H3C S5500-HI 系列以太网交换机

基础配置指导

杭州华三通信技术有限公司
http://www.h3c.com.cn

资料版本：6W102-20131220
产品版本：Release 52xx 系列

前 言

H3C S5500-HI 系列以太网交换机配置指导共分为十一本手册，介绍了 S5500-HI 系列以太网交换机 Release52xx 系列软件版本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》主要介绍如何使用命令行接口、如何登录交换机、对设备进行文件系统管理、设备管理、软件升级以及自动配置等功能的配置，包括 CLI、登录交换机、FTP 和 TFTP、文件系统管理、配置文件管理、软件升级、ISSU、设备管理以及自动配置。

前言部分包含如下内容：

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

新增及修改特性说明

本手册对应 S5500-HI 系列以太网交换机的 Release52xx 系列软件版本，各版本间特性差异如下：

- Release5206 与Release5203 版本相比，新增、修改了部分特性，具体请参见 表 1。
- Release5203 与Release5101 版本相比，新增、修改了部分特性，具体请参见 表 2。

表1 Release5206 与 Release5203 版本间特性差异

配置指导	新增及修改特性
FTP和TFTP	新增特性：配置FTP服务与SSL服务器端策略关联

表2 Release5203 与 Release5101 版本间特性差异

配置指导	新增及修改特性
CLI	修改特性：通过**super password**命令用来设置本地认证的密码时可采用哈希加密算法。
登录交换机	新增特性： • 配置 HTTP 发送的 IPv4、IPv6 报文的 DSCP 优先级 • 配置 Telnet 客户端发送的 IPv4、IPv6 报文的 DSCP 优先级 • 配置 Telnet 服务器发送的 IPv4、IPv6 报文的 DSCP 优先级

配置指导	新增及修改特性
	修改特性：通过**set authentication password**命令用来设置本地认证的密码时可采用哈希加密算法。
FTP和TFTP	新增特性： • 配置 FTP 服务器发送的 IPv4 报文的 DSCP 优先级 • 配置 TFTP 客户端发送的 IPv4、IPv6 报文的 DSCP 优先级 • 配置 FTP 客户端发送的 IPv4、IPv6 报文的 DSCP 优先级
文件系统管理	新增特性：验证文件的正确性和完整性配置
配置文件管理	新增特性：自动备份软件的配置文件 修改特性：出厂配置变更
软件升级	无
ISSU	无
设备管理	新增特性：密码修复功能 删除特性：禁止访问bootrom功能
自动配置	无

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. 图形界面格式约定

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

3. 各类标志

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

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

4. 图标约定

本书使用的图标及其含义如下：

	该图标及其相关描述文字代表一般网络设备，如路由器、交换机、防火墙等。
	该图标及其相关描述文字代表一般意义下的路由器，以及其他运行了路由协议的设备。
	该图标及其相关描述文字代表二、三层以太网交换机，以及运行了二层协议的设备。

5. 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 S5500-HI 系列以太网交换机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	产品彩页	帮助您了解产品的主要规格参数及亮点
	技术白皮书	帮助您了解产品和特性功能，对于特色及复杂技术从细节上进行介绍
硬件介绍及安装	安全兼容性手册	列出产品的兼容性声明，并对兼容性和安全的细节进行说明
	H3C 设备防雷安装指导手册	帮助您了解防雷接地设计和工程安装方法，以保证交换机具有良好的抗雷击性能
	快速安装指南	指导您对设备进行初始安装，通常针对最常用的情况，减少您的检索时间
	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
	风扇安装手册	帮助您了解产品支持的可插拔风扇模块的外观、功能、规格、安装及拆卸方法

大类	资料名称	内容介绍
	电源手册	帮助您了解产品支持的可插拔电源模块的外观、功能、规格、安装及拆卸方法
	RPS电源用户手册	帮助您了解产品支持的RPS电源的外观、功能、规格
	H3C低端系列以太网交换机RPS电源选购指南	帮助您了解各种RPS电源适用的交换机产品型号及RPS电源配套电缆的相关规格
	接口模块扩展卡用户手册	帮助您了解该接口模块扩展卡的外观、规格、安装及拆卸方法
	H3C低端系列以太网交换机可插拔模块手册	帮助您了解产品支持的可插拔模块类型、外观和规格
	H3C可插拔SFP[SFP+][XFP]模块安装指南	帮助您掌握SFP/SFP+/XFP模块的正确安装方法，避免因操作不当而造成器件损坏
业务配置	配置指导	帮助您掌握设备软件功能的配置方法及配置步骤
	命令参考	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	故障处理手册	指导您快速定位并处理软件故障
	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）

010-62982107

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！

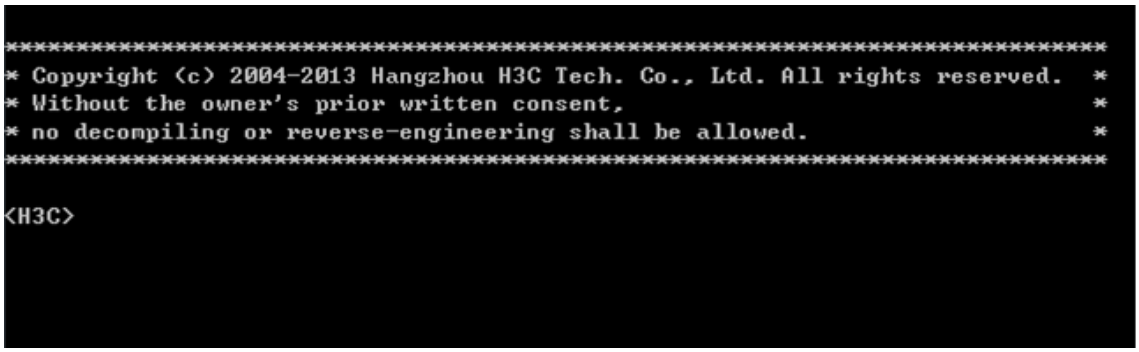
目 录

1 CLI

1.1 认识命令行接口

命令行接口是用户与设备之间的文本类指令交互界面，用户键入文本类命令，通过输入回车键提交设备执行相关命令，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。对比图形界面使用鼠标点击相关选项进行设置，命令行接口形式可以一次输入含义更为丰富的指令。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



1.2 开始使用命令行接口

设备支持多种方式进入命令行接口，比如通过 Console 口登录设备后进入命令行接口界面、通过 Telnet 方式登录设备后进入命令行接口界面、通过 SSH 方式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”中的相关章节。

1.3 命令行格式约定

命令行格式约定可以帮助您理解命令含义，产品手册中命令行表示规则遵循 表 1-1 约定：

表1-1 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。
[ ]	用“[ ]”括起来的部分在命令配置时是可选的。
{ x | y | ... }	从两个或多个选项中仅选取一个。
[x | y | ...]	从两个或多个选项中选取一个或者不选。
{ x | y | ... } *	从两个或多个选项中至少选取一个。
[x | y | ...] *	从两个或多个选项中选取一个、多个或者不选。

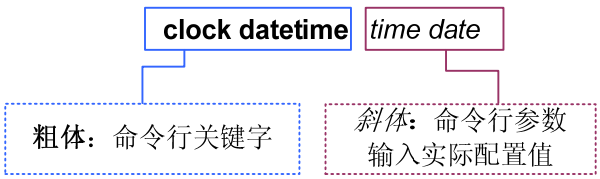
格式	意义
&<1-n>	符号“&”前面的参数可以重复输入1～n次。
#	由“#”号开始的行为注释行。

说明

命令行关键字输入时不区分大小写。

根据 表 1-1 规则解读命令**clock datetime** *time date*：

图1-2 命令行解读



示例：

使用如下命令行，则可以将设备的系统时间设置为 2010 年 2 月 23 日 10 时 30 分 20 秒。

```
<Sysname> clock datetime 10:30:20 2/23/2010
```

如遇到其他更为复杂的命令形式，都可以参照 表 1-1 的约定解读其逻辑关系。

1.4 命令的undo格式

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。

在命令前加 **undo** 关键字，即为命令的 **undo** 形式，几乎每条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 命令视图

1.5.1 命令视图简介

设备提供丰富的功能，也提供了相应的配置和查询命令。为便于您使用这些命令，设备将命令按功能进行分类组织。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。

命令视图采用分层结构，它们之间既有联系又有区别。如 图 1-3 所示，

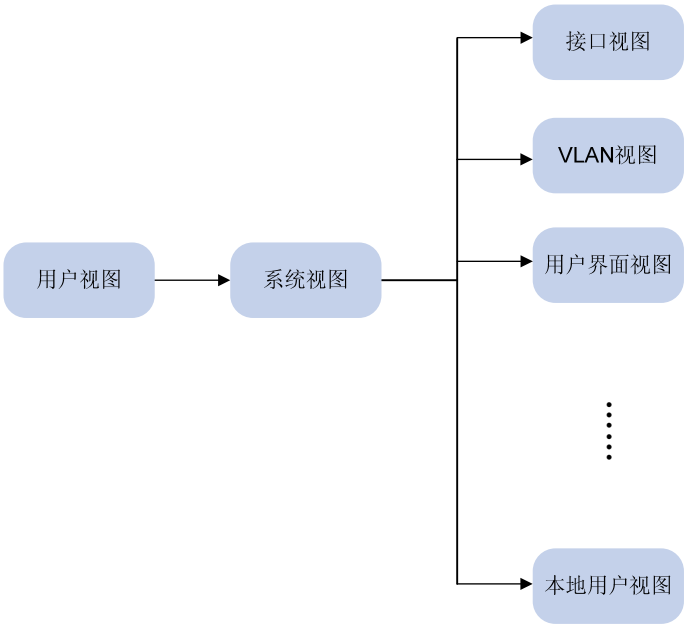
- 用户登录设备后，直接进入用户视图。此时屏幕显示的提示符是：<*设备名*>。用户视图下可执行的操作主要包括查看操作、调试操作、文件管理操作、设置系统时间、重启设备、FTP 和 Telnet 操作等。(“*设备名*”可以通过 **sysname** 命令来配置，缺省值为 Sysname，**sysname** 命令介绍请参见“基本配置命令参考”中的“设备管理”)

- 从用户视图可以进入系统视图，系统视图下能对设备运行参数进行配置，比如配置夏令时、配置欢迎信息、配置快捷键等。
- 在系统视图下键入不同的命令，可以进入相应的功能视图，完成各种功能的配置，比如：进入接口视图配置接口参数、创建 VLAN 并进入 VLAN 视图、进入用户界面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密码和级别等。

说明

想要了解某命令视图下支持哪些命令，请在命令视图提示符下键入“?”，系统将自动罗列出该命令行视图下可以执行的所有命令。

图1-3 命令视图示意图



1.5.2 进入系统视图

当用户登录到设备后，会自动进入用户视图，此时屏幕显示的提示符是：<*设备名*>。用户视图可执行的操作有限（比如查看操作、文件操作、FTP 和 Telnet 操作等），需要进入系统视图，才能进一步对设备进行配置。

表1-2 进入系统视图

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

1.5.3 退出当前视图

命令视图采用分层结构，比如用户视图下有系统视图，系统视图下又有接口视图、VLAN 视图等。当前视图下的功能配置完成，需要退出当前视图时，可以进行如下操作。

表1-3 退出当前视图

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

说明

- 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。
- 公共密钥编辑视图下请使用 **public-key-code end** 返回上一级视图（公共密钥视图）；公共密钥视图下请使用 **peer-public-key end** 命令返回系统视图。

1.5.4 返回用户视图

本特性为用户提供了一种快捷的、从任意的非用户视图返回到用户视图的方式，而不需要多次执行 **quit** 命令。用户也可以直接按组合键<Ctrl+Z>从当前视图退回到用户视图。

表1-4 退回用户视图

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

1.6 使用命令行在线帮助

在命令行输入过程中，您可以随时键入“?”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，供您参考使用：

(1) 在任意视图下，键入<?>即可获取该视图下您可以使用的所有命令及其简单描述。例如：

```
<Sysname> ?
User view commands:
  archive           Specify archive settings
  backup            Backup next startup-configuration file to TFTP server
  boot-loader       Set boot loader
  bootrom           Update/read/backup/restore bootrom
  cd                Change current directory
……略……
```

(2) 键入一条命令的关键字，后接以空格分隔的<?>。

如果<?>位置为关键字，则列出全部关键字及其简单描述。例如：

```
<Sysname> terminal ?
  debugging  Send debug information to terminal
  logging    Send log information to terminal
  monitor    Send information output to current terminal
  trapping   Send trap information to 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
[Sysname] interface vlan-interface 1 ?
  <cr>
[Sysname] interface vlan-interface 1
```

<cr>表示命令行当前位置无参数，直接键入回车即可执行。

(3) 键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
```

1.7 命令行输入

1.7.1 编辑命令行

输入命令行时的常用编辑功能，请参见 表 1-5 的介绍。

表1-5 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
退格键<Backspace>	删除光标位置的前一个字符，光标前移
左光标键←或<Ctrl+B>	光标向左移动一个字符位置
右光标键→或<Ctrl+F>	光标向右移动一个字符位置
<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，则反复按<Tab>键，可以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。

1.7.2 STRING类型参数的输入

编辑命令行时，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。需要注意的是，业务模块可能对 STRING 类型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手册中的参数描述。比如：

