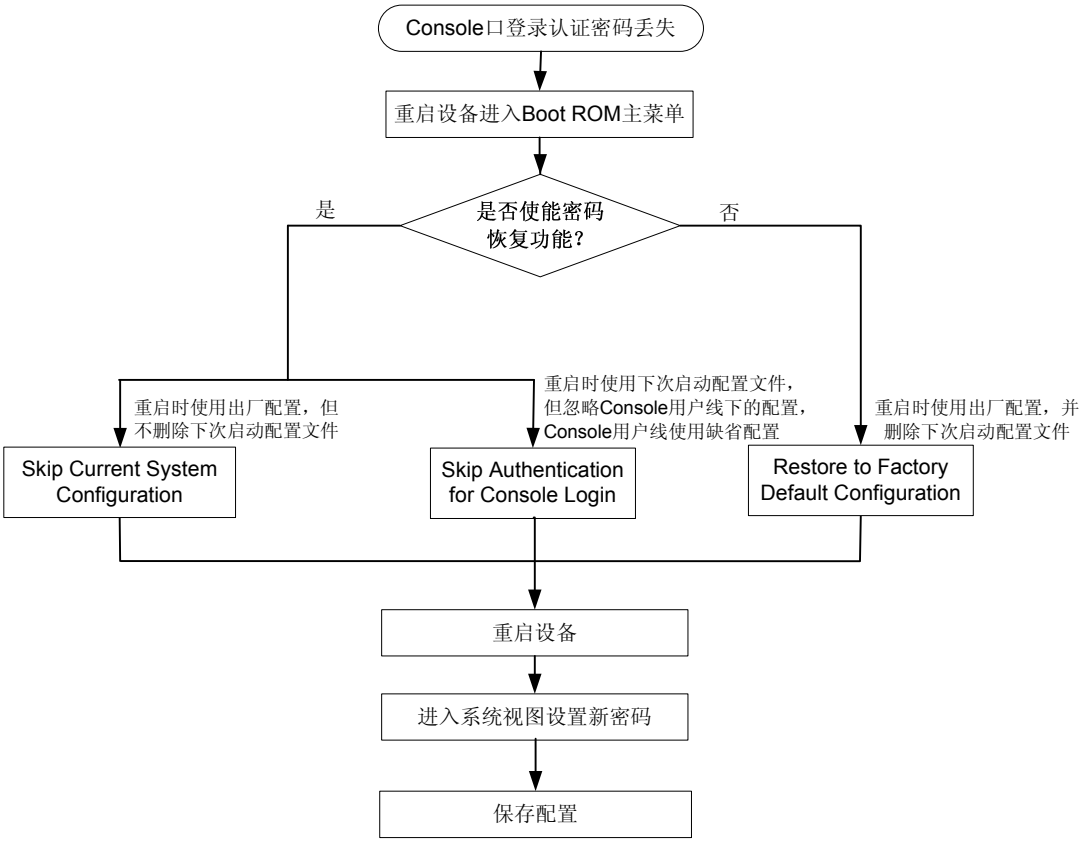


表1-10 配置密码恢复功能

操作	命令	说明
进入系统视图	**system-view**	-
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

1.10 电源管理

1.10.1 使能电源管理功能

MSR 系列路由器各款型对于本节所描述的特性的支持情况有所不同，详细差异信息如下：

型号	特性	描述
MSR 2600	电源管理	不支持
MSR 3600		不支持
MSR 5600		支持

某些电源具有自我保护机制，当电源模块发生过载、过流、过压、过温、短路等故障时，电源会进行自我硬件保护（比如：当电源由于输出过压而告警时，电源可能进入锁死状态、停止对整个机框

进行供电，以便保护电源和设备不被损坏）。这样虽然保护了电源和设备的安全使用，但会对设备的正常使用造成一定的影响，严重时将导致业务全部中断。为了尽可能减小这种影响，用户可通过启用电源管理功能，尽可能的避免电源模块发生过载现象。