```
<Sysname> system-view
[Sysname] domain ?
  STRING<1-24>  Domain name
```

以上举例表明，在设备创建一个安全域时，域名为 STRING 类型的参数，最多可以包含 24 个字符，每个字符可以是除“?”、“"”、“\”、空格、“|”、“/”、“:”、“*”、“<”、“>”、“@”之外的任意可见字符，比如，将域名定义为 forVPN1。

1.7.3 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**（注意不能只输入 **s**，因为输入不能确定唯一匹配关键字）。
- 如果要输入 **startup saved-configuration**，可以直接输入 **st s**；

您可以按<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。

1.7.4 配置命令行的别名

通过配置命令行别名，用户可以将设备当前支持的命令行的第一个关键字替换为自己惯用的关键字。比如将 **display** 的别名设置为 **show**，这样在设备上执行 **display** xx 命令时只需要输入 **show** xx 即可。

在配置命令行别名时，需要遵循以下约定：

- 当查看当前配置信息以及保存配置信息时，用户输入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。即用户的别名命令可以使用，但不会参与配置保存和恢复。
- 配置命令行别名时，输入的待替换的关键字（cmdkey）和替换后的关键字（alias）参数必须是完整的输入形式。
- 当用户输入字符与用户定义的别名以及现有某关键字同时部分匹配时，则优先匹配别名，如想输入现有关键字对应的命令则需要完整输入该关键字。当用户输入字符与某关键字完全匹配，而与别名部分匹配时，则优先匹配关键字，如想输入别名对应的命令则需要完整输入该别名。如果用户输入的字符串与多个别名部分匹配，则输出歧义匹配信息。
- 当用户对别名关键字使用<Tab>键时，将联想出所对应的原始关键字。
- 不支持对整个命令行的替换。只支持对第一关键字的别名设置，以及 undo 命令的第二关键字的别名替换。

表1-6 配置命令行的别名

操作	命令	说明
进入系统视图	**system-view**	-
使能命令行别名功能	**command-alias enable**	必选 缺省情况下，命令行别名功能处于关闭状态
给指定的命令行配置别名	**command-alias mapping** *cmdkey alias*	必选 缺省情况下，命令行没有配置别名

您可以随时使用 **display command-alias** 命令来显示当前已经设置的命令行别名。

1.7.5 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，系统提供了五个快捷键供用户自定义。只要用户按下某个快捷键，系统即可执行对应的命令。

表1-7 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*	可选 缺省情况请参见表下方的说明
显示系统中快捷键的分配信息	**display hotkey** [| { **begin** | **exclude** | **include** } *regular-expression*]	可在任意视图下执行，系统保留的快捷键请参见表1-8


说明

缺省情况下，系统为<Ctrl+G>、<Ctrl+L>、<Ctrl+O>三个快捷键指定了对应的命令，其它两个快捷键<Ctrl+T>、<Ctrl+U>缺省值为 NULL（空）。

- <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**（关闭所有模块的调试信息开关）。

表1-8 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

快捷键	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+N>	显示历史命令缓冲区中的后一条命令
<Ctrl+P>	显示历史命令缓冲区中的前一条命令
<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
<Ctrl+Z>	退回到用户视图
<Ctrl+]>	终止呼入的连接或重定向连接
<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（键入回车前有效）
<Esc+P>	将光标向上移动一行（键入回车前有效）
<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

说明

以上快捷键为设备所定义，当用户使用终端软件与设备进行交互时，这些快捷键可能在终端软件中被定义为其它指令。此时，快捷键的操作优先遵从终端软件的定义，而不会对设备生效。

1.7.6 命令行输入回显功能

当您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您已经输入而未提交执行的信息，方便您继续完成未输入的内容。

表1-9 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**	必选 缺省情况下，命令行输入回显功能处于关闭状态

说明

- 在当前命令行提示符下，如果用户没有任何输入，此时若有日志等系统信息输出，输出后将不会回显命令行提示符；
- 当处在交互状态，需要用户输入一些交互信息时（非 Y/N 确认信息），因为情况各异，所以若有系统信息输出，输出后不再回显提示信息，而只是将用户已有的输入换行打印出来。
- **info-center synchronous** 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”。

1.8 解读输入错误提示信息

您所有键入的命令，如果通过设备的语法检查，则正确执行，否则向您报告错误信息，常见错误信息参见 表 1-10。

表1-10 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.	在符号'^'指示位置的命令无法解析
% Incomplete command found at '^' position.	在符号'^'指示位置的命令不完整
% Ambiguous command found at '^' position.	在符号'^'指示位置的参数不明确，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

1.9 使用历史命令

命令行接口会将您最近使用的历史命令自动保存到历史命令缓存区，您可以随时了解最近执行的命令，以及调用保存的历史命令来进行重复输入。

1.9.1 调用历史命令

表1-11 调用历史命令

操作	命令或按键	结果
显示历史命令	**display history-command** [**|** { **begin** | **exclude** | **include** } *regular-expression*]	显示用户输入的有效历史命令
访问上一条历史命令	上光标键↑或<Ctrl+P>	如果还有更早的历史命令，则显示上一条历史命令
访问下一条历史命令	下光标键↓或<Ctrl+N>	如果还有更晚的历史命令，则显示下一条历史命令

说明

用光标键对历史命令进行访问，在 Windows 200X 及 XP 的 Terminal 和 Telnet 下均有效，但对于 Windows 9X 超级终端，↑、↓光标键会无效，这是由于 Windows 9X 的超级终端对这两个键作了不同解释所致，这时可以用组合键<Ctrl+P>和<Ctrl+N>来达到同样效果。

下面是关于历史命令的一些详细说明，您可以做进一步了解：

- 设备保存的历史命令与用户输入的命令格式相同，如果您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。
- 如果您连续多次执行同一条命令，设备的历史命令中只保留最早的一次。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：多次执行 **display cu** 命令，历史命令中只保存一条。如果执行 **display cu** 和 **display current-configuration**，将保存为两条历史命令。

1.9.2 配置历史命令缓冲区的大小

表1-12 配置终端属性

操作	命令	说明
进入系统视图	**system-view**	-
进入用户界面视图	**user-interface** { *first-num1* [*last-num1*] | { **aux** | **vty** } *first-num2* [*last-num2*] }	-
设置历史命令缓冲区可存放的历史命令的条数	**history-command max-size** *size-value*	可选 缺省情况下，历史命令缓冲区可存放10条历史命令

说明

user-interface和**history-command max-size**命令的详细介绍请参见“基础配置命令参考”中的“登录交换机”。

1.10 便捷的查看显示信息

1.10.1 分屏显示

1. 控制分屏显示

当显示信息较多超过一屏时，系统会自动暂停将信息分屏显示，方便您查看显示信息。

这时您可以使用 表 1-13 所示的按键来选择下一步操作。

表1-13 显示功能表

按键或命令	功能
键入空格键	继续显示下一屏信息
键入回车键	继续显示下一行信息
键入<Ctrl+C>	停止显示和命令执行
<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，您也可以使用 **screen-length** 命令设置用户界面下一屏显示的行数（**screen-length** 命令的详细介绍请参见“基础配置命令参考”中的“登录交换机”）。

2. 关闭分屏显示功能

您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，不方便立即查看。

表1-14 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**	必选 缺省情况下，用户登录后将遵循用户界面下的**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，仅对当前用户有效，用户重登录后将恢复到缺省情况

1.10.2 正则表达式过滤显示

1. 正则表达式过滤简介

在执行 **display** 命令查看显示信息时，用户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。

过滤显示的使用方法有两种：

- 在命令行中通过输入**| { begin | exclude | include }** *regular-expression* 参数的方式来过滤显示；

- 在分屏显示时，使用“/”、“-”或“+”符号加正则表达式的方式，它将对剩余还未显示的信息使用正则表达式进行过滤显示。其中，“/”等同关键字 **begin**；“-”等同关键字 **exclude**；“+”等同关键字 **include**。

begin、**exclude** 或 **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，它还支持多种特殊字符，特殊字符的匹配规则如 表 1-15 所示。

表1-15 正则表达式中的特殊字符

特殊字符	含义	使用说明
^string	行首匹配符，string只能出现在每行的开始	如：^user只能匹配以user开始的行，不能匹配以Auser开始的行
string$	行尾匹配符，string只能出现在每行的末尾	如：user$只能匹配以user结尾的行，不能匹配以userA结尾的行
.	句点，通配符，匹配任何一个字符，包括单个字符、特殊字符和空格等	如：.s可以匹配as和bs等
*	星号，匹配星号前面的字符或字符组零次或多次	如：zo*可以匹配z以及zoo；(zo)*可以匹配zo以及zozo
+	加号，匹配加号前面的字符或字符组一次或多次	如：zo+可以匹配zo以及zoo，但不能匹配z
|	竖线，匹配|左边的整个字符串或者右边的整个字符串	如：def|int只能匹配包含def或者int的字符串
_	下划线，该字符出现在表达式的开头或结尾时，等效于行首匹配符或行尾匹配符（即特殊字符^或$），其它情况下等效于逗号、空格或者作为普通字符时的左括号、右括号、左大括号、右大括号	如：a_b可以匹配a b和a(b等；_ab只能匹配以ab开头的行；ab_只能匹配以ab结束的行
-	连接符，用于连接两个数值或字母（小的在前，大的在后），与“[ ]”符号连用表示一个范围	如：从1到9表示为1-9（包括1和9）；从a到h表示为a-h（包括a和h）
[ ]	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	如：[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[ ]的最前面，形如[]string]，才能匹配到]。[没有这样的限制
( )	表示字符组，一般与“+”或“*”等符号一起使用	如：(123A)表示字符组123A；408(12)+可以匹配40812或408121212等字符串，但不能匹配408

特殊字符	含义	使用说明
\index	表示重复一次指定字符组，字符组是指\前用()括起来的字符串，index对应\前字符组的顺序号按从左至右的顺序从1开始编号：如果\前面只有一个字符组，则index只能为1；如果\前面有n个字符组，则index可以为1到n中的任意整数	如：(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	如：[^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
\<string	匹配以string开头的字符串	如：\<do可以匹配单词domain，还可以匹配字符串doa
string\>	匹配以string结尾的字符串	如：do\>可以匹配单词undo，还可以匹配字符串abcdo
\bcharacter2	匹配characte1character2，characte1可以是除了数字、字母和下划线外的任意字符，\b等效于[^A-Za-z0-9_]	如：\ba可以匹配-a，-为characte1，a为character2，但是不能匹配2a和ba等
\Bcharacter	匹配到的字符串中必须包含字符character，且character前不能是空格	如：\Bt可以匹配install里的t而不能匹配big top中的t
character1\w	匹配characte1character2，character2必须是数字、字母或下划线。\w相当于[A-Za-z0-9_]	如：v\w能匹配到vlan，v为characte1，l为character2，v\w还能匹配service，i为character2
\W	等效于\b	如：\Wa可以匹配-a，-为characte1，a为character2，但是不能匹配2a和ba等
\	转义操作符，\后紧跟本表列的单个特殊字符时，将去除特殊字符的特定含义	如：\\可以匹配包含\的字符串，\^可以匹配包含^的字符串，\\b可以匹配包含\b的字符串

2. 正则表达式过滤举例

(1) **begin** 参数应用举例

查看当前生效的配置中，从包含“user-interface”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 user-interface
user-interface aux 0
user-interface vty 0 15
authentication-mode none
user privilege level 3
#
return
```

(2) **exclude** 参数应用举例

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
Routing Tables: Public

Destination/Mask    Proto   Pre  Cost        NextHop         Interface
```

```
1.1.1.0/24          Static 60   0           192.168.0.0     Vlan1
```

(3) **include** 参数应用举例

查看路由表中包含 Vlan 的路由表项（该显示信息与用户的当前配置有关）。

```
<Sysname> display ip routing-table | include Vlan
Routing Tables: Public

Destination/Mask    Proto  Pre  Cost        NextHop         Interface

192.168.1.0/24      Direct 0    0           192.168.1.42    Vlan999
```

1.11 配置用户级别和命令级别

1.11.1 级别简介

为了限制不同用户对设备的访问权限，系统对用户进行了分级管理。用户的级别与命令级别对应，不同级别的用户登录后，只能使用等于或低于自己级别的命令。

命令的级别由低到高分为访问级、监控级、系统级和管理级四种，分别对应级别值 0、1、2、3。详细介绍请见 表 1-16：

表1-16 命令级别简介

级别值	级别名称	描述
0	访问级	用于网络诊断等功能的命令、从本设备出发访问外部设备的命令。该级别命令配置后不允许保存，设备重启后，该级别命令会恢复到缺省状态 缺省情况下，访问级的命令包括：**ping**、**tracert**、**telnet**、**ssh2**等
1	监控级	用于系统维护、业务故障诊断等功能的命令。该级别命令配置后不允许保存，设备重启后，该级别命令会恢复到缺省状态 缺省情况下，监控级的命令包括：**debugging**、**terminal**、**refresh**、**send**等
2	系统级	业务配置命令，包括路由、各个网络层次的命令，这些命令用于向用户提供直接网络服务 缺省情况下，系统级的命令包括：所有配置命令（管理级的命令除外）
3	管理级	关系到系统的基本运行、系统支撑模块功能的命令，这些命令对业务提供支撑作用 缺省情况下，管理级的命令包括：文件系统命令、FTP命令、TFTP命令、用户管理命令、级别设置命令、系统内部参数设置命令（非协议规定、非RFC规定）等

1.11.2 配置用户级别

用户级别可以通过 AAA 认证参数或者用户界面来配置：

1. 通过AAA认证参数配置用户级别

如果用户登录时使用的用户界面的认证方式为 **scheme**，并且用户登录时需要输入用户名和密码，则用户级别以及用户可使用的命令，在配置 AAA 认证时指定。

表1-17 通过 AAA 认证参数配置用户级别

操作		命令	说明
进入系统视图		**system-view**	-
进入用户界面视图		**user-interface** { *first-num1* [*last-num1*] | { **aux** | **vty** } *first-num2* [*last-num2*] }	-
设置登录用户界面的认证方式为**scheme**		**authentication-mode scheme**	必选 缺省情况下，VTY用户界面认证方式为**password**，AUX用户界面不需要认证
退回系统视图		**quit**	-
配置SSH用户的认证方式为password方式		相关内容请参见“安全配置指导”中的“SSH”	如果用户使用SSH方式登录，并且认证时要求输入用户名和密码，则该步骤必选
通过认证参数设置用户的级别	使用本地认证时	• 使用 **local-user** 命令创建本地用户并进入本地用户视图 • 使用 **authorization-attribute** 命令的 **level** 参数配置用户本身的级别	二者必选其一 使用本地认证时，如果没有配置用户级别，则用户级别为0，即只能使用0级别的命令 使用远程认证时，如果没有配置用户级别，则用户级别由认证服务器的缺省配置决定
	使用远程认证（RADIUS认证或者HWTACACS认证）时	在认证服务器上进行配置	

说明

- 关于用户界面的介绍请参见“基础配置指导”中的“登录交换机”。有关 **user-interface**、**authentication-mode**、**user privilege level** 命令的介绍请参见“基础配置命令参考”中的“登录交换机”。
- 有关 AAA 认证的介绍请参见“安全配置指导”中的“AAA”。**local-user** 和 **authorization-attribute** 命令的介绍请参见“安全命令参考”中的“AAA”。
- 有关 SSH 的介绍请参见“安全配置指导”中的“SSH”。

2. 通过AAA认证参数配置用户级别举例

设置使用 VTY 1 的 Telnet 用户登录设备时，需要本地验证用户名和口令，用户级别为 3。

```
<Sysname> system-view
[Sysname] user-interface vty 1
[Sysname-ui-vty1] authentication-mode scheme
[Sysname-ui-vty1] quit
[Sysname] local-user test
[Sysname-luser-test] password simple 123
[Sysname-luser-test] service-type telnet
```

通过以上配置，用户使用 VTY 1 Telnet 登录设备时，需要输入用户名 test，密码 123，认证通过后只能使用级别为 0 的命令，想要使用级别为 0、1、2、3 的命令还需要配置：

```
[Sysname-luser-test] authorization-attribute level 3
```

3. 通过用户界面配置用户级别

- 如果用户登录时使用的用户界面的认证方式为 **scheme**，而且是 SSH 的 publickey 认证方式时（该方式只需要输入用户名，不需要输入密码），则用户级别等于用户界面的级别；
- 如果用户登录时使用的用户界面的认证方式为 **none** 或者 **password**（即不需要输入用户名），用户级别也等于用户界面的级别。

表1-18 通过用户界面配置用户级别（SSH 的 publickey 认证方式）

操作	命令	说明
配置SSH用户的认证方式为publickey方式	相关内容请参见“安全配置指导”中的“SSH”	如果用户使用SSH方式登录，并且认证时只要输入用户名，不用输入密码，则该步骤必选 配置该步骤后，相应的用户界面的认证方式必须设置为**scheme**
进入系统视图	**system-view**	-
进入用户界面视图	**user-interface** { *first-num1* [*last-num1*] | **vty** *first-num2* [*last-num2*] }	-
设置用户使用当前用户界面登录设备时的认证方式	**authentication-mode scheme**	必选 缺省情况下，VTY用户界面认证方式为**password**，AUX用户界面不需要认证
配置从当前用户界面登录系统的用户的级别	**user privilege level** *level*	可选 缺省情况下，通过AUX用户界面登录系统的用户级别是3，通过VTY用户界面登录系统的用户级别是0

表1-19 通过用户界面配置用户级别（none 或者 password 认证方式）

操作	命令	说明
进入系统视图	**system-view**	-
进入用户界面视图	**user-interface** { *first-num1* [*last-num1*] | { **aux** | **vty** } *first-num2* [*last-num2*] }	-
设置用户使用当前用户界面登录设备时的认证方式	**authentication-mode** { **none** | **password** }	可选 缺省情况下，VTY用户界面认证方式为**password**，AUX用户界面不需要认证
配置从当前用户界面登录系统的用户的级别	**user privilege level** *level*	可选 缺省情况下，通过AUX用户界面登录系统的用户级别是3，通过VTY用户界面登录系统的用户级别是0

4. 通过用户界面配置用户级别举例

- 设置所有的 Telnet 用户登录设备时，不需要身份认证，用户级别为 1。（不设置身份认证可能存在安全隐患，请确保在安全性较高的网络环境中使用本配置）

```
<Sysname> system-view
[Sysname] user-interface vty 0 15
[Sysname-ui-vty0-15] authentication-mode none
[Sysname-ui-vty0-15] user privilege level 1
```

如果不设置用户级别，用户不需要输入用户名和密码，就能使用 Telnet 方式登录设备，但只能使用以下命令：

```
<Sysname> ?
User view commands:
  cfd      Connectivity fault detection (IEEE 802.1ag)
  cluster  Run cluster command
  display  Display current system information
  ping     Ping function
  quit     Exit from current command view
  ssh2     Establish a secure shell client connection
  super    Set the current user priority level
  telnet   Establish one TELNET connection
  tracert  Trace route function
```

设置用户级别后，用户不需要输入用户名和密码，就能使用 Telnet 方式登录设备，可使用的命令明显增多：

```
<Sysname> ?
User view commands:
  cfd                Connectivity fault detection (IEEE 802.1ag)
  cluster            Run cluster command
  debugging          Enable system debugging functions
  display            Display current system information
  graceful-restart   Graceful restart
  ipc                Interprocess communication
  oam                OAM protocol
  ping               Ping function
  quit               Exit from current command view
  refresh            Do soft reset
  reset              Reset operation
  screen-length      Specify the lines displayed on one screen
  send               Send information to other user terminal interface
  ssh2               Establish a secure shell client connection
  super              Set the current user priority level
  telnet             Establish one TELNET connection
  terminal           Set the terminal line characteristics
  tracert            Trace route function
  undo               Cancel current setting
```

- 设置所有的 Telnet 用户登录设备时，需要验证口令，用户级别为 2。

```
<Sysname> system-view
[Sysname] user-interface vty 0 15
[Sysname-ui-vty0-15] authentication-mode password
```

```
[Sysname-ui-vty0-15] set authentication password simple 123
[Sysname-ui-vty0-15] user privilege level 2
```

缺省情况下，用户使用 Telnet 方式登录设备，通过口令验证后，只能使用级别为 0 的命令。通过用户界面设置级别后，用户使用 Telnet 方式登录设备，输入密码 123 后，就可以使用级别为 0、1、2 的命令。

1.11.3 切换用户级别

1. 用户级别切换功能简介

切换用户级别是指在不退出当前登录、不断开当前连接的前提下暂时的修改用户级别。级别修改后不需要重新登录，可以继续配置设备，只是可以执行的命令会不一样。比如用户的级别为 3，可以对系统参数进行设置，如果将用户的级别切换到 0，则只能执行简单的 **ping**、**tracert** 和很少一部分 **display** 命令等。切换后的级别是临时的，只对当前登录生效，用户重新登录后，又会恢复到原有级别。

- 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级别的用户登录设备、查看设备运行参数，当需要对设备进行维护时，再临时切换到较高的级别；
- 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的级别，来限制其它人员的操作。

2. 配置用户级别切换时的认证方式

- 从高级别切换到低级别或相同级别时，可以直接切换，不需要进行身份验证。
- 从低级别切换到高级别时，为了保证操作的安全性，需要进行身份认证。如 表 1-20 所示，认证方式有四种。

表1-20 用户级别切换认证方式表

认证方式	涵义	说明
local	本地密码认证	设备验证用户输入的级别切换密码 使用该方式时，需要在设备上使用**super password**命令设置级别切换密码
scheme	通过HWTACACS/RADIUS进行远程AAA认证	设备将级别切换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
local scheme	本地密码认证和远程AAA认证相结合	先本地密码认证，若设备上没有设置本地级别切换密码，使用AUX用户界面登录的用户会直接进行级别切换，其它用户（使用VTY用户界面登录的用户）则转为远程AAA认证
scheme local	远程AAA认证和本地密码认证相结合	先远程AAA认证，远程HWTACACS/RADIUS服务器无响应或设备上的AAA配置无效时，转为本地密码认证

表1-21 配置用户级别切换时的认证方式

操作	命令	说明
进入系统视图	**system-view**	-
配置用户级别切换时的认证方式	**super authentication-mode** { **local** | **scheme** } *	可选 缺省情况下，采用**local**认证方式
配置用户级别切换的密码	非FIPS模式下： **super password** [**level** *user-level*] [**hash**] { **cipher** | **simple** } *password* FIPS模式下： **password**	如果使用本地认证（即认证方式配置时选择了**local**参数），则该步骤必选 缺省情况下，没有设置切换用户级别的密码

注意

- 在使用 **super password** 命令时，若不指定用户级别，则配置的是切换到 3 级用户的密码。
- 如当用户使用 AUX 用户界面（指 Console 口）登录设备进行低级别到高级别的切换时，即便认证方式为 **local**，没有配置对应的用户级别切换密码，也可以成功的实现级别切换。

3. 切换用户级别

表1-22 切换用户级别

操作	命令	说明
切换用户级别	**super** [*level*]	必选 用户在登录设备时，已经具有了一定的级别，该级别由用户界面或者认证用户级别决定 该命令在用户视图下执行

切换用户级别时，根据用户界面认证方式和 Super 认证方式的不同组合设置，系统会要求用户输入不同的信息：

表1-23 用户级别切换时输入信息描述表

用户界面认证方式	用户级别切换认证方式	第一种认证方式下切换用户级别需要输入的信息	认证方式转换后切换用户级别需要输入的信息
none/password	**local**	本地级别切换密码（设备上设置）	-
	local scheme	本地级别切换密码	级别切换用户名和密码（AAA服务器上设置）
	scheme	级别切换用户名和密码	-
	scheme local	级别切换用户名和密码	本地级别切换密码
scheme	**local**	本地级别切换密码	-
	local scheme	本地级别切换密码	级别切换密码（AAA服务器上设置），系统使用登录用户名作为级别切换用户名
	scheme	级别切换密码（AAA服务器上设置），系统使用登录用户名作为级别切换用户名	-
	scheme local	级别切换密码（AAA服务器上设置），系统使用登录用户名作为级别切换用户名	本地级别切换密码

注意

- 当使用的认证方式中有 **local** 时，切换用户级别前需要配置用户级别切换的密码。
- 当使用的认证方式中有 **scheme** 时，切换用户级别前需要配置 AAA 相关参数。
- 级别切换认证方式为 **scheme** 方式时，用户最多可以连续输入三次密码。级别切换认证方式为 **local** 时，用户最多可以连续输入五次密码。达到最大尝试次数密码都错误则本次切换失败。
- 通过 **scheme** 认证登录的用户如果连续 5 次密码错误则会被锁定 15 分钟，期间无法切换到高级别。锁定期间重新尝试，则会重新计时。所以一旦锁定，请耐心等待。
- 关于用户界面认证方式的相关描述请参见“基础配置指导”中的“登录交换机”。

1.11.4 修改命令级别

缺省情况，各个视图下的每条命令都有指定的级别（如 表 1-16 所示）。管理员也可以根据用户需要改变命令的级别：实现低级别用户可以使用部分高级别命令的需求；或者将命令的级别提高，增加设备的安全性。

表1-24 修改命令的级别

操作	命令	说明
进入系统视图	**system-view**	-

操作	命令	说明
设置指定视图下的命令的级别	**command-privilege level** *level* **view** *view command*	可选 缺省情况请参见表1-16

注意

通常情况下，建议用户不要修改缺省的命令级别或者在专业人员的指导下进行修改，以免造成操作和维护上的不便甚至给设备带来安全隐患。

1.12 保存当前配置

在设备上，您可以随时输入 **save** 命令，将已经提交执行的所有命令行保存在配置文件中。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** 类显示命令（执行后即显示相关信息），**reset** 类清除命令（执行后即清除相关信息）。这类命令执行一次性操作要求，不会进行配置保存。

1.13 CLI显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以查看系统相应的配置信息和运行信息。

表1-25 系统基本配置显示和维护

操作	命令
显示当前用户设置的命令行及其别名	**display command-alias** [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示剪贴板的内容	**display clipboard** [**|** { **begin** | **exclude** | **include** } *regular-expression*]

目 录

1 登录交换机方式介绍

说明

- 设备运行于 FIPS 模式时，本特性的相关配置相对于非 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”。
- 本章中典型配置举例中的配置，如无特殊说明，均以设备运行在非 FIPS 模式下的命令行为准。
- FIPS 模式下不支持 Telnet 和 HTTP 功能。

1.1 登录交换机方式综述

用户可以通过以下几种方式登录到交换机上，对交换机进行配置和管理：

登录方式及介绍		各种登录方式缺省状况分析
通过CLI登录设备	配置通过Console口登录设备	缺省情况下，用户可以直接通过Console口本地登录设备，登录时认证方式为None（不需要用户名和密码），登录用户级别为3
	配置通过Telnet登录设备	缺省情况下，用户不能直接通过Telnet方式登录设备。如需采用Telnet方式登录，需要先通过Console口本地登录设备、并完成如下配置： • 开启设备的 Telnet 功能（缺省情况下，Telnet 功能关闭） • 配置设备 VLAN 接口的 IP 地址，确保设备与 Telnet 登录用户间路由可达（缺省情况下，设备没有 IP 地址） • 配置 VTY 用户的认证方式（缺省情况下，VTY 用户采用 Password 认证方式） • 配置 VTY 用户的用户级别（缺省情况下，VTY 用户的用户级别为 0）
	配置通过SSH登录	缺省情况下，用户不能直接通过SSH方式登录设备。如需采用SSH方式登录，需要先通过Console口本地登录设备、并完成如下配置： • 开启设备 SSH 功能并完成 SSH 属性的配置（缺省情况下，SSH 功能关闭） • 配置设备 VLAN 接口的 IP 地址，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 用户的用户级别（缺省情况下，VTY 用户的用户级别为 0）
	配置通过Modem登录设备	缺省情况下，用户可以直接通过Modem拨号方式登录设备，Modem用户的用户级别为3

登录方式及介绍	各种登录方式缺省状况分析
配置通过Web网管登录设备	缺省情况下，用户不能直接通过Web登录设备。如需采用Web方式登录，需要先通过Console口本地登录设备、并完成如下配置： • 配置设备 VLAN 接口的 IP 地址，确保设备与 Web 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 Web 用户的用户名与密码（缺省情况下，没有 Web 登录的用户名和密码） • 配置 Web 登录的用户级别（缺省情况下，未配置 Web 登录用户的用户级别） • 配置 Web 登录用户的服务类型为 Web（缺省情况下，未配置 Web 登录用户的服务类型）
配置通过NMS登录设备	缺省情况下，用户不能直接通过NMS登录设备。如需采用NMS方式登录，需要先通过Console口本地登录设备、并完成如下配置： • 配置设备 VLAN 接口的 IP 地址，确保设备与 NMS 登录用户间路由可达（缺省情况下，设备没有 IP 配置地址） • 配置 SNMP 基本参数

在以下的章节中，将分别为您介绍如何通过 Console 口、Telnet、SSH、Modem、Web 及 NMS 登录到设备上。

1.2 用户界面简介

1.2.1 用户界面概述

当用户使用 Console 口、Telnet 或者 SSH 方式登录设备的时候，系统会分配一个用户界面（也称为 Line）用来管理、监控设备和用户间的当前会话。每个用户界面有对应的用户界面视图（User-interface view），在用户界面视图下网络管理员可以配置一系列参数，比如用户登录时是否需要认证、用户登录后的级别等，当用户使用该用户界面登录的时候，将受到这些参数的约束，从而达到统一管理各种用户会话连接的目的。

目前系统支持的命令行配置方式有：

- Console 口本地配置
- Telnet、Modem 或 SSH 本地或远程配置

与这些配置方式对应的是两种类型的用户界面：

- AUX 用户界面：用来管理和监控通过 Console 口登录的用户。Console 口端口类型为 EIA/TIA-232 DCE。
- VTY（Virtual Type Terminal，虚拟类型终端）用户界面：用来管理和监控通过 VTY 方式登录的用户。VTY 口属于逻辑终端线，用于对设备进行 Telnet 或 SSH 访问。

1.2.2 用户与用户界面的关系

用户界面的管理和监控对象是使用某种方式登录的用户，虽然单个用户界面某一时刻只能被一个用户使用，但它并不针对某个用户。比如用户 A 使用 Console 口登录设备时，将受到 AUX 用户界面视图下配置的约束，当使用 VTY 1 登录设备时，将受到 VTY 1 用户界面视图下配置的约束。

一台设备上最多支持 1 个 AUX 用户界面、16 个 VTY 用户界面，这些用户界面与用户并没有固定的对应关系。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界面，整个登录过程将受该用户界面视图下配置的约束。同一用户登录的方式不同，分配的用户界面不同；同一用户登录的时机不同，分配的用户界面可能不同。

1.2.3 用户界面的编号

用户界面的编号有两种方式：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界面或一组用户界面。绝对编号从 0 开始自动编号，每次增长 1，先给所有 AUX 用户界面编号，其次是所有 VTY 用户界面。使用 **display user-interface**（不带参数）可查看到设备当前支持的用户界面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界面的内部编号。该方式只能指定某种类型的用户界面中的一个或一组，而不能跨类型操作。

相对编号方式的形式是：“用户界面类型 编号”，遵守如下规则：

- 控制台的相对编号：第一个为 AUX 0，第二个为 AUX 1，依次类推。
- VTY 的相对编号：第一个为 VTY 0，第二个为 VTY 1，依次类推。

2 配置用户通过CLI登录设备

2.1 配置用户通过CLI登录设备简介

CLI（命令行接口）是用户与设备之间的文本类指令交互界面，用户键入文本类命令，通过输入回车键提交设备执行相关命令，用户可以输入命令对设备进行配置，并可以通过查看输出的信息确认配置结果，方便用户配置和管理设备。

通过CLI登录设备包括：通过Console口、Telnet、SSH或Modem这几种登录方式。当您使用Console口、Telnet、SSH或Modem登录设备时，都需要使用CLI来与设备进行交互。

- 缺省情况下，用户不需要任何认证即可通过Console口及Modem方式登录设备，这给设备带来许多安全隐患；
- 缺省情况下，用户不能通过Telnet和SSH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。

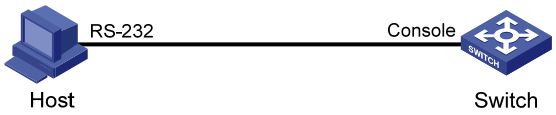
以下章节将分别为您介绍如何通过Console口、Telnet、SSH及Modem登录到设备，并配置通过Console口、Telnet、SSH及Modem登录设备时的认证方式、用户级别及公共属性，来实现对登录用户的控制和管理。

2.2 配置通过Console口登录设备

2.2.1 通过Console口登录设备简介

通过Console口进行本地登录是登录设备的最基本的方式，也是配置通过其他方式登录设备的基础。如 图 2-1 所示。

图2-1 通过 Console 口登录设备示意图



缺省情况下，设备可以通过Console口进行本地登录，用户登录到设备上后，即可以对各种登录方式进行配置。

本节将为您介绍：

- 设备缺省情况下，如何通过Console口登录设备。具体请参见“2.2.2 缺省配置下如何通过Console口登录设备”。
- 设备Console口支持的登录方式及配置Console口登录认证方式的意义、各种认证方式的特点及注意事项。具体请参见“2.2.3 Console口登录的认证方式介绍”。
- 当用户确定了今后通过Console口登录设备时将采用何种认证方式后、并通过缺省配置登录到设备后，用户如何在设备上配置Console口登录设备时的认证方式及用户级别，实现对Console口登录用户的控制和管理。具体请参见“2.2.4 配置通过Console口登录设备时无需认证

（None）”、“2.2.5 配置通过Console口登录设备时采用密码认证（Password）“及”2.2.6 配置通过Console口登录设备时采用AAA认证（Scheme）“。

- 配置通过Console口登录设备时的公共属性。具体请参见“2.2.7 配置Console口登录方式的公共属性（可选）“。

2.2.2 缺省配置下如何通过Console口登录设备

表2-1 通过 Console 登录设备需要具备的条件

对象	需要具备的条件
设备	缺省情况下，设备侧不需要任何配置
Console口登录用户	运行超级终端程序
	配置超级终端属性

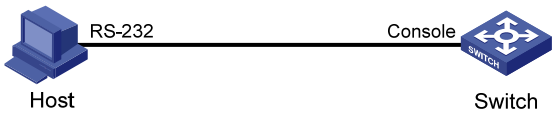
当用户使用 Console 口登录设备时，用户终端的通信参数配置要和设备 Console 口的缺省配置保持一致，才能通过 Console 口登录到设备上。设备 Console 口的缺省配置如下：

表2-2 设备 Console 口缺省配置

属性	缺省配置
传输速率	9600bit/s
流控方式	不进行流控
校验方式	不进行校验
停止位	1
数据位	8

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

图2-2 将设备与 PC 通过配置口电缆进行连接



警告

连接时请认准接口上的标识，以免误插入其它接口。

说明

由于 PC 机串口不支持热插拔，请不要在设备带电的情况下，将串口插入或者拔出 PC 机。当连接 PC 和设备时，请先安装配置电缆的 DB-9 端到 PC 机，再连接 RJ-45 到设备；在拆下时，在拆下时，先拔出 RJ-45 端，再拔下 DB-9 端。

(2) 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），选择与设备相连的串口，设置终端通信参数：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 2-3 至 图 2-5 所示。

说明

如果您的 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；如果您的 PC 使用的是 Windows Server 2008、Windows 7 、Windows Vista 或其他操作系统，请您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2-3 新建连接

图2-4 连接端口设置

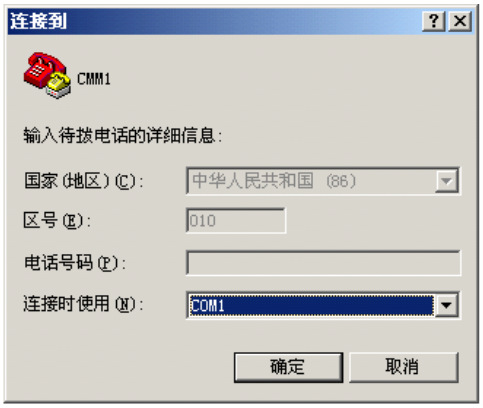
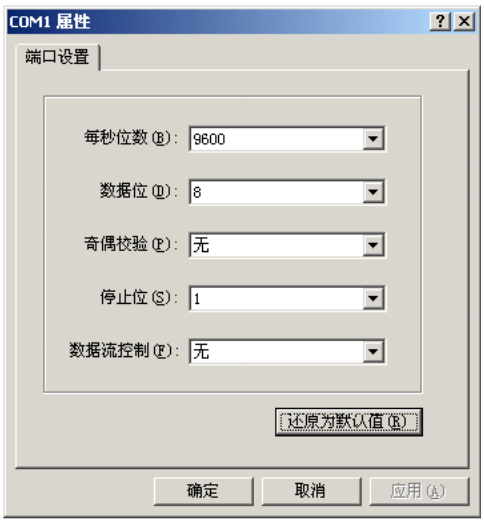
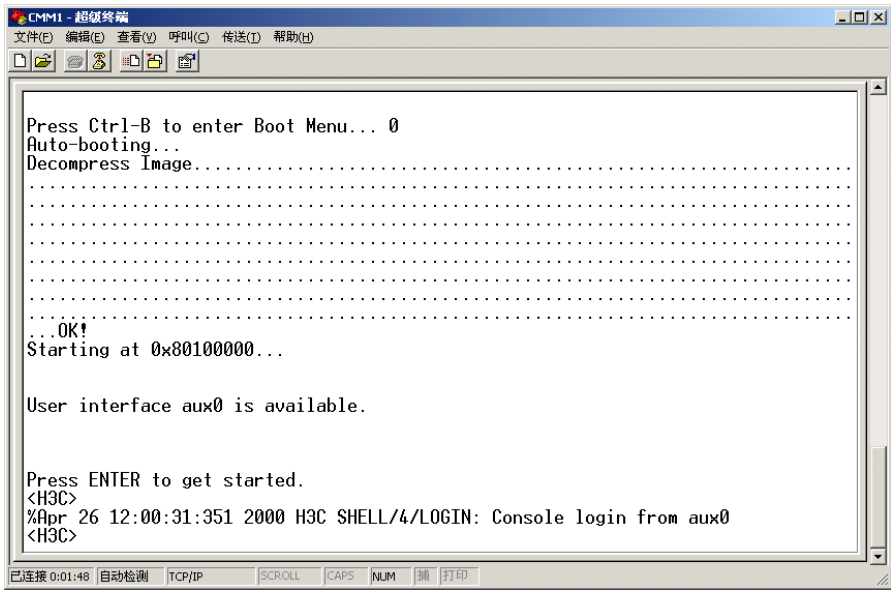


图2-5 端口通信参数设置



(3) 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，之后将出现命令行提示符（如<H3C>），如 图 2-6 所示。

图2-6 设备配置界面



(4) 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“?”，具体的配置命令请参考本手册中相关部分的内容。

2.2.3 Console口登录的认证方式介绍

通过在 Console 口用户界面下配置认证方式，可以对使用 Console 口登录的用户进行限制，以提高设备的安全性。Console 口支持的认证方式有 **none**、**password** 和 **scheme** 三种。

- 认证方式为 **none**：表示下次使用 Console 口本地登录设备时，不需要进行用户名和密码认证、任何人都可以通过 Console 口登录到设备上，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 Console 口本地登录设备时，需要进行密码认证、只有密码认证成功、用户才能登录到设备上。
- 认证方式为 **scheme**：表示下次使用 Console 口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。用户认证又分为本地认证和远程认证，如果采用本地认证，则需要配置本地用户及相应参数；如果采用远程认证，则需要在远程认证服务器上配置用户名和密码。有关用户认证方式及参数的详细介绍请参见“安全配置指导”中的“AAA”。

不同的认证方式下，Console口登录方式需要进行的配置不同，具体配置如 表 2-3 所示。

表2-3 配置任务简介

<table>
<tr><th>认证方式</th><th colspan="3">认证所需配置</th><th>说明</th></tr>
<tr><td>None</td><td colspan="3">设置登录用户的认证方式为不认证</td><td>具体内容请参见2.2.4</td></tr>
<tr><td rowspan="2">Password</td><td colspan="3">设置登录用户的认证方式为Password认证</td><td rowspan="2">具体内容请参见2.2.5</td></tr>
<tr><td colspan="3">设置本地验证的密码</td></tr>
<tr><td rowspan="6">Scheme</td><td colspan="3">设置登录用户的认证方式为Scheme认证</td><td rowspan="6">具体内容请参见2.2.6</td></tr>
<tr><td rowspan="5">选择认证方案</td><td rowspan="3">采用远端AAA服务器认证</td><td>在设备上配置RADIUS/HWTACACS方案</td></tr>
<tr><td>在设备上配置域使用的AAA方案</td></tr>
<tr><td>在AAA服务器上配置相关的用户名和密码</td></tr>
<tr><td rowspan="2">采用本地认证</td><td>在设备上配置认证用户名和密码</td></tr>
<tr><td>在设备上配置域使用的AAA方案为本地认证</td></tr>
</table>

说明

改变 Console 口登录方式的认证方式后，该认证方式的设置不会立即生效。用户需要退出命令行接口后重新登录，该设置才会生效。

2.2.4 配置通过Console口登录设备时无需认证（None）

1. 配置前提

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

缺省情况下，用户可以直接通过Console口本地登录设备，登录时认证方式为None（不需要用户名和密码），登录用户级别为 3。如何在缺省情况下登录设备，具体请参见“2.2.2 缺省配置下如何通过Console口登录设备“。

2. 配置过程

表2-4 配置用户通过 Console 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AUX用户界面视图	**user-interface aux** *first-number* [*last-number*]	-
设置登录用户的认证方式为不认证	**authentication-mode none**	必选 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） FIPS模式下不支持该命令
配置Console口的公共属性	-	可选 详细配置请参见“2.2.7 配置Console口登录方式的公共属性（可选）”

配置完成后，当用户再次通过 Console 口登录设备时，设备将提示用户键入回车，之后将出现命令行提示符（如<H3C>）。

2.2.5 配置通过Console口登录设备时采用密码认证（Password）

1. 配置前提

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

缺省情况下，用户可以直接通过Console口本地登录设备，登录时认证方式为None（不需要用户名和密码），登录用户级别为 3。如何在缺省情况下登录设备，具体请参见“2.2.2 缺省配置下如何通过Console口登录设备”。

2. 配置过程

表2-5 配置用户通过 Console 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AUX用户界面视图	**user-interface aux** *first-number* [*last-number*]	-
设置登录用户的认证方式为本地密码认证	**authentication-mode password**	必选 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） FIPS模式下不支持该命令
设置本地验证的密码	**set authentication password** [**hash**] { **cipher** | **simple** } *password*	必选 缺省情况下，没有设置本地认证的密码 FIPS模式下不支持该命令。

操作	命令	说明
配置Console口的公共属性	-	可选 详细配置请参见“2.2.7 配置Console口登录方式的公共属性（可选）”

配置完成后，当用户再次通过 Console 口登录设备时，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>）。

2.2.6 配置通过Console口登录设备时采用AAA认证（Scheme）

1. 配置前提

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

缺省情况下，用户可以直接通过Console口本地登录设备，登录时认证方式为None（不需要用户名和密码），登录用户级别为 3。如何在缺省情况下登录设备，具体请参见“2.2.2 缺省配置下如何通过Console口登录设备”。

2. 配置过程

表2-6 配置用户通过 Console 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AUX用户界面视图	**user-interface aux** *first-number* [*last-number*]	-
设置登录用户的认证方式为通过认证方案认证	**authentication-mode scheme**	必选 具体采用本地认证还是RADIUS认证、HWTACACS认证视AAA方案配置而定 非FIPS模式的缺省情况下，用户通过Console口登录，认证方式为none（即不需要进行认证） FIPS模式的缺省情况下，认证为**scheme**方式
使能命令行授权功能	**command authorization**	可选 • 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 • 缺省情况下，用户登录设备后可以使用的命令行由用户级别决定，用户只能使用缺省级别等于/低于用户级别的命令行。配置命令行授权功能后，用户可使用的命令行将受到用户级别和 AAA 授权的双重限制。即便是足够级别的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。

操作		命令	说明
使能命令行计费功能		**command accounting**	可选 • 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 • 命令行计费功能用来在HWTACACS服务器上记录用户对设备执行过的命令（只要设备支持的命令，不管执行成功或者失败都会记录），以便集中监视、控制用户对设备的操作。命令行计费功能生效后，如果没有配命令行授权功能，用户执行的每一条命令都会发送到HWTACACS服务器上做记录；如果配置了命令行授权功能，则每一条授权成功的命令都会发送到HWTACACS服务器上做记录。
退出至系统视图		**quit**	-
配置设备采用的认证方案	进入ISP域视图	**domain** *domain-name*	可选 缺省情况下，系统使用的AAA方案为**local** 如果采用**local**认证，则必须进行后续的本地用户配置；如果采用RADIUS或者HWTACACS方式认证，则需进行如下配置： • 设备上的RADIUS、HWTACACS方案配置请参见“安全配置指导”中的“AAA” • AAA服务器上需要配置相关的用户名和密码，具体请参见服务器的指导书
	配置域使用的AAA方案	**authentication default** { **hwtacacs-scheme** *hwtacacs-scheme-name* [**local**] | **local** | **none** | **radius-scheme** *radius-scheme-name* [**local**] }	
	退出至系统视图	**quit**	
创建本地用户（进入本地用户视图）		**local-user** *user-name*	必选 缺省情况下，无本地用户
设置本地用户认证密码		非FIPS模式下： **password** [[**hash**] { **cipher** | **simple** } *password*] FIPS模式下： **password**	必选 缺省情况下，没有配置本地认证密码
设置本地用户的命令级别		**authorization-attribute level** *level*	可选 缺省情况下，命令级别为0
设置本地用户的服务类型		**service-type terminal**	必选 缺省情况下，无用户服务类型
配置Console口的公共属性		-	可选 详细配置请参见“2.2.7 配置Console口登录方式的公共属性（可选）”

说明

使能命令行授权功能或命令行计费功能后，还需要进行如下配置才能保证命令行授权功能生效：

- 需要创建 HWTACACS 方案，在方案中指定授权服务器的 IP 地址以及授权过程的其它参数；
- 需要在 ISP 域中引用已创建的 HWTACACS 方案。

详细介绍请参见“安全配置指导”中的“AAA”。

说明

需要注意的是用户采用 Scheme 认证方式登录设备时，其所能访问的命令级别取决于 AAA 方案中定义的用户级别。

- AAA 方案为 local 认证时，用户级别通过 **authorization-attribute level** *level* 命令设定。
- AAA 方案为 RADIUS 或者 HWTACACS 方案认证时，在相应的 RADIUS 或者 HWTACACS 服务器上设定相应用户的级别。

有关 AAA、RADIUS、HWTACACS 的详细内容，请参见“安全配置指导”中的“AAA”。

配置完成后，当用户再次通过 Console 口登录设备时，键入回车后，设备将要求用户输入登录用户名和密码，正确输入用户名和密码并回车，登录界面中出现命令行提示符（如<H3C>）。

2.2.7 配置Console口登录方式的公共属性（可选）

Console口登录方式的公共属性配置，如 表 2-7 所示。

表2-7 Console 口登录方式公共属性配置

操作		命令	说明
进入系统视图		**system-view**	-
使能显示版权信息		**copyright-info enable**	可选 缺省情况下，显示版权信息处于使能状态
进入AUX用户界面视图		**user-interface aux** *first-number* [*last-number*]	-
配置Console口的属性	配置传输速率	**speed** *speed-value*	可选 缺省情况下，Console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
	配置校验方式	**parity** { **even** | **none** | **odd** }	可选 缺省情况下，Console口的校验方式为**none**，即不进行校验

操作		命令	说明
	配置停止位	**stopbits** { **1** | **1.5** | **2** }	可选 缺省情况下，Console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
	配置数据位	**databits** { **7** | **8** }	可选 缺省情况下，Console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
	配置启动终端会话的快捷键	**activation-key** *character*	可选 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** { **default** | *character* }	可选 缺省情况下，键入<Ctrl+C>中止当前运行的任务
	配置流量控制方式	**flow-control** { **hardware** | **none** | **software** }	可选 缺省情况下，流量控制方式为**none** 目前设备只支持配置流量控制方式为none
	配置终端的显示类型	**terminal type** { **ansi** | **vt100** }	可选 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
	设置用户登录后可以访问的命令级别	**user privilege level** *level*	可选 缺省情况下，从AUX用户界面登录后可以访问的命令级别为3级
	设置终端屏幕一屏显示的行数	**screen-length** *screen-length*	可选 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*	可选 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
	设置用户界面的超时时间	**idle-timeout** *minutes* [*seconds*]	可选 缺省情况下，所有的用户界面的超时时间为10分钟，如果10分钟内某用户界面没有用户进行操作，则该用户界面将自动断开 **idle-timeout** 0表示关闭用户界面的超时功能

注意

改变 Console 口属性后会立即生效，所以通过 Console 口登录来配置 Console 口属性可能在配置过程中发生连接中断，建议通过其他登录方式来配置 Console 口属性。若用户需要通过 Console 口再次登录设备，需要改变 PC 机上运行的终端仿真程序的相应配置，使之与设备上配置的 Console 口属性保持一致。

2.3 配置通过Telnet登录设备

2.3.1 通过Telnet登录设备简介

设备支持Telnet功能，用户可以通过Telnet方式登录到设备上，对设备进行远程管理和维护。如 图2-7。

图2-7 通过 Telnet 登录设备示意图

表2-8 采用 Telnet 方式登录需要具备的条件

对象	需要具备的条件
Telnet服务器端	配置设备IP地址，设备与Telnet用户间路由可达
	配置Telnet登录的认证方式和其它配置（根据Telnet服务器端的情况而定）
Telnet客户端	运行Telnet程序
	获取要登录设备的IP地址

设备可以作为 Telnet Client 登录到 Telnet Server 上，从而对其进行操作。

设备可以充当 Telnet Server：

- 设备支持 Telnet Server 功能、可作为 Telnet Server，并可在设备上进行一系列的配置，从而实现对不同 Telnet Client 登录的具体认证方式、用户级别等方面的控制与管理。
- 缺省情况下，设备的 Telnet Server 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。因此当您使用 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 Server 功能，然后对认证方式、用户级别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。

本节将为您介绍设备充当 Telnet 服务器端时：

- 设备支持的各种登录认证方式及配置Telnet登录认证方式的意义、各种认证方式的特点及注意事项。具体介绍请参见“2.3.2 Telnet登录的认证方式介绍”。

- 当用户确定了今后通过Telnet客户端登录设备时将采用何种认证方式后、并已成功登录到设备后，用户如何在设备上配置Telnet客户端登录设备时的认证方式、用户级别及公共属性，从而实现对Telnet登录用户的控制和管理。具体介绍请参见“2.3.3 配置通过Telnet Client登录设备时无需认证（None）”、“2.3.4 配置通过Telnet Client登录设备时采用密码认证（Password）”及“2.3.5 配置通过Telnet Client登录设备时采用AAA认证（Scheme）”。
- 配置通过Telnet登录设备时的公共属性。具体介绍请参见“2.3.6 配置VTY用户界面的公共属性（可选）”。

本节还将为您介绍设备充当Telnet客户端、Telnet登录到Server时的配置，具体请参见“2.3.7 配置设备充当Telnet Client登录到Telnet Server”。

2.3.2 Telnet登录的认证方式介绍

通过在 Telnet 的用户界面下配置认证方式，可以对使用 Telnet 登录的用户进行限制，以提高设备的安全性。通过 Telnet 登录支持的认证方式有 **none**、**password** 和 **scheme** 三种。

- 认证方式为 **none**：表示下次使用 Telnet 登录设备时不需要进行用户名和密码认证，任何人都可以通过 Telnet 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 Telnet 登录设备时需要进行密码认证，只有密码认证成功，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，如果密码丢失，可以使用 Console 口登录到设备，对 Telnet 的密码配置进行修改。
- 认证方式为 **scheme**：表示下次使用 Telnet 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。用户认证又分为本地认证和远程认证，如果采用本地认证，则需要配置本地用户及相应参数；如果采用远程认证，则需要在远程认证服务器上配置用户名和密码。有关用户认证方式及参数的详细介绍请参见“安全配置指导”中的“AAA”。配置认证方式为 **scheme** 后，请妥善保存用户名及密码，如果本地认证密码丢失，可以使用 Console 口登录到设备，对 Telnet 的密码配置进行修改。如果远程认证密码丢失，建议您联系服务器管理员。

不同的认证方式下，Telnet登录方式需要进行的配置不同，具体配置如 表 2-9 所示。

表2-9 配置 Telnet 登录的认证方式

<table>
<tr><th>认证方式</th><th colspan="3">认证所需配置</th><th>说明</th></tr>
<tr><td>None</td><td colspan="3">设置登录用户的认证方式为不认证</td><td>具体内容请参见2.3.3</td></tr>
<tr><td rowspan="2">Password</td><td colspan="3">设置登录用户的认证方式为Password认证</td><td rowspan="2">具体内容请参见2.3.4</td></tr>
<tr><td colspan="3">设置本地验证的密码</td></tr>
<tr><td rowspan="4">Scheme</td><td colspan="3">设置登录用户的认证方式为Scheme认证</td><td rowspan="4">具体内容请参见2.3.5</td></tr>
<tr><td rowspan="3">选择认证方案</td><td rowspan="3">采用远端AAA服务器认证</td><td>在设备上配置RADIUS/HWTACACS方案</td></tr>
<tr><td>在设备上配置域使用的AAA方案</td></tr>
<tr><td>在AAA服务器上配置相关的用户名和密码</td></tr>
</table>

认证方式	认证所需配置			说明
		采用本地认证	在设备上配置认证用户名和密码	
			在设备上配置域使用的AAA方案为本地认证	

2.3.3 配置通过Telnet Client登录设备时无需认证（None）

1. 配置前提

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。

缺省情况下，用户可以直接通过Console口本地登录设备，登录时认证方式为None（不需要用户名和密码），登录用户级别为 3。如何在缺省情况下登录设备，具体请参见“2.2.2 缺省配置下如何通过Console口登录设备”。

2. 配置过程

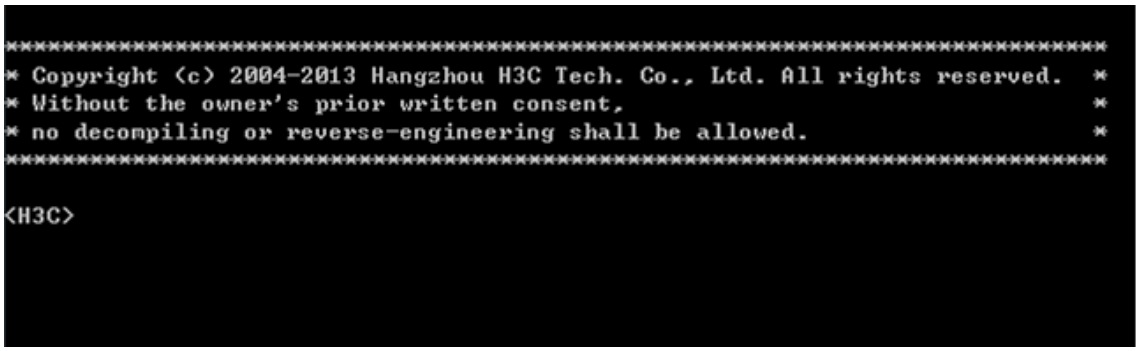
表2-10 认证方式为 None 的配置

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**	必选 缺省情况下，Telnet服务处于关闭状态
进入一个或多个VTY用户界面视图	**user-interface vty** *first-number* [*last-number*]	-
设置VTY登录用户的认证方式为不认证	**authentication-mode none**	必选 缺省情况下，VTY用户界面的认证方式为**password**
配置从当前用户界面登录系统的用户所能访问的命令级别	**user privilege level** *level*	必选 缺省情况下，通过VTY用户界面登录系统所能访问的命令级别是0
配置VTY用户界面的公共属性	-	可选 详细配置请参见“2.3.6 配置VTY用户界面的公共属性（可选）”

配置完成后，当用户再次通过 Telnet 登录设备时：

- 用户将直接进入VTY用户界面，如 图 2-8 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2-8 用户通过 Telnet 登录设备时无需认证登录界面



2.3.4 配置通过Telnet Client登录设备时采用密码认证（Password）

1. 配置前提

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。

缺省情况下，用户可以直接通过Console口本地登录设备，登录时认证方式为None（不需要用户名和密码），登录用户级别为 3。如何在缺省情况下登录设备，具体请参见“2.2.2 缺省配置下如何通过Console口登录设备”。

2. 配置过程

表2-11 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**	必选 缺省情况下，Telnet服务处于关闭状态
进入一个或多个VTY用户界面视图	**user-interface vty** *first-number* [*last-number*]	-
设置登录用户的认证方式为本地密码认证	**authentication-mode password**	必选 缺省情况下，VTY用户界面的认证方式为**password**
设置本地验证的密码	**set authentication password** [**hash**] { **cipher** | **simple** } *password*	必选 缺省情况下，没有设置本地认证的密码
配置从当前用户界面登录系统的用户所能访问的命令级别	**user privilege level** *level*	必选 缺省情况下，通过VTY用户界面登录系统所能访问的命令级别是0
配置VTY用户界面的公共属性	-	可选 详细配置请参见“2.3.6 配置VTY用户界面的公共属性（可选）”

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 2-9 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2-9 配置用户通过 Telnet 登录设备时采用密码认证登录界面

2.3.5 配置通过Telnet Client登录设备时采用AAA认证（Scheme）

1. 配置前提

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。

缺省情况下，用户可以直接通过Console口本地登录设备，登录时认证方式为None（不需要用户名和密码），登录用户级别为 3。如何在缺省情况下登录设备，具体请参见“2.2.2 缺省配置下如何通过Console口登录设备”。

2. 配置过程

表2-12 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**	必选 缺省情况下，Telnet服务处于关闭状态
进入一个或多个VTY用户界面视图	**user-interface vty** *first-number* [*last-number*]	-
设置登录用户的认证方式为通过认证方案认证	**authentication-mode scheme**	必选 具体采用本地认证还是RADIUS认证、HWTACACS认证视AAA方案配置而定 缺省情况下采用本地认证方式

操作		命令	说明
使能命令行授权功能		**command authorization**	可选 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 • 需要创建 HWTACACS 方案，在方案中指定授权服务器的 IP 地址以及授权过程的其它参数，详细介绍请参见“安全配置指导”中的“AAA” • 需要在 ISP 域中引用已创建的 HWTACACS 方案，详细介绍请参见“安全配置指导”中的“AAA”
使能命令行计费功能		**command accounting**	可选 • 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 • 命令行计费功能用来在 HWTACACS 服务器上记录用户对设备执行过的命令（只要设备支持的命令，不管执行成功或者失败都会记录），以便集中监视、控制用户对设备的操作。命令行计费功能生效后，如果没有配命令行授权功能，用户执行的每一条命令都会发送到 HWTACACS 服务器上做记录；如果配置了命令行授权功能，则每一条授权成功的命令都会发送到 HWTACACS 服务器上做记录。
退出至系统视图		**quit**	-
配置设备采用的认证方案	进入ISP域视图	**domain** *domain-name*	可选 缺省情况下，系统使用的AAA方案为**local** 如果采用**local**认证，则必须进行后续的本地用户配置；如果采用RADIUS或者HWTACACS方式认证，则需进行如下配置： • 设备上的配置请参见“安全配置指导”中的“AAA” • AAA 服务器上需要配置相关的用户名和密码，具体请参见服务器的指导书
	配置域使用的AAA方案	**authentication default** { **hwtacacs-scheme** *hwtacacs-scheme-name* [**local**] | **local** | **none** | **radius-scheme** *radius-scheme-name* [**local**] }	
	退出至系统视图	**quit**	
创建本地用户（进入本地用户视图）		**local-user** *user-name*	缺省情况下，无本地用户
设置本地认证密码		**password** [[**hash**] { **cipher** | **simple** } *password*]	必选 缺省情况下，没有配置本地认证密码
设置用户的命令级别		**authorization-attribute level** *level*	可选 缺省情况下，命令级别为0

操作	命令	说明
设置用户的服务类型	**service-type telnet**	必选 缺省情况下，无用户的服务类型
退出至系统视图	**quit**	-
配置VTY用户界面的公共属性	-	可选 详细配置请参见“2.3.6 配置VTY用户界面的公共属性（可选）”

说明

使能命令行授权功能或命令行计费功能后，还需要进行如下配置才能保证命令行授权功能生效：

- 需要创建 HWTACACS 方案，在方案中指定授权服务器的 IP 地址以及授权过程的其它参数；