电源管理功能的原理是，系统实时监控电源的可用功率和系统负载，在电源将要过载、进行自身硬件保护之前，采取保护措施（比如给用户发送提示信息、启用冗余电源以及抑制接口板供电）。

冗余电源是从总电源中预留的一部分电源，用于电源备份，比如当前插入了 3 个电源模块，可以将其中的 1 个设备设置为冗余电源。冗余电源的配置并不影响系统总电源的使用，如果使能了电源管理功能并配置了冗余电源，当电源模块故障或被拔出、或者设备耗电量增加导致不能维持配置的冗余模块数时，系统会自动启用冗余电源，请使用 **display power-supply** 命令随时了解电源的使用情况，以便提前采取措施预防。

该功能的作用体现在以下两个方面：

- 接口板插入时，如果没有使能电源管理功能，系统会直接给接口板上电，这样可能会因为电源供电不足导致电源停止对整个机框供电；如果使能了电源管理功能，系统会先比较待上电接口板的最大功耗和系统的剩余功率，当最大功耗小于等于剩余功率时，才给接口板供电，当最大功耗大于剩余功率时，会启用冗余电源，如果仍然不够接口板的最大功耗，则不给接口板供电。
- 电源模块故障或者被拔出导致供电不足时，如果没有使能电源管理功能，电源会进行自我硬件保护；如果使能了电源管理，系统会启用冗余电源，当没有冗余电源可用时，则使用电源的自我硬件保护机制。

表1-11 使能电源管理功能

操作	命令	说明
进入系统视图	**system-view**	-
使能电源管理功能	**power-supply policy enable**	缺省情况未使能电源管理功能
配置冗余电源模块数	**power-supply policy redundant** *module-count*	缺省情况冗余电源模块数目为0 只有在电源管理功能使能的情况下该命令配置后才会生效

1.10.2 手工给单板供电与断电

当系统供电不足时，设备会按照一定的机制自动对单板供电（具体原则请参见 1.10.1 ），用户也可以通过**display power-supply**命令随时了解电源的使用情况以及各单板的供电情况，再结合网络业务情况，手工对单板进行供电和断电操作，来调节系统可用功率。

表1-12 手工给单板供电/断电（MSR 2600/MSR 3600）

操作	命令	说明
手工给指定单板供电	**power-supply on slot** *slot-number*]	本命令在用户视图下执行
强制给指定单板断电	**power-supply off slot** *slot-number*	本命令在用户视图下执行

表1-13 手工给单板供电/断电（MSR MSR 5600）

操作	命令	说明
手工给指定单板供电	**power-supply on slot** *slot-number* [**subslot** *subslot-number*]	本命令在用户视图下执行
强制给指定单板断电	**power-supply off slot** *slot-number* [**subslot** *subslot-number*]	本命令在用户视图下执行

1.11 配置端口状态检测定时器

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。

表1-14 配置端口状态检测定时器

操作	命令	说明
进入系统视图	**system-view**	-
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

1.12 监控CPU利用率

开启 CPU 利用率历史记录功能后，系统每隔一定时间（可通过 **monitor cpu-usage interval** 命令配置）会对 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，以便用户监控设备近期的运行情况。

表1-15 监控 CPU 利用率（MSR 2600/MSR 3600）

操作	命令	说明
进入系统视图	**system-view**	-
开启CPU利用率历史记录功能	**monitor cpu-usage enable**	缺省情况下，CPU使用率历史记录功能处于开启状态
配置CPU利用率历史记录的采样周期	**monitor cpu-usage interval** *interval-value*	缺省情况下，CPU使用率历史记录采样周期为1分钟
退回用户视图	**quit**	-
显示CPU利用率的统计信息	**display cpu-usage**	该命令在任意视图下执行
显示CPU利用率历史信息记录功能相关配置	**display cpu-usage configuration**	该命令在任意视图下执行
以图表方式显示CPU利用率的历史记录	**display cpu-usage history** [**job** *job-id*]	该命令在任意视图下执行