- 需要在 ISP 域中引用已创建的 HWTACACS 方案。

详细介绍请参见“安全配置指导”中的“AAA”。

说明

需要注意的是用户采用 Scheme 认证方式登录设备时，其所能访问的命令级别取决于 AAA 方案中定义的用户级别。

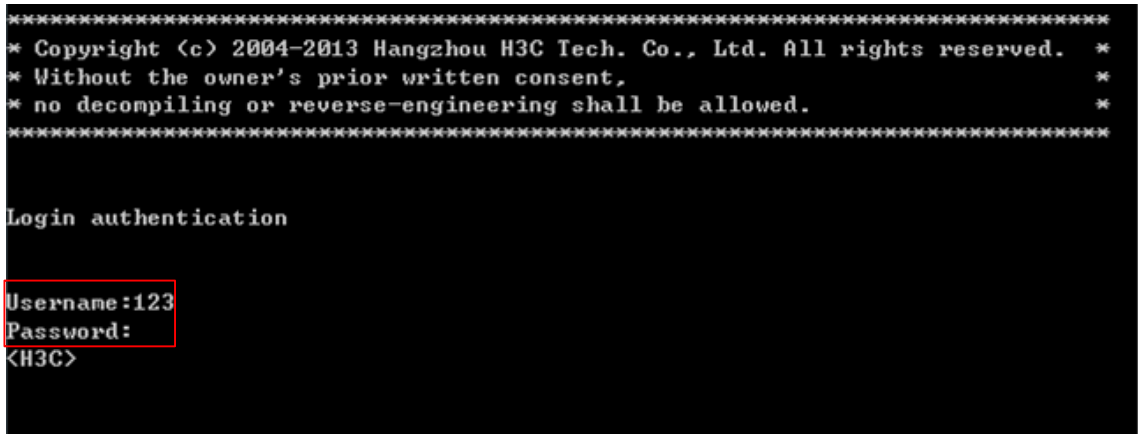
- AAA 方案为 local 认证时，用户级别通过 **authorization-attribute level** *level* 命令设定。
- AAA 方案为 RADIUS 或者 HWTACACS 方案认证时，在相应的 RADIUS 或者 HWTACACS 服务器上设定相应用户的级别。

有关 AAA、RADIUS、HWTACACS 的详细内容，请参见“AAA 配置指导”中的“AAA”。

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（此处以用户名 123 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 2-10 所示。
- 如果用户输入正确的登录用户名和密码后，设备提示用户再次输入一个指定类型的密码，则表示当前用户需要进行二次密码认证，即用户还必须根据提示信息输入一个正确的密码后才能通过认证。
- 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2-10 用户通过 Telnet 登录设备时 AAA 认证登录界面



2.3.6 配置VTY用户界面的公共属性（可选）

表2-13 VTY 用户界面的公共属性配置

操作		命令	说明
进入系统视图		**system-view**	-
使能显示版权信息		**copyright-info enable**	可选 缺省情况下，显示版权信息处于使能状态
进入一个或多个VTY用户界面视图		**user-interface vty** *first-number* [*last-number*]	-
VTY用户界面配置	启动终端服务	**shell**	可选 缺省情况下，在所有的用户界面上启动终端服务
	配置VTY用户界面支持的协议	**protocol inbound** { **all** | **ssh** | **telnet** }	可选 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界面登录时生效 FIPS模式下不包括**telnet**参数
	配置中止当前运行任务的快捷键	**escape-key** { **default** | *character* }	可选 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** }	可选 缺省情况下，终端显示类型为ANSI

操作		命令	说明
	设置终端屏幕一屏显示的行数	**screen-length** *screen-length*	可选 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*	可选 缺省情况下，每个用户的历史缓冲区大小为10，即可存放10条历史命令
	设置VTY用户界面的超时时间	**idle-timeout** *minutes* [*seconds*]	可选 缺省情况下，所有的用户界面的超时时间为10分钟 如果10分钟内某用户界面没有用户进行操作，则该用户界面将自动断开 **idle-timeout** 0表示关闭用户界面的超时功能
	设置从用户界面登录后自动执行的命令	**auto-execute command** *command*	可选 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

注意

- 使用 **auto-execute command** 命令后，可能导致用户不能通过该终端线对本系统进行常规配置，需谨慎使用。
- 在配置 **auto-execute command** 命令并保存配置（执行 save 操作）之前，要确保可以通过其他 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。

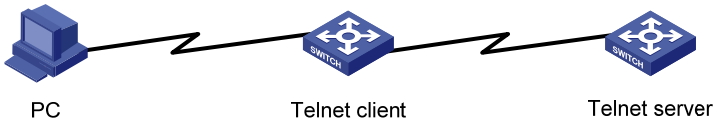
2.3.7 配置设备充当Telnet Client登录到Telnet Server

1. 配置前提

用户已经成功登录到了设备上，并希望将当前设备作为Telnet Client登录到Telnet Server上进行操作。具体请参见 图 2-11 所示。

缺省情况下，用户可以直接通过Console口本地登录设备，登录时认证方式为None（不需要用户名和密码），登录用户级别为 3。如何在缺省情况下登录设备，具体请参见“2.2.2 缺省配置下如何通过Console口登录设备”。

图2-11 通过交换机登录到其它交换机



说明

如果 Telnet Client 与 Telnet Server 相连的端口不在同一子网内，请确保两台设备间路由可达。

2. 配置过程

表2-14 设备作为 Telnet Client 登录到 Telnet Server 的配置

操作	命令	说明
设备作为Telnet Client登录到Telnet Server	**telnet** *remote-host* [*service-port*] [[**vpn-instance** *vpn-instance-name*] | [**source** { **interface** *interface-type interface-number* | **ip** *ip-address* }]]	二者必选其一 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*]	
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* }	可选 此命令在系统视图下执行 缺省情况下，没有指定发送Telnet报文的源IPv4地址和源接口，此时通过路由选择源IPv4地址

配置完成后，设备即可登录到相应的 Telnet Server 上。

2.3.8 配置Telnet报文的DSCP优先级

表2-15 配置 Telnet 报文的 DSCP 优先级

操作	命令	说明
进入系统视图	**system-view**	-
配置IPv4 Telnet客户端发送报文的DSCP优先级	**telnet client dscp** *dscp-value*	可选 缺省情况下，IPv4 Telnet客户端发送报文的DSCP优先级为16
配置IPv6 Telnet客户端发送报文的DSCP优先级	**telnet client ipv6 dscp** *dscp-value*	可选 缺省情况下，IPv6 Telnet客户端发送报文的DSCP优先级为0
配置IPv4 Telnet服务器发送报文的DSCP优先级	**telnet server dscp** *dscp-value*	可选 缺省情况下，IPv4 Telnet服务器发送报文的DSCP优先级为48

操作	命令	说明
配置IPv6 Telnet服务器发送报文的DSCP优先级	**telnet server ipv6 dscp** *dscp-value*	可选 缺省情况下，IPv6 Telnet服务器发送报文的DSCP优先级为0

2.4 配置通过SSH登录

2.4.1 通过SSH登录设备简介

SSH是Secure Shell（安全外壳）的简称。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。设备支持SSH功能，用户可以通过SSH方式登录到设备上，对设备进行远程管理和维护如 图 2-12 所示。

图2-12 通过 SSH 登录

表2-16 采用 SSH 方式登录需要具备的条件

对象	需要具备的条件
SSH服务器端	配置设备的IP地址，设备与SSH客户端间路由可达
	配置SSH登录的认证方式和其它配置（根据SSH服务器端的情况而定）
SSH客户端	如果是主机作为SSH客户端，则需要在主机上运行SSH客户端程序
	获取要登录设备的IP地址

设备可以作为 SSH Client 登录到 SSH Server 上，从而对其进行操作。

设备可以充当 SSH Server：

- 设备支持 SSH Server 功能：可作为 SSH Server，并可在设备上进行一系列的配置、实现对不同 SSH Client 的登录权限的控制。
- 缺省情况下，设备的 SSH Server 功能处于关闭状态，因此当您使用 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 Server 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。

本节将为您介绍：

- 设备充当SSH服务器端时：当用户确定了今后通过SSH客户端登录设备、并已成功登录到设备后，用户如何在设备上配置SSH客户端登录设备时的认证方式及其它属性，从而实现对SSH登录用户的控制和管理。具体介绍请参见“2.4.2 配置设备充当SSH服务器”。
- 设备充当SSH客户端时：设备SSH登录到Server时的配置，具体请参见“2.4.3 配置设备充当SSH客户端登录其它设备”。

2.4.2 配置设备充当SSH服务器

1. 配置前提

用户已经成功登录到了设备上，并希望以后通过 SSH Client 登录设备。

缺省情况下，用户可以直接通过Console口本地登录设备，登录时认证方式为None（不需要用户名和密码），登录用户级别为 3。如何在缺省情况下登录设备，具体请参见“2.2.2 缺省配置下如何通过Console口登录设备”。

2. 配置过程

表2-17 设备充当 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** }	必选 缺省情况下，没有生成密钥对
使能SSH服务器功能		**ssh server enable**	必选 缺省情况下，SSH服务器功能处于关闭状态
进入VTY用户界面视图		**user-interface vty** *first-number* [*last-number*]	-
配置登录用户界面的认证方式为**scheme**方式		**authentication-mode scheme**	必选 非FIPS模式的缺省情况下，用户界面认证为**password**方式 FIPS模式的缺省情况下，认证为**scheme**方式
配置所在用户界面支持SSH协议	非FIPS模式下	**protocol inbound** { **all** | **ssh** | **telnet**}	可选 非FIPS模式的缺省情况下，系统支持所有的协议，即支持Telnet和SSH FIPS模式的缺省情况下，用户界面仅支持SSH协议
	FIPS模式下	**protocol inbound { all | ssh }**	
使能命令行授权功能		**command authorization**	可选 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 • 需要创建 HWTACACS 方案，在方案中指定授权服务器的 IP 地址以及授权过程的其它参数，详细介绍请参见“安全配置指导”中的“AAA” • 需要在 ISP 域中引用已创建的 HWTACACS 方案，详细介绍请参见“安全配置指导”中的“AAA”

操作		命令	说明
使能命令行计费功能		**command accounting**	可选 • 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 • 命令行计费功能用来在HWTACACS服务器上记录用户对设备执行过的命令（只要设备支持的命令，不管执行成功或者失败都会记录），以便集中监视、控制用户对设备的操作。命令行计费功能生效后，如果没有配命令行授权功能，用户执行的每一条命令都会发送到HWTACACS服务器上做记录；如果配置了命令行授权功能，则每一条授权成功的命令都会发送到HWTACACS服务器上做记录。
退出至系统视图		**quit**	-
配置设备采用的认证方案	进入ISP域视图	**domain** *domain-name*	可选 缺省情况下，系统使用的AAA方案为local 如果采用local认证，则必须进行后续的本地用户配置；如果采用RADIUS或者HWTACACS方式认证，则需进行如下配置： • 设备上的配置请参见“安全配置指导”中的“AAA” • AAA服务器上需要配置相关的用户名和密码，具体请参见服务器的指导书
	配置域使用的AAA方案	**authentication default** { **hwtacacs-scheme** *hwtacacs-scheme-name* [**local**] | **local** | **none** | **radius-scheme** *radius-scheme-name* [**local**] }	
	退出至系统视图	**quit**	
创建本地用户，并进入本地用户视图		**local-user** *user-name*	必选 缺省情况下，没有配置本地用户
设置本地认证密码		非FIPS模式下： **password** [[**hash**] { **cipher** | **simple** } *password*] FIPS模式下： **password**	必选 缺省情况下，没有配置本地认证密码
设置本地用户的命令级别		**authorization-attribute level** *level*	可选 缺省情况下，命令级别为0
设置本地用户的服务类型		**service-type ssh**	必选 缺省情况下，无用户的服务类型
退回系统视图		**quit**	-

操作	命令	说明
建立SSH用户，并指定SSH用户的认证方式	**ssh user** *username* **service-type stelnet authentication-type** { **password** | { **any** | **password-publickey** | **publickey** } **assign publickey** *keyname* }	必选
配置VTY用户界面的公共属性	-	可选 详细配置请参见“2.3.6 配置VTY用户界面的公共属性（可选）”

说明

本章只介绍采用 **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”。

说明

使能命令行授权功能或命令行计费功能后，还需要进行如下配置才能保证命令行授权功能生效：

- 需要创建 HWTACACS 方案，在方案中指定授权服务器的 IP 地址以及授权过程的其它参数；
- 需要在 ISP 域中引用已创建的 HWTACACS 方案。

详细介绍请参见“安全配置指导”中的“AAA”。

说明

- 用户采用 **password** 认证方式登录设备时，其所能访问的命令级别取决于 AAA 方案中定义的用户级别。AAA 方案为 local 认证时，用户级别通过 **authorization-attribute level** *level* 命令设定；AAA 方案为 RADIUS 或者 HWTACACS 方案认证时，在相应的 RADIUS 或者 HWTACACS 服务器上设定相应用户的级别。有关 AAA、RADIUS、HWTACACS 的详细内容，请参见“AAA 配置指导”中的“AAA”。
- 用户采用 **publickey** 认证方式登录设备时，其所能访问的命令级别取决于用户界面上通过 **user privilege level** 命令配置的级别。

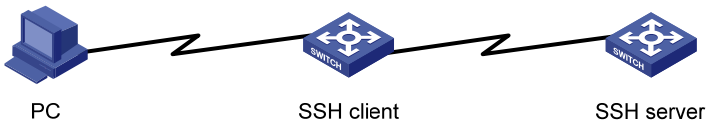
2.4.3 配置设备充当SSH客户端登录其它设备

1. 配置前提

用户已经成功登录到了设备上，并希望将当前设备作为SSH Client登录到其它设备上进行操作。具体请参见 图 2-11 所示。

缺省情况下，用户可以直接通过Console口本地登录设备，登录时认证方式为None（不需要用户名和密码），登录用户级别为 3。如何在缺省情况下登录设备，具体请参见“2.2.2 缺省配置下如何通过Console口登录设备”。

图2-13 通过设备登录到其它设备



说明

如果 SSH Client 与 SSH Server 相连的端口不在同一子网内，请确保两台设备间路由可达。

2. 配置过程

表2-18 设备作为 SSH Client 登录到其它设备的配置

操作	命令	说明
设备作为SSH Client登录到SSH IPv4服务器端	**ssh2** *server*	必选 *server*：服务器IPv4地址或主机名称，为1～20个字符的字符串，不区分大小写 此命令在用户视图下执行
设备作为SSH Client登录到SSH IPv6服务器端	**ssh2 ipv6** *server*	必选 *server*：服务器的IPv6地址或主机名称，为1～46个字符的字符串，不区分大小写。

说明

为配合 SSH Server，设备充当 SSH Client 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”。

配置完成后，设备即可登录到相应的 SSH Server 上。

2.5 配置通过Modem登录设备

2.5.1 通过Modem登录设备简介

网络管理员可以通过设备的 Console 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。

本节将为您介绍如何通过 Modem 登录设备，并配置登录时的认证方式、用户级别及公共属性，实现对 Modem 登录用户的控制。

本节将为您介绍：

- 设备支持Modem登录认证方式及配置Modem登录认证方式的意义、各种认证方式的特点及注意事项。具体请参见“2.5.3 Modem拨号登录的认证方式介绍”。
- 当用户确定了今后通过Modem登录设备时将采用何种认证方式后、并通过缺省配置登录到设备后，用户如何在设备上配置Modem登录设备时的认证方式及用户级别，实现对Modem登录用户的控制和管理。具体请参见“2.5.4 配置用户通过Modem登录设备时无需认证（None）”、“2.5.5 配置用户通过Modem登录设备时采用密码认证（Password）”及“2.5.6 配置用户通过Modem登录设备时采用AAA认证（Scheme）”。
- 配置通过Modem登录设备时的公共属性。具体请参见“2.5.7 配置AUX用户界面的公共属性（可选）”。

2.5.2 缺省配置下如何通过Modem登录设备

缺省情况下，用户通过 Modem 登录设备时，设备不需要任何登录认证，缺省可以访问命令级别为 3 级的命令。

通过 Modem 登录设备的方法如下：

表2-19 通过 Console 口利用 Modem 拨号进行远程登录需要具备的条件

配置对象	需要具备的条件
网络管理员端	PC终端与Modem正确连接
	Modem与可正常使用的电话线正确相连
	获取了远程设备端Console口所连Modem上对应的电话号码
设备端	Console口与Modem正确连接
	在Modem上进行了正确的配置
	Modem与可正常使用的电话线正确相连
	设备上配置了登录用户的认证方式、用户级别及其它配置

(1) 如 图 2-14 所示，建立远程配置环境，在PC机（或终端）的串口和设备的Console口分别挂接Modem。

图2-14 搭建远程配置环境

(2) 网络管理员端的相关配置。

PC 终端与 Modem 正确连接、Modem 与可正常使用的电话线正确相连、获取了远程设备端 Console 口所连 Modem 上对应的电话号码。

注意

通过 Console 口利用 Modem 拨号进行远程登录时，使用的是 AUX 用户界面，设备上的配置需要注意以下几点：

- 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。
- Console 口的其它属性（校验方式、停止位、数据位）均采用缺省值。

(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 2-15 至 图 2-17 所示。

说明

如果您的 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；如果您的 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2-15 新建连接

图2-16 拨号号码配置

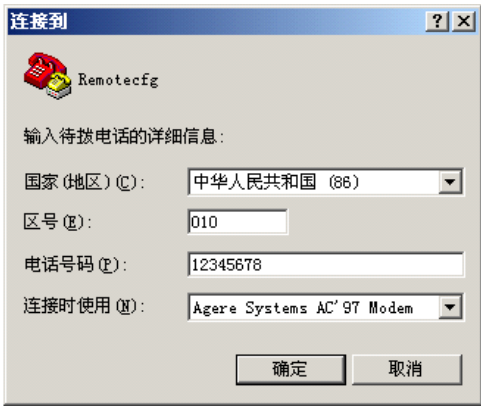
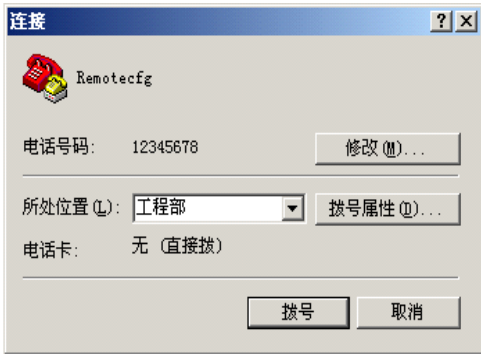
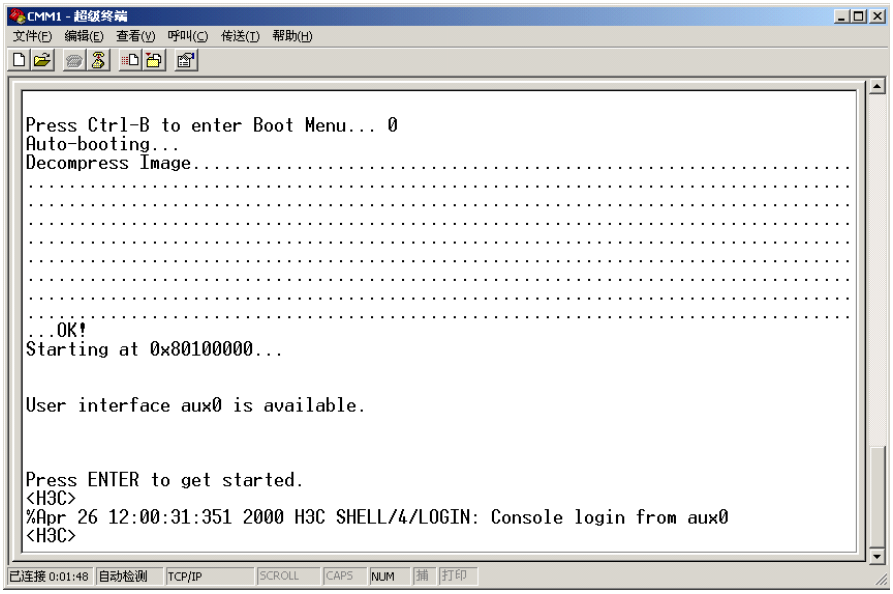


图2-17 在远端 PC 机上拨号



(6) 当听到拨号音后，超级终端窗口将返回字符串“CONNECT9600”，键入回车键之后将出现命令行提示符（如<H3C>），如 图 2-18 所示。

图2-18 Console 口登录界面



(7) 如果配置验证方式为 Password，在远端的终端仿真程序上输入已配置的登录密码，出现命令行提示符（如<H3C>），即可对设备进行配置或管理。需要帮助可以随时键入“?”，具体的配置命令请参考本手册中相关模块的内容。

(8) 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“?”，具体的配置命令请参考本手册中相关部分的内容。

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。

2.5.3 Modem拨号登录的认证方式介绍

通过在 AUX 用户界面下配置认证方式，可以对使用 Modem 拨号登录的用户进行限制，以提高设备的安全性。Modem 拨号支持的认证方式有 **none**、**password** 和 **scheme** 三种。

- 认证方式为 **none**：表示下次使用 Modem 拨号登录设备时，不需要进行用户名和密码认证、任何人都可以通过 Modem 拨号登录到设备上，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 Modem 拨号登录设备时，需要进行密码认证、只有密码认证成功、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，如果密码丢失，则无法使用该方式登录。

- 认证方式为 **scheme**：表示下次使用 Modem 拨号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。用户认证又分为本地认证和远程认证，如果采用本地认证，则需要配置本地用户及相应参数；如果采用远程认证，则需要在远程认证服务器上配置用户名和密码。有关用户认证方式及参数的详细介绍请参见“安全配置指导”中的“AAA”。配置认证方式为 **scheme** 后，请妥善保存用户名及密码。如果远程认证密码丢失，建议您联系服务器管理员。

不同的认证方式下，Modem拨号登录方式需要进行的配置不同，具体配置如 表 2-3 所示。

表2-20 配置任务简介

<table>
<tr><th>认证方式</th><th colspan="3">认证所需配置</th><th>说明</th></tr>
<tr><td>None</td><td colspan="3">设置登录用户的认证方式为不认证</td><td>具体内容请参见2.5.4</td></tr>
<tr><td rowspan="2">Password</td><td colspan="3">设置登录用户的认证方式为Password认证</td><td rowspan="2">具体内容请参见2.5.5</td></tr>
<tr><td colspan="3">设置本地验证的密码</td></tr>
<tr><td rowspan="6">Scheme</td><td colspan="3">设置登录用户的认证方式为Scheme认证</td><td rowspan="6">具体内容请参见2.5.6</td></tr>
<tr><td rowspan="5">选择认证方案</td><td rowspan="3">采用远端AAA服务器认证</td><td>在设备上配置RADIUS/HWTACACS方案</td></tr>
<tr><td>在设备上配置域使用的AAA方案</td></tr>
<tr><td>在AAA服务器上配置相关的用户名和密码</td></tr>
<tr><td rowspan="2">采用本地认证</td><td>在设备上配置认证用户名和密码</td></tr>
<tr><td>在设备上配置域使用的AAA方案为本地认证</td></tr>
</table>

说明

改变 Modem 拨号登录方式的认证方式后，该认证方式的设置不会立即生效。用户需要退出命令行接口后重新登录，该设置才会生效。

2.5.4 配置用户通过Modem登录设备时无需认证（None）

1. 配置前提

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

缺省情况下，用户可以直接通过Console口本地登录设备，登录时认证方式为None（不需要用户名和密码），登录用户级别为 3。如何在缺省情况下登录设备，具体请参见“2.2.2 缺省配置下如何通过Console口登录设备”。

2. 配置过程

表2-21 配置用户通过 Modem 拨号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AUX用户界面视图	**user-interface aux** *first-number* [*last-number*]	-
设置登录用户的认证方式为不认证	**authentication-mode none**	必选 缺省情况下，用户通过Modem拨号登录，认证方式为none（即不需要进行认证） FIPS模式下不支持该命令
配置AUX用户界面的公共属性	-	可选 详细配置请参见“2.5.7 配置AUX用户界面的公共属性（可选）”

配置完成后，当用户再次通过 Modem 拨号登录设备时，设备将提示用户键入回车，之后将出现命令行提示符（如<H3C>）。

2.5.5 配置用户通过Modem登录设备时采用密码认证（Password）

1. 配置前提

用户已经成功登录到了设备上，并希望以后通过 Modem 拨号登录设备时采用密码认证、以提高设备的安全性。

缺省情况下，用户可以直接通过Console口本地登录设备，登录时认证方式为None（不需要用户名和密码），登录用户级别为 3。如何在缺省情况下登录设备，具体请参见“2.2.2 缺省配置下如何通过Console口登录设备”。

2. 配置过程

表2-22 配置用户通过 Modem 拨号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AUX用户界面视图	**user-interface aux** *first-number* [*last-number*]	-
设置登录用户的认证方式为本地密码认证	**authentication-mode password**	必选 缺省情况下，用户通过Modem登录，认证方式为none（即不需要进行认证） FIPS模式下不支持该命令
设置本地验证的密码	**set authentication password** [**hash**] { **cipher** | **simple** } *password*	必选 缺省情况下，没有设置本地认证的密码 FIPS模式下不支持该命令。

操作	命令	说明
配置AUX用户界面的公共属性	-	可选 详细配置请参见“2.5.7 配置AUX用户界面的公共属性（可选）”

配置完成后，当用户再次通过 Modem 拨号登录设备时，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>）。

2.5.6 配置用户通过Modem登录设备时采用AAA认证（Scheme）

1. 配置前提

用户已经成功的登录到了设备上，并希望以后通过 Modem 拨号登录设备时采用 AAA 认证、以提高设备的安全性。

缺省情况下，用户可以直接通过Console口本地登录设备，登录时认证方式为None（不需要用户名和密码），登录用户级别为 3。如何在缺省情况下登录设备，具体请参见“2.2.2 缺省配置下如何通过Console口登录设备”。

2. 配置过程

表2-23 配置用户通过 Modem 拨号登录设备时采用 AAA 认证

操作	命令	说明
进入系统视图	**system-view**	-
进入AUX用户界面视图	**user-interface aux** *first-number* [*last-number*]	-
设置登录用户的认证方式为通过认证方案认证	**authentication-mode scheme**	必选 具体采用本地认证还是RADIUS认证、HWTACACS认证视AAA方案配置而定 非FIPS模式的缺省情况下，用户通过Console口登录，认证方式为none（即不需要进行认证） FIPS模式的缺省情况下，认证为**scheme**方式

操作		命令	说明
使能命令行授权功能		**command authorization**	可选 • 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 • 缺省情况下，用户登录设备后可以使用的命令行由用户级别决定，用户只能使用缺省级别等于/低于用户级别的命令行。配置命令行授权功能后，用户可使用的命令行将受到用户级别和 AAA 授权的双重限制。即便是足够级别的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。
使能命令行计费功能		**command accounting**	可选 • 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 • 命令行计费功能用来在 HWTACACS 服务器上记录用户对设备执行过的命令（只要设备支持的命令，不管执行成功或者失败都会记录），以便集中监视、控制用户对设备的操作。命令行计费功能生效后，如果没有配命令行授权功能，用户执行的每一条命令都会发送到 HWTACACS 服务器上做记录；如果配置了命令行授权功能，则每一条授权成功的命令都会发送到 HWTACACS 服务器上做记录。
退出至系统视图		**quit**	-
配置设备采用的认证方案	进入ISP域视图	**domain** *domain-name*	可选 缺省情况下，系统使用的AAA方案为local 如果采用local认证，则必须进行后续的本地用户配置；如果采用RADIUS或者HWTACACS方式认证，则需进行如下配置： • 设备上的 RADIUS、HWTACACS 方案配置请参见“安全配置指导”中的“AAA” • AAA 服务器上需要配置相关的用户名和密码，具体请参见服务器的指导书
	配置域使用的AAA方案	**authentication default** { **hwtacacs-scheme** *hwtacacs-scheme-name* [**local**] | **local** | **none** | **radius-scheme** *radius-scheme-name* [**local**] }	
	退出至系统视图	**quit**	
创建本地用户（进入本地用户视图）		**local-user** *user-name*	必选 缺省情况下，无本地用户

操作	命令	说明
设置本地用户认证密码	非FIPS模式下： **password** [[**hash**] { **cipher** | **simple** } *password*] FIPS模式下： **password**	必选 缺省情况下，没有配置本地认证密码
设置本地用户的命令级别	**authorization-attribute level** *level*	可选 缺省情况下，命令级别为0
设置本地用户的服务类型	**service-type terminal**	必选 缺省情况下，无用户服务类型
配置AUX用户界面的公共属性	-	可选 详细配置请参见“2.5.7 配置AUX用户界面的公共属性（可选）”

说明

使能命令行授权功能或命令行计费功能后，还需要进行如下配置才能保证命令行授权功能生效：

- 需要创建 HWTACACS 方案，在方案中指定授权服务器的 IP 地址以及授权过程的其它参数；
- 需要在 ISP 域中引用已创建的 HWTACACS 方案。

详细介绍请参见“安全配置指导/AAA”中的“配置 ISP 域的 AAA 授权方法”。

说明

需要注意的是用户采用 Scheme 认证方式登录设备时，其所能访问的命令级别取决于 AAA 方案中定义的用户级别。

- AAA 方案为 local 认证时，用户级别通过 **authorization-attribute level** *level* 命令设定。
- AAA 方案为 RADIUS 或者 HWTACACS 方案认证时，在相应的 RADIUS 或者 HWTACACS 服务器上设定相应用户的级别。

有关 AAA、RADIUS、HWTACACS 的详细内容，请参见“安全配置指导”中的“AAA”。

配置完成后，当用户再次通过 Modem 拨号登录设备时，键入回车后，设备将要求用户输入登录用户名和密码，正确输入用户名和密码并回车，登录界面中出现命令行提示符（如<H3C>）。

2.5.7 配置AUX用户界面的公共属性（可选）

表2-24 AUX 用户界面的公共属性配置

操作	命令	说明
进入系统视图	**system-view**	-

操作		命令	说明
使能显示版权信息		**copyright-info enable**	可选 缺省情况下，显示版权信息处于使能状态
进入AUX用户界面视图		**user-interface aux** *first-number* [*last-number*]	-
配置AUX用户界面的属性	配置传输速率	**speed** *speed-value*	可选 缺省情况下，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
	配置校验方式	**parity** { **even** | **none** | **odd** }	可选 缺省情况下，校验方式为**none**，即不进行校验
	配置停止位	**stopbits** { **1** | **1.5** | **2** }	可选 缺省情况下，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
	配置数据位	**databits** { **7** | **8** }	可选 缺省情况下，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
	配置启动终端会话的快捷键	**activation-key** *character*	可选 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** { **default** | *character* }	可选 缺省情况下，键入<Ctrl+C>中止当前运行的任务
	配置流量控制方式	**flow-control** { **hardware** | **none** | **software** }	可选 缺省情况下，流量控制方式为none 目前设备只支持配置流量控制方式为none
	配置终端的显示类型	**terminal type** { **ansi** | **vt100** }	可选 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
	设置用户登录后可以访问的命令级别	**user privilege level** *level*	可选 缺省情况下，从AUX用户界面登录后可以访问的命令级别为3级

操作		命令	说明
	设置终端屏幕一屏显示的行数	**screen-length** *screen-length*	可选 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*	可选 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
	设置用户界面的超时时间	**idle-timeout** *minutes* [*seconds*]	可选 缺省情况下，所有的用户界面的超时时间为10分钟，如果10分钟内某用户界面没有用户进行操作，则该用户界面将自动断开 **idle-timeout** 0表示关闭用户界面的超时功能

注意

- 改变 Console 口属性后会立即生效，通过 Console 口登录来配置 Console 口属性可能在配置过程中发生连接中断，建议通过其他登录方式来配置 Console 口属性。若用户需要通过 Console 口再次登录设备，需要改变 PC 机上运行的终端仿真程序的相应配置，使之与设备上配置的 Console 口属性保持一致。
- 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。

2.6 CLI登录显示和维护

表2-25 CLI 显示和维护

操作	命令	说明
显示当前正在使用的用户界面以及用户的相关信息	**display users** [**|** { **begin** | **exclude** | **include** } *regular-expression*]	在任意视图下执行
显示设备支持的所有用户界面以及用户的相关信息	**display users all** [**|** { **begin** | **exclude** | **include** } *regular-expression*]	在任意视图下执行
显示用户界面的相关信息	**display user-interface** [*num1* | { **aux** | **vty** } *num2*] [**summary**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	在任意视图下执行

操作	命令	说明
显示设备作为Telnet客户端的相关配置信息	**display telnet client configuration** [**|** { **begin** | **exclude** | **include** } *regular-expression*]	在任意视图下执行
释放指定的用户界面	**free user-interface** { *num1* | { **aux** | **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，其他在线用户的配置影响到管理员的操作，或者管理员正在进行一些重要配置不想被其他用户干扰时，可以使用以下命令强制断开该用户的连接 不能使用该命令释放用户当前自己使用的连接
锁住当前用户界面	**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界面 FIPS模式下不支持该命令。
设置在用户界面之间传递消息	**send** { **all** | *num1* | { **aux** | **vty** } *num2* }	在用户视图下执行

3 配置通过Web网管登录设备

3.1 通过Web网管登录设备简介

为了方便您对网络设备进行配置和维护，设备提供 Web 网管功能。设备提供一个内置的 Web 服务器，您可以通过 PC 登录到设备上，使用 Web 界面直观地配置和维护设备。

设备支持两种内置的 Web 登录方式：

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

如果要使用 Web 登录设备，您首先需要通过 Console 口登录到设备上，开启设备的 Web 登录功能（缺省情况下，HTTP 服务处于关闭状态、HTTPS 服务处于关闭状态），并配置设备 VLAN 接口的 IP 地址、Web 登录用户及认证密码等，配置完成后，您即可使用 Web 网管的方式登录设备。

表3-1 通过 Web 登录设备需要具备的条件

对象	需要具备的条件	
设备	配置设备的IP地址，设备与Web登录用户间路由可达	
	配置Web登录用户的属性 （HTTP和HTTPs是两种独立的登录方式，不存在配置依赖关系，请根据需要二者必选其一）	HTTP方式配置
		HTTPS方式配置
Web登录用户	运行Web浏览器	
	获取要登录设备VLAN接口的IP地址	

本节将为您介绍如何通过 Web 登录设备，并配置通过 Web 登录时的认证方式及用户级别等，实现对 Web 登录用户的控制。

3.2 配置通过HTTP方式登录设备

表3-2 配置通过 HTTP 方式登录设备

操作	命令	说明
进入系统视图	**system-view**	-

操作	命令	说明
启动HTTP服务器	**ip http enable**	必选 • 空配置启动时，使用软件功能缺省值，Web 服务处于开启状态 • 缺省配置启动时，使用软件功能出厂值，Web 服务器处于关闭状态 关于空配置启动和缺省配置启动，请参见“基础配置指导”中的“配置文件管理”
配置HTTP服务的端口号	**ip http port** *port-number*	可选 缺省情况下，HTTP服务的端口号为80 如果重复执行此命令，HTTP服务将使用最后一次配置的端口号
配置HTTP服务与ACL关联	**ip http acl** *acl-number*	可选 缺省情况下，没有ACL与HTTP服务关联 通过将HTTP服务与ACL关联，可以过滤掉来自某些客户端的请求，只允许通过ACL过滤的客户端访问设备
创建本地用户（进入本地用户视图）	**local-user** *user-name*	必选 缺省情况下，无本地用户
配置本地认证密码	**password** [**hash**] { **cipher** | **simple** } *password*]	必选 缺省情况下，无本地认证密码
配置Web登录的用户级别	**authorization-attribute level** *level*	必选 缺省情况下，没有配置Web登录的用户级别
配置Web登录用户的服务类型	**service-type web**	必选 缺省情况下，没有配置用户的服务类型
退回系统视图	**quit**	-
配置IPv4 HTTP报文发送的DSCP优先级	**ip http dscp** *dscp-value*	可选 缺省情况下，IPv4 HTTP报文发送的DSCP优先级为16
配置IPv6 HTTP报文发送的DSCP优先级	**ipv6 http dscp** *dscp-value*	可选 缺省情况下，IPv6 HTTP报文发送的DSCP优先级为0
创建VLAN接口并进入VLAN接口视图	**interface vlan-interface** *vlan-interface-id*	必选 如果该VLAN接口已经存在，则直接进入该VLAN接口视图

操作	命令	说明
配置VLAN接口的IP地址	**ip address** *ip-address* { *mask* | *mask-length* }	必选 缺省情况下，没有配置VLAN接口的IP地址

说明

当设备由 FIPS 模式重新切回到非 FIPS 模式时，HTTP 服务将变为开启，如果要关闭 HTTP 服务请使用 **undo ip http enable** 命令关闭。

3.3 配置通过HTTPS方式登录设备

说明

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

表3-3 配置通过 HTTPS 方式登录设备

操作	命令	说明
进入系统视图	**system-view**	-
配置HTTPS服务与SSL服务器端策略关联	**ip https ssl-server-policy** *policy-name*	必选 缺省情况下，没有SSL服务器端策略与HTTPS服务关联 • 关闭 HTTPS 服务后，系统将自动取消 HTTPS 服务与 SSL 服务器端策略的关联。再次使能 HTTPS 服务之前，需要重新配置 HTTPS 服务与 SSL 服务器端策略关联 • HTTPS 服务处于使能状态时，对与其关联的 SSL 服务器端策略进行的修改不会生效

操作	命令	说明
使能HTTPS服务	**ip https enable**	必选 缺省情况下，HTTPS服务处于关闭状态 使能HTTPS服务，会触发SSL的握手协商过程。在SSL握手协商过程中，如果设备的本地证书已经存在，则SSL协商可以成功，HTTPS服务可以正常启动；如果设备的本地证书不存在，则SSL协商过程会触发证书申请流程。由于证书申请需要较长的时间，会导致SSL协商不成功，从而无法正常启动HTTPS服务。因此，在这种情况下，需要多次执行**ip https enable**命令，这样HTTPS服务才能正常启动
配置HTTPS服务与证书属性访问控制策略关联	**ip https certificate access-control-policy** *policy-name*	可选 缺省情况下，没有证书属性访问控制策略与HTTPS服务关联 • 通过将 HTTPS 服务与已配置的客户端证书属性访问控制策略关联，可以实现对客户端的访问权限进行控制，进一步保证设备的安全性 • 如果配置 HTTPS 服务与证书属性访问控制策略关联，则必须同时在与 HTTPS 服务关联的 SSL 服务器端策略中配置 client-verify enable 命令，否则，客户端无法登录设备。 • 如果配置 HTTPS 服务与证书属性访问控制策略关联，则证书属性访问控制策略中必须至少包括一条 permit 规则，否则任何 HTTPS 客户端都无法登录设备。 • 证书属性访问控制策略的详细介绍请参见“安全配置指导”中的“PKI”
配置HTTPS服务的端口	**ip https port** *port-number*	可选 缺省情况下，HTTPS服务的端口号为443
配置HTTPS服务与ACL关联	**ip https acl** *acl-number*	必选 缺省情况下，没有ACL与HTTPS服务关联 通过将HTTP服务与ACL关联，可以过滤掉来自某些客户端的请求，只允许通过ACL过滤的客户端访问设备
创建本地用户（进入本地用户视图）	**local-user** *user-name*	必选 缺省情况下，无本地用户

操作	命令	说明
配置本地认证密码	非FIPS模式下： **password** [[**hash**] { **cipher** | **simple** } *password*] FIPS模式下： **password**	必选 缺省情况下，无本地认证密码
配置Web登录的用户级别	**authorization-attribute level** *level*	必选 缺省情况下，没有配置Web登录的用户级别
配置Web登录用户的服务类型	**service-type web**	必选 缺省情况下，没有配置用户的服务类型
退出至系统视图	**quit**	-
创建VLAN接口并进入VLAN接口视图	**interface vlan-interface** *vlan-interface-id*	必选 如果该VLAN接口已经存在，则直接进入该VLAN接口视图
配置VLAN接口的IP地址	**ip address** *ip-address* { *mask* | *mask-length* }	必选 缺省情况下，没有配置VLAN接口的IP地址

3.4 通过Web网管登录设备显示与维护

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

表3-4 Web 用户显示

操作	命令
显示Web用户的相关信息	**display web users** [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示HTTP的状态信息	**display ip http** [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示HTTPS的状态信息	**display ip https** [**|** { **begin** | **exclude** | **include** } *regular-expression*]

3.5 通过Web网管登录设备典型配置举例

3.5.1 使用HTTP方式登录设备典型配置举例

1. 组网需求

PC 与设备通过以太网相连，设备的 IP 地址为 192.168.0.58/24。

2. 组网图

图3-1 配置 HTTP 方式登录组网图

3. 配置步骤

(1) 配置 Device

创建 VLAN 999，用作远程登录，并将 Device 上与 PC 相连的接口 GigabitEthernet 1/0/1 加入 VLAN 999.