表1-16 监控 CPU 利用率（MSR 5600）

操作	命令	说明
进入系统视图	**system-view**	-
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
配置CPU利用率历史记录的采样周期	**monitor cpu-usage interval** *interval-value* [**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
退回用户视图	**quit**	-
显示CPU利用率的统计信息	**display cpu-usage** [**slot** *slot-number* [**cpu** *cpu-number*]]	该命令在任意视图下执行
显示CPU利用率历史信息记录功能相关配置	**display cpu-usage configuration** [**slot** *slot-number* [**cpu** *cpu-number*]]	该命令在任意视图下执行
以图表方式显示CPU利用率的历史记录	**display cpu-usage history** [**job** *job-id*] [**slot** *slot-number* [**cpu** *cpu-number*]]	该命令在任意视图下执行

1.13 配置内存告警门限

系统实时监控系统剩余空闲内存大小，当条件达到时，就产生相应的告警/告警解除通知，以便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。

设备支持一级（**minor**）、二级（**severe**）和三级（**critical**）三个级别的门限，对应的系统剩余空闲内存越来越少，紧急程度越来越严重，关联模块根据收到的不同级别的告警可以采取不同的响应。

- 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 1-3 中曲线所示时，会生成如 图 1-3 所示的告警和解除告警通知。

图1-3 内存告警示意图

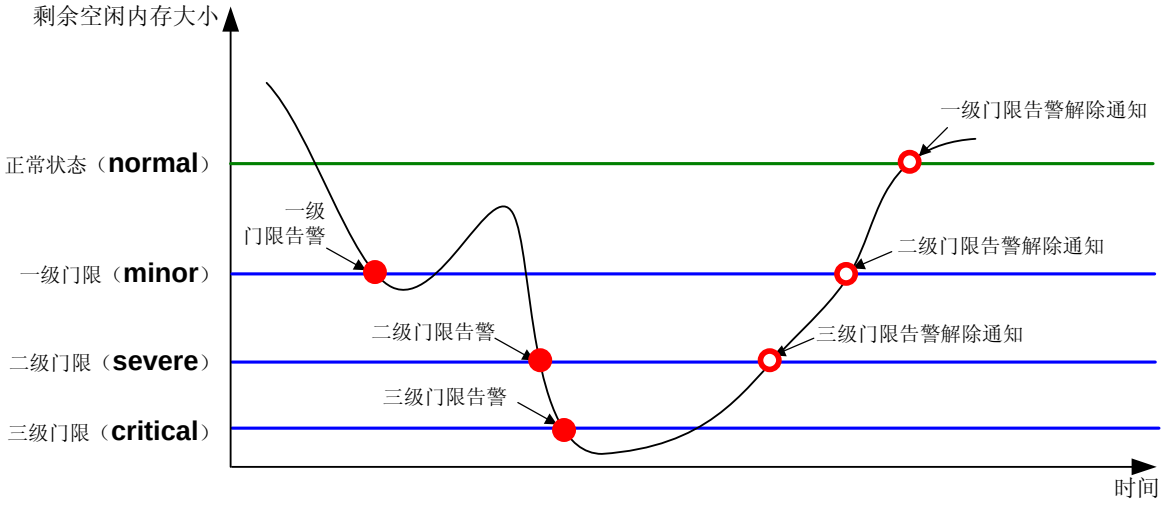


表1-17 配置内存告警门限

操作	命令	说明
进入系统视图	**system-view**	-
配置内存告警的门限值（MSR 2600/MSR 3600）	**memory-threshold minor** *minor-value* **severe** *severe-value* **critical** *critical-value* **normal** *normal-value*	缺省情况下，一级告警门限为96MB，二级告警门限为64MB，三级告警门限为48MB，系统恢复到正常的内存门限为128MB
配置内存告警的门限值（MSR 5600）	**memory-threshold** [**slot** *slot-number* [**cpu** *cpu-number*]] **minor** *minor-value* **severe** *severe-value* **critical** *critical-value* **normal** *normal-value*	缺省情况下，一级告警门限为96MB，二级告警门限为64MB，三级告警门限为48MB，系统恢复到正常的内存门限为128MB

1.14 关闭USB接口

用户可通过 USB 口进行文件的上传和下载或者接 USB 3G Modem 模块。缺省状态下 USB 口处于开启状态，用户可根据需要关闭 USB 口。

表1-18 关闭 USB 接口

操作	命令	说明
进入系统视图	**system-view**	-
关闭设备上所有的USB接口	**usb disable**	缺省情况下，设备上所有的USB接口处于开启状态

1.15 配置接口卡的工作模式

对于支持一卡多用的接口卡，使用该特性可完成整个接口卡工作模式的切换。模式切换成功后，该接口卡上的接口就可以当成另外一种类型的接口使用。

表1-19 配置接口卡的工作模式（MSR 2600/MSR 3600）

操作	命令	说明
进入系统视图	**system-view**	-
（可选）设置接口卡的工作模式	**card-mode slot** *slot-number mode-name*	*mode-name*的实际取值与接口卡的型号有关，请以接口卡的实际情况为准

表1-20 配置接口卡的工作模式（MSR 5600）

操作	命令	说明
进入系统视图	**system-view**	-
（可选）设置接口卡的工作模式	**card-mode slot** *slot-number* **subslot** *subslot-number mode-name*	*mode-name*的实际取值与接口卡的型号有关，请以接口卡的实际情况为准

1.16 可插拔接口模块的识别与诊断

1.16.1 识别可插拔接口模块

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，在单板或者设备的调试、测试过程中被写入到设备的存储器件中，包括单板的名称、生产序列号、MAC 地址、制造商等信息。

表1-21 识别可插拔接口模块信息

操作	命令	说明
显示可插拔接口模块的主要特征参数	**display transceiver** { **interface** [*interface-type interface-number*] }	本命令在任意视图下执行
显示可插拔接口模块的电子标签信息	**display transceiver manuinfo interface** [*interface-type interface-number*] }	本命令在任意视图下执行

1.16.2 诊断可插拔接口模块

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，以便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。

表1-22 诊断可插拔接口模块

操作	命令	说明
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*] }	本命令在任意视图下执行
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*] }	本命令在任意视图下执行

1.16.3 关闭可插拔模块告警信息开关

MSR 系列路由器各款型对于本节所描述的特性的支持情况有所不同，详细差异信息如下：

型号	特性	描述
MSR 2600	关闭可插拔模块告警信息开关	不支持
MSR 3600		• MSR3600-28/3600-51 不支持 • MSR 36-10/MSR 36-20/MSR 36-40/MSR 36-60 支持
MSR 5600		支持

当设备上插入的光模块的生产或定制厂商不是H3C时，设备会不停打印Trap和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。而 H3C 早期销售的光模块，可能没有记录厂商信息，但为了保护用户投资，这样的光模块还需要能继续正常使用。此时，可以关闭可插拔模块告警信息开关，停止输出相关告警信息。

表1-23 关闭可插拔模块告警信息开关

操作	命令	说明
进入系统视图	**system-view**	-
关闭可插拔模块告警信息开关	**transceiver phony-alarm-disable**	缺省情况下，可插拔模块告警信息开关处于开启状态

1.17 恢复出厂状态

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。执行 restore factory-default 命令后，设备将只保留“.bin”软件包、MAC 地址、电子标签等维持设备正常工作必需的信息，其它文件和参数均恢复到出厂状态。例如，设备存储介质根目录下的所有配置文件（即后缀为“.cfg”的文件）将被清除，设备在使用过程中生成的日志信息（即/logfile 下的“.log”文件以及 logbuffer 中的信息）、Trap 信息、Debug 信息将被清除，Boot ROM 菜单中各选项的值将恢复到缺省值等。因此，请谨慎使用本特性。

表1-24 恢复出厂状态

操作	命令	说明
将设备恢复到出厂状态	**restore factory-default**	执行该命令后，需手工重启设备才能使该命令生效 本命令在用户视图下执行