```
<Sysname> system-view
[Sysname] vlan 999
[Sysname-vlan999] port GigabitEthernet 1/0/1
[Sysname-vlan999] quit
```

配置 VLAN 999 接口的 IP 地址为 192.168.0.58，子网掩码为 255.255.255.0。

```
[Sysname] interface vlan-interface 999
[Sysname-VLAN-interface999] ip address 192.168.0.58 255.255.255.0
[Sysname-VLAN-interface999] quit
```

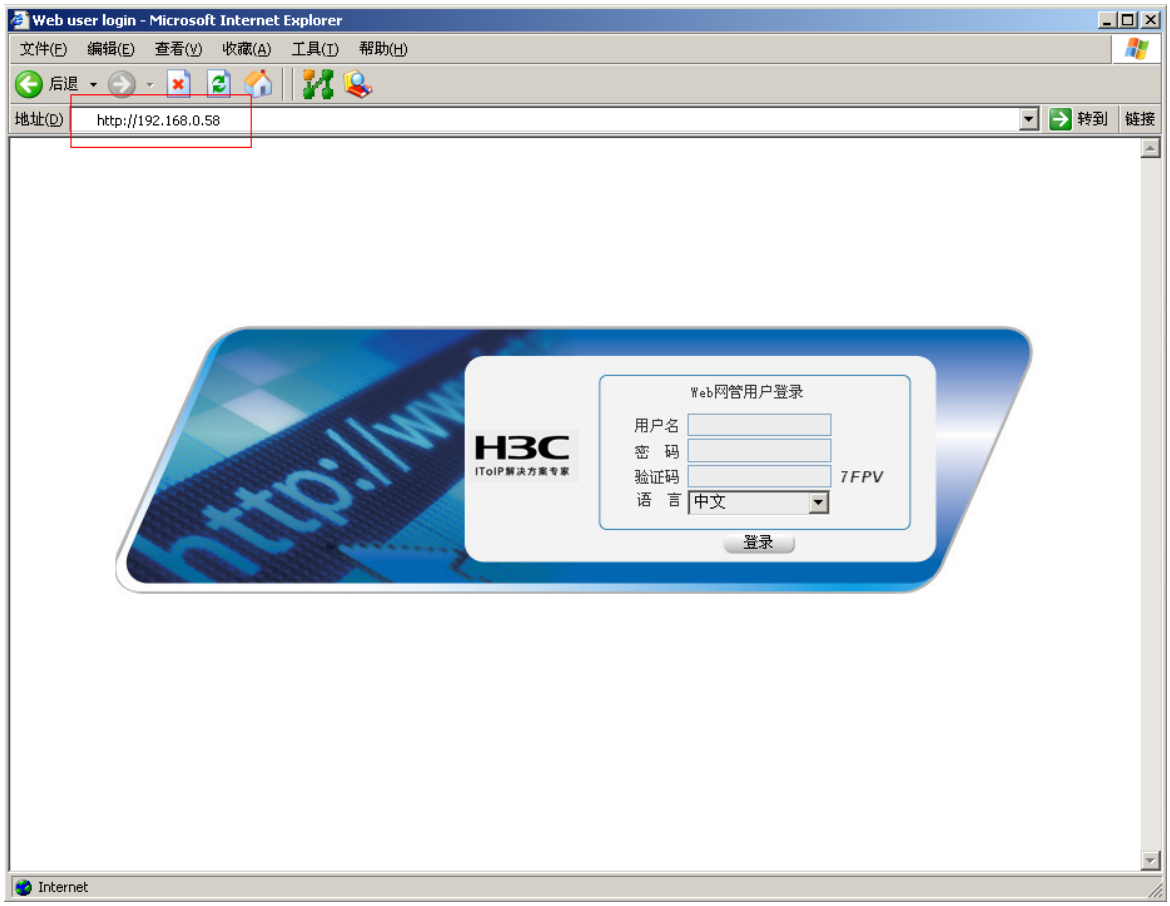
配置 Web 网管用户名为 admin，认证密码为 admin，用户级别为 3 级。