1.18 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。

表1-25 设备管理显示和维护（MSR 2600/MSR 3600）

操作	命令
显示设备的告警信息	**display alarm** [**slot** *slot-number*]
显示系统版本信息	**display version**
显示系统当前的时间、日期、本地时区以及夏令时配置	**display clock**
显示系统软件和硬件的详细版权信息	**display copyright**
显示设备信息	**display device** [**cf-card** | **usb**] [**slot** *slot-number* | **verbose**]
显示设备的电子标签信息	**display device manuinfo** [**slot** *slot-number*]
显示指定电源的电子标签信息	**display device manuinfo power** *power-id*
显示系统当前多个功能模块运行的统计信息	**display diagnostic-information** [**hardware** | **infrastructure** | **l2** | **l3** | **service**]
显示设备的温度信息	**display environment**
显示设备风扇的工作状态	**display fan** [*fan-id*]
显示设备的内存使用状态	**display memory**
显示内存告警门限相关信息	**display memory-threshold**
显示设备电源的信息	**display power-supply** [**verbose**]
显示Job的配置信息	**display scheduler job** [*job-name*]
显示Schedule日志文件的相关信息	**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** [*schedule-name*]
显示设备启动软件包版本更新操作的记录	**display version-update-record**
清除设备启动软件包版本更新操作的记录	**reset version-update-record**
清除Schedule日志文件的相关信息	**reset scheduler logfile**

表1-26 设备管理显示和维护（MSR 5600）

操作	命令
显示设备的告警信息	**display alarm** [**slot** *slot-number*]
显示系统版本信息	**display version**
显示系统当前的时间、日期、本地时区以及夏令时配置	**display clock**
显示系统软件和硬件的详细版权信息	**display copyright**
显示设备信息	**display device** [**cf-card** | **usb**] [**slot** *slot-number* [**subslot** *subslot-number*] | **verbose**]
显示设备的电子标签信息	**display device manuinfo** [**slot** *slot-number* [**subslot** *subslot-number*]]
显示指定风扇的电子标签信息	**display device manuinfo fan** *fan-id*
显示指定电源的电子标签信息	**display device manuinfo power** *power-id*
显示系统当前多个功能模块运行的统计信息	**display diagnostic-information** [**hardware** | **infrastructure** | **l2** | **l3** | **service**]
显示设备的温度信息	**display environment** [**slot** *slot-number*]
显示设备接口板上交换芯片的通道利用率信息	**display fabric utilization** [**slot** *slot-number*]
显示设备风扇的工作状态	**display fan** [*fan-id*]
显示设备的内存使用状态	**display memory** [**slot** *slot-number* [**cpu** *cpu-number*]]
显示内存告警门限相关信息	**display memory-threshold** [**slot** *slot-number* [**cpu** *cpu-number*]]
显示设备电源的信息	**display power-supply** [**verbose**]
显示Job的配置信息	**display scheduler job** [*job-name*]
显示Schedule日志文件的相关信息	**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** [*schedule-name*]
显示主用主控板启动软件包版本更新操作的记录	**display version-update-record**
清除主用主控板启动软件包版本更新操作的记录	**reset version-update-record**
清除Schedule日志文件的相关信息	**reset scheduler logfile**

目 录

1 Tcl

1.1 Tcl配置方式简介

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。

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 通过Tcl脚本配置设备

1.2.1 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：

- 如果输入的是 Tcl 脚本命令，不支持输入?键获得在线帮助和 Tab 键补全功能；如果输入的是 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 配置”。
- 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，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。
- 在 Tcl 中定义的环境变量可以应用到 Comware 系统的命令。
- 支持在同一行写多条 Comware 系统的命令，命令间用分号隔开，多条命令会一起下发，按照下发顺序执行。

1.2.2 进入Tcl配置视图

表1-1 进入 Tcl 配置视图

操作	命令	说明
进入Tcl配置视图	**tclsh**	该命令在用户视图下执行

1.2.3 退出Tcl配置视图

- 如果在 Tcl 配置视图下使用了 Comware 命令进入了子视图，则只能用 **quit** 命令退回到上一级视图，不能执行 **tclquit** 命令。
- 执行 **tclquit** 命令效果等同于在 Tcl 配置视图下执行 **quit** 命令。

表1-2 退出 Tcl 配置视图

操作	命令	说明
从Tcl配置视图退回到用户视图	**tclquit**	该命令在Tcl配置视图下执行

目 录

1 简介

H3C MSR 2600/3600/5600 路由器的启动软件包括 BootWare 文件和 4 个功能软件包。这 4 个功能软件包根据其包含应用软件的功能特性分别命名为基础软件包、数据软件包、安全软件包和语音软件包，其中除基础软件包之外的三个软件包均需要激活和安装相应功能的 License 才能使用。

- 基础软件包：包含系统的一些基本功能，约 80 个特性，不需要激活和安装 License。
- 数据软件包：包含 MPLS、DLSw 等数据相关特性，需要完成数据 License 的激活和安装。
- 安全软件包：包含 VPN 等安全相关特性，需要完成安全 License 的激活和安装。
- 语音软件包：包含 BUSYOUT、VOICE 等语音相关特性，需要完成语音 License 的激活和安装。

H3C 网站提供 License 的激活申请功能。H3C 网站根据设备序列号和用户购买的《软件使用授权书》上的授权码等信息，激活并生成相应的 License 文件。只有将 License 文件安装到设备上，才能使用相应软件包中的软件功能。

说明

设备必须安装有 BootWare 文件和基础软件包才能正常运行，其它软件包可以根据用户需要选择安装。

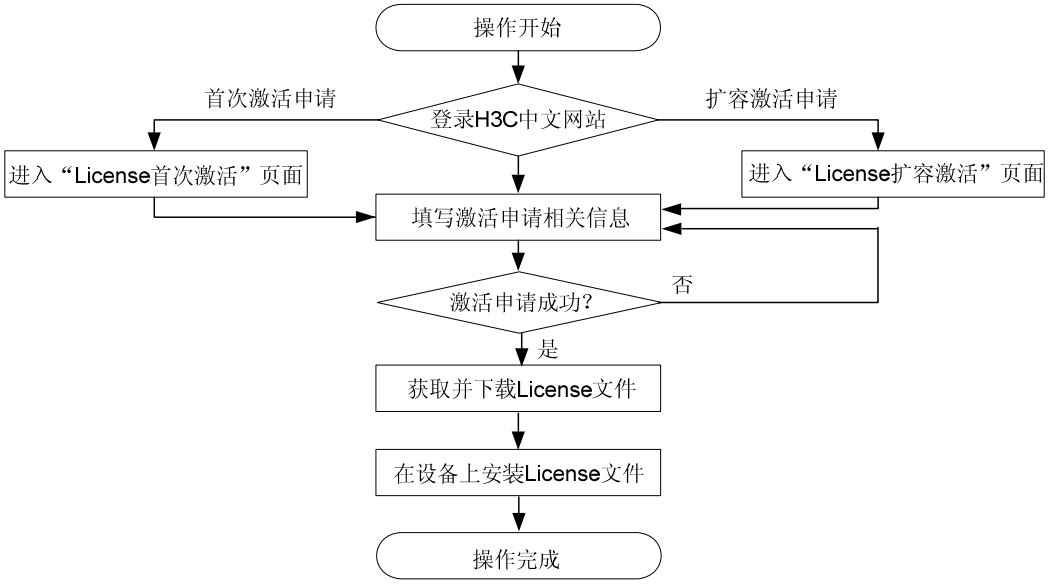
2 License的激活和安装流程

License 的激活申请有两种类型：

- License首次激活申请：如果设备是第一次申请激活文件（License文件），那么需要完成 License首次激活申请；
- License扩容激活申请：如果设备已经申请过激活文件（License文件），又需要申请其它类型的激活文件时，那么需要完成 License扩容激活申请。