```
[Sysname] local-user admin
[Sysname-luser-admin] service-type web
[Sysname-luser-admin] authorization-attribute level 3
[Sysname-luser-admin] password simple admin
```

(2) 配置 PC

在PC的浏览器地址栏内输入设备的IP地址并回车，浏览器将显示Web网管的登录页面，如 图 3-2 所示：

图3-2 通过 Web 登录设备



在“Web 网管用户登录”对话框中输入用户名、密码及验证码，并选择登录使用的语言，点击<登录>按钮后即可登录，显示 Web 网管初始页面。成功登录后，您可以在配置区对设备进行各种配置。

3.5.2 使用HTTPS方式登录设备典型配置举例

1. 组网需求

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

为了满足上述需求，需要进行如下配置：

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

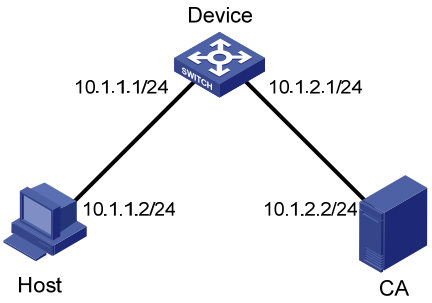
其中，负责为 Device 和 Host 颁发证书的 CA（Certificate Authority，认证颁发机构）名称为 new-ca。

说明

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

2. 组网图

图3-3 HTTPS 配置组网图



3. 配置步骤

(1) 配置 HTTPS 服务器 Device

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

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

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

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

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

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

生成本地的 RSA 密钥对。

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

获取 CA 的证书。

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

为 Device 申请证书。

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

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

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

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

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

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

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

配置 HTTPS 服务与 SSL 服务器端策略 myssl 关联。

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

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

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

使能 HTTPS 服务。

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

创建本地用户 usera，密码为 123，服务类型为 web，级别为 3（最高级别，具有该级别的用户登录后能够执行设备支持的所有操作）。