License 激活申请完成后，还需要将 License 文件安装到设备上。

图2-1 License 激活示意图

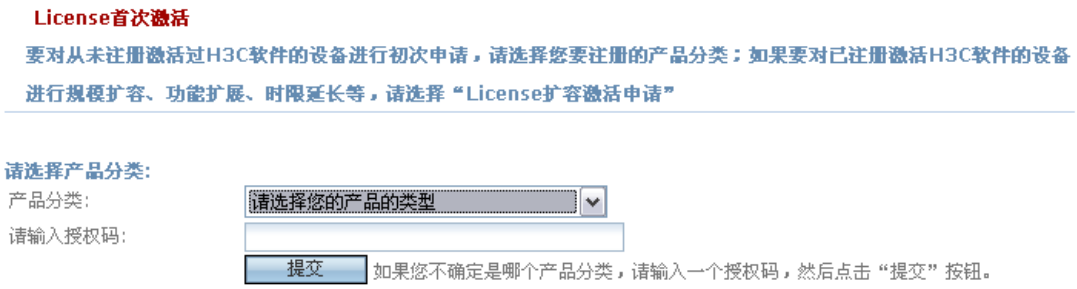


3 License的激活申请

3.1 License首次激活申请

步骤1 访问H3C公司中文网站www.h3c.com.cn，依次点击“服务支持-> 授权业务-> License首次激活申请”，即可进入如 图 3-1所示的“License首次激活”页面。

图3-1 License 首次激活页面



步骤2 在“产品分类”中选择“路由器_H3C MSR26”或者“路由器_H3C MSR36”或者“路由器_H3C MSR56”。如果不知道产品所属的分类，可以通过输入授权码的方式，自动联想出“产品分类”。

图3-2 选择产品类型

步骤3 在弹出来的“授权信息”、“设备信息”和“用户信息”对话框中，根据 表 3-1中的说明，输入相应的信息，然后勾选“已阅读并同意法律声明所述服务条款各项内容”，最后点击按钮<获取激活码（文件）>。

图3-3 输入 License 首次激活信息

表3-1 License 首次激活申请信息说明

项目	说明	
授权码	《软件使用授权书》上的授权序列号	必选
H3C设备S/N	设备的固有序列号，20位的数字或字母。可以通过**display license device-id**命令获取。 注意 该序列号不是《软件使用授权书》上的授权序列号	必选
DID	设备的Device ID，32位的数字或字母。可以通过**display license device-id**命令获取。	必选
最终客户单位名称	使用设备的最终用户的单位名称	必选
申请单位名称	您所在的工作单位名称	必选
申请联系人姓名	您的姓名	必选
申请联系人电话	您的联系电话	必选

项目	说明	
申请联系人E-mail	您的E-mail邮箱 除了“操作成功”对话框附带激活申请下来的License文件链接之外，H3C网站还会将License文件也发送一份到您的E-mail邮箱	必选
申请联系人邮编	您所在地区的邮政编码	可选
申请联系人地址	您的联系地址	可选
项目名称	应用路由器设备的项目名称	可选
验证码	网站显示的验证码，按照右边显示的数字，照样输入即可	必选

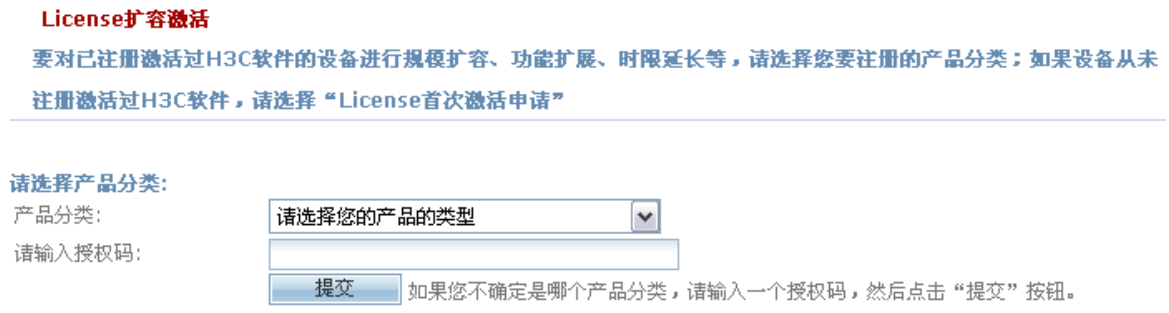
步骤4 如果 步骤 3的信息填写无误，系统将提示如 图 3-4所示的对话框，并且对话框中附有已经申请下来的License文件的链接，点击并下载License文件到本地PC，然后按照 4 License激活文件的安装中所述的方法，完成License文件的安装。