```
[Device] local-user usera
[Device-luser-usera] password simple 123
[Device-luser-usera] service-type web
[Device-luser-usera] authorization-attribute level 3
```

(2) 配置 HTTPS 客户端 Host

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

(3) 验证配置结果

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

说明

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

4 配置通过NMS登录设备

4.1 通过NMS登录设备简介

用户可通过 NMS（Network Management Station，网络管理系统）登录到设备上，通过设备上的 Agent 模块对设备进行管理、配置。设备支持多种 NMS 软件。

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，您首先需要通过 Console 口登录到设备上，在设备上进行相关配置。配置完成后，您即可使用 NMS 网管的方式登录设备。

表4-1 通过 NMS 登录设备需要具备的条件

对象	需要具备的条件
设备	配置设备VLAN接口的IP地址，设备与NMS间路由可达
	配置SNMP基本功能
NMS（网络管理系统）	NMS网络管理系统进行了正确配置，具体配置请参见NMS附带的网管手册

4.2 配置通过NMS登录设备

建立配置环境，将 NMS 通过网络与设备连接，确保 NMS 和设备之间路由可达。

图4-1 通过 NMS 方式登录组网环境

表4-2 配置 SNMP 基本参数（SNMP v3 版本）

操作	命令	说明
进入系统视图	**system-view**	-
启动SNMP Agent服务	**snmp-agent**	可选 缺省情况下，SNMP Agent服务处于关闭状态 执行此命令或执行**snmp-agent**的任何一条配置命令（不含**display**命令），都可以启动SNMP Agent

操作	命令	说明
配置SNMP组	**snmp-agent group v3** *group-name* [**authentication** | **privacy**] [**read-view** *read-view*] [**write-view** *write-view*] [**notify-view** *notify-view*] [**acl** *acl-number* | **acl ipv6** *ipv6-acl-number*] *	必选 缺省情况下，没有配置SNMP组
为SNMP组添加新用户	**snmp-agent usm-user v3** *user-name group-name* [[**cipher**] **authentication-mode** { **md5** | **sha** } *auth-password* [**privacy-mode** { **3des** | **aes128** | **des56** } *priv-password*]] [**acl** *acl-number* | **acl ipv6** *ipv6-acl-number*] *	必选 如果使用**cipher**参数，则后面的*auth-password*和*priv-password*都将被视为密文密码

表4-3 配置 SNMP 基本参数（SNMP v1 版本、SNMP v2c 版本）

操作			命令	说明
进入系统视图			**system-view**	-
启动SNMP Agent服务			**snmp-agent**	可选 缺省情况下，SNMP Agent服务处于关闭状态。 执行此命令或执行**snmp-agent**的任何一条配置命令，都可以启动SNMP Agent
创建或更新MIB视图内容			**snmp-agent mib-view** { **excluded** | **included** } *view-name oid-tree* [**mask** *mask-value*]	可选 缺省情况下，视图名为ViewDefault，OID为1
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*] *	二者必选其一 直接设置是以SNMP v1和v2c版本的团体名进行设置 间接设置采用与SNMP v3版本一致的命令形式，添加的用户到指定的组，即相当于SNMP v1和SNMP v2c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** *read-view*] [**write-view** *write-view*] [**notify-view** *notify-view*] [**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*] *	

说明

设备支持 SNMP v1、SNMP v2c 和 SNMP v3 三种版本，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”。

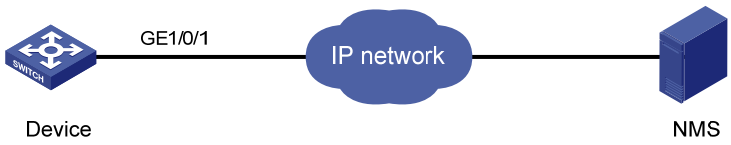
4.3 通过NMS登录设备典型配置举例

1. 组网需求

使用 SNMPv3 版本通过 NMS 对设备进行自动管理。

2. 组网图

通过 NMS 登录设备典型配置组网图



3. 配置步骤

(1) 配置 Device

配置设备的 IP 地址，并确保设备与 NMS 之间路由可达。（配置步骤略）

进入系统视图。

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

启动 SNMP Agent 服务。