图3-4 License 首次激活申请操作成功

3.2 License扩容激活申请

步骤1 访问H3C公司中文网站www.h3c.com.cn，依次点击“服务支持-> 授权业务-> License扩容激活申请”，即可进入如 图 3-5所示的“License扩容激活”页面。

图3-5 License 扩容激活页面



步骤2 在“产品分类”中选择“路由器_H3C MSR26”或者“路由器_H3C MSR36”或者“路由器_H3C MSR56”。如果不知道产品所属的分类，可以通过输入授权码的方式，自动联想出“产品分类”。

图3-6 选择产品类型

步骤2 在弹出的“设备信息”对话框中，根据 License扩容激活申请用户信息说明的说明，输入相应的信息，然后点击<提交>按钮。

图3-7 输入 License 扩容激活用户信息

表3-2 License 扩容激活申请用户信息说明

项目	说明	
H3C设备S/N	设备的固有序列号，20位的数字或字母。可以通过**display license device-id**命令获取。 ⚠ 注意 该序列号不是《软件使用授权书》上的授权序列号	必选
DID	设备的Device ID，32位的数字或字母。可以通过**display license device-id**命令获取。	必选

步骤3 在弹出来的 “授权信息”和“用户信息”对话框中，根据 表 3-3中的说明，输入相应的信息，然后勾选“已阅读并同意法律声明所述服务条款各项内容”，最后点击按钮<获取激活码（文件）>。

图3-8 输入 License 扩容激活授权和用户信息

表3-3 License 扩容激活申请授权和用户信息说明

项目	说明	
授权码	《软件使用授权书》上的授权序列号	必选
最终客户单位名称	使用路由器设备的最终用户的单位名称	必选
申请单位名称	您所在的工作单位名称	必选
申请联系人姓名	您的姓名	必选
申请联系人电话	您的联系电话	必选
申请联系人E-mail	您的E-mail邮箱 除了“操作成功”对话框附带激活申请下来的License文件链接之外，H3C网站还会将License文件也发送一份到您的E-mail邮箱	必选
申请联系人邮编	您所在地区的邮政编码	可选
申请联系人地址	您的联系地址	可选
项目名称	应用路由器设备的项目名称	可选
验证码	网站显示的验证码，按照右边显示的数字，照样输入即可	必选

步骤4 如果 步骤 3的信息填写无误，系统将提示如 图 3-4所示的对话框，并且对话框中附有已经申请下来的License文件的链接，点击并下载License文件到本地PC，然后按照 4 License激活文件的安装 中所述的方法，完成License文件的安装。

图3-9 License 扩容激活申请操作成功

4 License激活文件的安装

(1) 将获取到的激活文件通过 FTP 或 TFTP 等方式上传到设备的存储介质上。

(2) 在系统视图下，通过 **license activation-file install** *filepath* 命令完成激活文件的安装，其中 filepath 为激活文件路径及名称。

```
<H3C> system-view
[H3C] license activation-file install cfa0:/CN29FV10112012092014434896415_data.ak
```

(3) 在用户视图下，可以通过 **display license** 命令查看 License 激活文件的状态信息，如果 Current State 显示为 In use，则说明安装成功。

```
<H3C> display license
cfa0:/license/CN29FV10112012092014434896415_data.ak
Feature: pkg_license
Product Description: H3C MSR 56 Data Software License
Registered at: 2012-03-23 03:56:53
License Type: Trial (days restricted)
Trial Time Left (days): 30
Current State: In use
```