```
[Sysname] snmp-agent
```

配置 SNMP 组。

```
[Sysname] snmp-agent group v3 managev3group
```

为 SNMP 组添加新用户

```
[Sysname] snmp-agent usm-user v3 managev3user managev3group
```

(2) 配置 NMS

用户可利用网管系统完成对设备的查询和配置操作，具体情况请参考 NMS 的配套手册。

说明

NMS 侧的版本、用户名配置必须和设备侧保持一致，否则无法进行相应操作。

5 对登录用户的控制

5.1 对登录用户的控制简介

设备提供对不同登录方式进行控制，如 表 5-1 所示。

表5-1 对登录用户的控制

登录方式	控制方式	实现方法	相关小节
Telnet	通过源IP对Telnet进行控制	通过基本ACL实现	5.2.2
	通过源IP、目的IP对Telnet进行控制	通过高级ACL实现	5.2.3
	通过源MAC对Telnet进行控制	通过二层ACL实现	5.2.4
NMS	通过源IP对网管用户进行控制	通过基本ACL实现	5.3.2
Web	通过源IP对Web用户进行控制	通过基本ACL实现	5.4.2

5.2 配置对Telnet用户的控制

5.2.1 配置准备

确定了对 Telnet 的控制策略，包括对哪些源 IP、目的 IP、源 MAC 进行控制，控制的动作是允许访问还是拒绝访问。

5.2.2 通过源IP对Telnet进行控制

本配置需要通过基本访问控制列表实现。基本访问控制列表的序号取值范围为 2000～2999。关于 ACL 的定义请参见“ACL 和 QoS 配置指导”中的“ACL”。

表5-2 通过源 IP 对 Telnet 进行控制

操作	命令	说明
进入系统视图	**system-view**	-
创建或进入基本ACL视图	**acl** [**ipv6**] **number** *acl-number* [**match-order** { **config** | **auto** }]	必选 缺省情况下，匹配顺序为**config**
定义子规则	**rule** [*rule-id*] { **permit** | **deny** } [**source** { *sour-addr sour-wildcard* | **any** } | **time-range** *time-name* | **fragment** | **logging**]*	必选 缺省情况下，没有定义子规则
退出ACL视图	**quit**	-
进入用户界面视图	**user-interface** [*type*] *first-number* [*last-number*]	-

操作	命令	说明
引用访问控制列表，通过源IP对Telnet进行控制	**acl** [**ipv6**] *acl-number* { **inbound** | **outbound** }	必选 **inbound**：对Telnet到本设备的用户进行ACL控制 **outbound**：对从本设备Telnet到其他Telnet服务器的用户进行ACL控制

5.2.3 通过源IP、目的IP对Telnet进行控制

本配置需要通过高级访问控制列表实现。高级访问控制列表的序号取值范围为 3000～3999。关于 ACL 的定义请参见“ACL 和 QoS 配置指导”中的“ACL”。

表5-3 配置高级 ACL 规则

操作	命令	说明
进入系统视图	**system-view**	-
创建或进入高级ACL视图	**acl** [**ipv6**] **number** *acl-number* [**match-order** { **config** | **auto** }]	必选 缺省情况下，匹配顺序为config
定义子规则	**rule** [*rule-id*] { **permit** | **deny** } *rule-string*	必选 用户可以根据需要配置对相应的源IP、目的IP进行过滤的规则
退出ACL视图	**quit**	-
进入用户界面视图	**user-interface** [*type*] *first-number* [*last-number*]	-
引用访问控制列表，通过源IP、目的IP对Telnet进行控制	**acl** [**ipv6**] *acl-number* { **inbound** | **outbound** }	必选 inbound：对Telnet到本设备的用户进行ACL控制 outbound：对从本设备Telnet到其他Telnet服务器的用户进行ACL控制

5.2.4 通过源MAC地址对Telnet进行控制

本配置需要通过二层访问控制列表实现。二层访问控制列表的序号取值范围为 4000～4999。关于 ACL 的定义请参见“ACL 和 QoS 配置指导”中的“ACL”。

表5-4 配置二层 ACL 规则

操作	命令	说明
进入系统视图	**system-view**	-
创建或进入二层ACL视图	**acl number** *acl-number* [**match-order** { **config** | **auto** }]	必选 缺省情况下，匹配顺序为**config**

操作	命令	说明
定义子规则	**rule** [*rule-id*] { **permit** | **deny** } *rule-string*	必选 用户可以根据需要配置对相应的源MAC进行过滤的规则
退出ACL视图	**quit**	-
进入用户界面视图	**user-interface** [*type*] *first-number* [*last-number*]	-
引用访问控制列表，通过源MAC对Telnet进行控制	**acl** *acl-number* **inbound**	必选 inbound：对Telnet到本设备的用户进行ACL控制

说明

二层访问控制列表对于 Telnet Client 的源 IP 与 Telnet 服务器的接口 IP 不在同一网段的不生效。

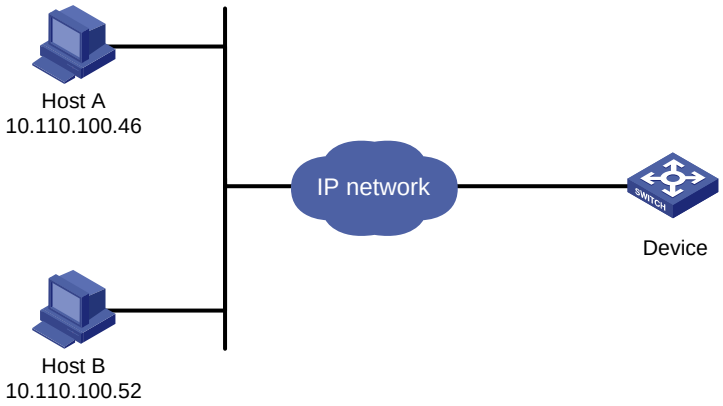
5.2.5 配置举例

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 对 Device 的 Telnet 用户进行 ACL 控制



3. 配置步骤

定义基本访问控制列表。

```
<Sysname> system-view
[Sysname] acl 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
```

引用访问控制列表，允许源地址为 10.110.100.52 和 10.110.100.46 的 Telnet 用户访问设备。

```
[Sysname] user-interface vty 0 15
[Sysname-ui-vty0-15] acl 2000 inbound
```

5.3 通过源IP对网管用户进行控制

设备支持通过网管软件进行远程管理。网管用户可以通过 SNMP 访问设备。通过引用访问控制列表，可以对访问设备的 SNMP 用户进行控制。

5.3.1 配置准备

确定了对网管用户的控制策略，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。

5.3.2 通过源IP对网管用户进行控制

本配置需要通过基本访问控制列表实现。基本访问控制列表的序号取值范围为 2000～2999。关于 ACL 的定义请参见“ACL 和 QoS 配置指导”中的“ACL”。

表5-5 通过源 IP 对网管用户进行控制

操作	命令	说明
进入系统视图	**system-view**	-
创建或进入基本ACL视图	**acl** [**ipv6**] **number** *acl-number*[**name** *name*] [**match-order** { **config** | **auto** }]	必选 缺省情况下，匹配顺序为config
定义子规则	**rule** [*rule-id*] { **permit** | **deny** } [**source** { *sour-addr sour-wildcard* | **any** } | **time-range** *time-name* | **fragment** | **logging**]*	必选
退出ACL视图	**quit**	-
在配置SNMP团体名的命令中引用访问控制列表	**snmp-agent community** { **read** | **write** } *community-name* [**mib-view** *view-name*] [**acl** *acl-number* | **acl ipv6** *ipv6-acl-number*] *	必选 根据网管用户运行的SNMP版本及配置习惯，可以在团体名、组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SNMP组名的命令中引用访问控制列表	**snmp-agent group** { **v1** | **v2c** } *group-name* [**read-view** *read-view*] [**write-view** *write-view*] [**notify-view** *notify-view*] [**acl** *acl-number* | **acl ipv6** *ipv6-acl-number*] * **snmp-agent group v3** *group-name* [**authentication** | **privacy**] [**read-view** *read-view*] [**write-view** *write-view*] [**notify-view** *notify-view*] [**acl** *acl-number* | **acl ipv6** *ipv6-acl-number*] *	
在配置SNMP用户名的命令中引用访问控制列表	**snmp-agent usm-user** { **v1** | **v2c** } *user-name group-name* [**acl** *acl-number* | **acl ipv6** *ipv6-acl-number*] * **snmp-agent usm-user v3** *user-name group-name* [[**cipher**] **authentication-mode** { **md5** | **sha** } *auth-password* [**privacy-mode** { **3des** | **aes128** | **des56** } *priv-password*]] [**acl** *acl-number* | **acl ipv6** *ipv6-acl-number*] *	

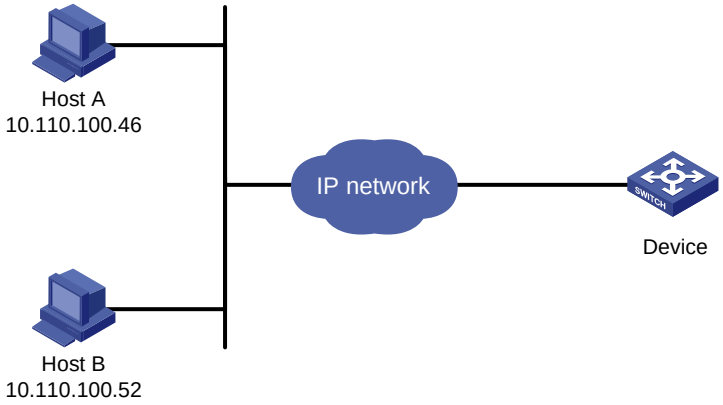
5.3.3 配置举例

1. 组网需求

通过源 IP 对网管用户进行控制，仅允许来自 10.110.100.52 和 10.110.100.46 的 NMS 用户访问设备。

2. 组网图

图5-2 对 NMS 用户进行 ACL 控制



3. 配置步骤

定义基本访问控制列表。

```
<Sysname> system-view
[Sysname] acl 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
```

引用访问控制列表，仅允许来自 10.110.100.52 和 10.110.100.46 的 SNMP 用户访问设备。

```
[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
```

5.4 通过源IP对Web用户进行控制

设备支持通过 Web 方式进行远程管理。Web 用户可以通过 HTTP 协议访问设备。通过引用访问控制列表，可以对访问设备的 Web 用户进行控制。

5.4.1 配置准备

确定了对 Web 用户的控制策略，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。

5.4.2 通过源IP对Web用户进行控制

本配置需要通过基本访问控制列表实现。基本访问控制列表的序号取值范围为 2000～2999。关于 ACL 的定义请参见“ACL 和 QoS 配置指导”中的“ACL”。

表5-6 通过源 IP 对 Web 用户进行控制

操作	命令	说明
进入系统视图	**system-view**	-
创建或进入基本ACL视图	**acl** [**ipv6**] **number** *acl-number* [**match-order** { **config** | **auto** }]	必选 缺省情况下，匹配顺序为**config**
定义子规则	**rule** [*rule-id*] { **permit** | **deny** } [**source** { *sour-addr sour-wildcard* | **any** } | **time-range** *time-name* | **fragment** | **logging**]*	必选
退出ACL视图	**quit**	-
引用访问控制列表对Web用户进行控制	**ip http acl** *acl-number*	HTTP和HTTPs是两种独立的登录方式，不存在配置依赖关系，请根据需要二者必选其一
	ip https acl *acl-number*	

5.4.3 强制在线Web用户下线

网络管理员可以通过命令行强制在线 Web 用户下线。

表5-7 强制在线 Web 用户下线

操作	命令	说明
强制在线Web用户下线	**free web-users** { **all** | **user-id** *user-id* | **user-name** *user-name* }	必选 在用户视图下执行

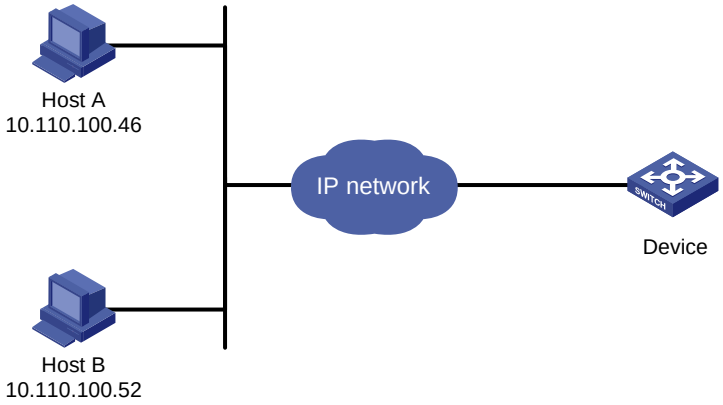
5.4.4 配置举例

1. 组网需求

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

2. 组网图

图5-3 对 Device 的 HTTP 用户进行 ACL 控制



3. 配置步骤

定义基本访问控制列表。

```
<Sysname> system-view
[Sysname] acl number 2030 match-order config
[Sysname-acl-basic-2030] rule 1 permit source 10.110.100.52 0
```

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

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

目 录

1 FTP

说明

FIPS 模式下不支持 FTP。

1.1 FTP简介

1.1.1 FTP概述

FTP（File Transfer Protocol，文件传输协议）用于在远端服务器和本地主机之间传输文件，是 IP 网络上传输文件的通用协议。在万维网（WWW，World Wide Web）出现以前，用户使用命令行方式传输文件，最通用的应用程序就是 FTP。虽然目前大多数用户在通常情况下选择使用 Email 和 Web 传输文件，但是 FTP 仍然有着比较广泛的应用。

FTP 协议在 TCP/IP 协议族中属于应用层协议，用于在远端服务器和本地客户端之间传输文件，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 RFC959 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.bin 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）。

FTP 有两种工作方式：

- 主动方式（PORT），数据连接由 FTP 服务器发起，当 FTP 客户端处于防火墙后时不适用；
- 被动方式（PASV），数据连接由 FTP 客户端程序发起，当 FTP 服务器限制客户端连接其高位端口（一般情况下大于 1024）时不适用。

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

1.1.2 FTP的实现

设备在支持 FTP 协议上有两种方式：

- 设备作为FTP客户端：如 图 1-1 所示，设备（Device）作为FTP客户端，PC作为FTP服务器。在Device上执行**ftp**命令，与PC建立FTP连接，完成文件的上传/下载操作。
- 设备作为FTP服务器：如 图 1-1 所示，设备（Device）作为FTP服务器，PC作为FTP客户端。在PC上运行FTP客户端程序，与Device建立FTP连接，完成文件的上传/下载操作。

图1-1 FTP 配置示意图

设备作为 FTP 客户端时，需要进行如下配置：

表1-1 设备作为 FTP 客户端时的配置

设备	操作	说明
Device（作为FTP客户端）	可以直接使用**ftp**命令登录远端的FTP服务器	如果远端FTP服务器支持匿名访问，设备可以直接登录；如果远端FTP服务器不支持匿名访问，则必须先获取FTP用户名和密码后，才能成功登录远端的FTP服务器
PC（作为FTP服务器）	启动FTP服务器，并做了用户名、密码、用户的权限等相关的配置	-

设备作为 FTP 服务器时，需要进行如下配置：

表1-2 设备作为 FTP 服务器时的配置

设备	操作	说明
Device（作为FTP服务器）	启动FTP服务器功能	缺省情况下，系统关闭FTP服务器功能 可以通过**display ftp-server**命令查看设备上FTP服务器功能的配置信息
	配置FTP服务器的验证和授权	配置FTP用户的用户名、密码、授权的工作目录。出于安全考虑，设备不支持匿名登录，用户必须使用合法的用户名和密码。缺省情况下，合法用户可访问的目录为设备的根目录
	配置FTP服务器的运行参数	配置FTP连接的超时时间等参数
PC（作为FTP客户端）	使用FTP客户端程序登录设备	用户必须获取FTP用户名和密码后，才能成功登录远端的FTP服务器

注意

- 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。
- 当设备作为 FTP 服务器，使用 Internet Explorer 浏览器登录设备时，因为 Internet Explorer 浏览器在登录过程中建立了多个用户连接，而目前设备某一时刻只支持一个用户连接，所以使用 Internet Explorer 浏览器登录设备时 FTP 的部分功能不支持。

1.2 配置FTP客户端

说明

只有级别为 3（管理级）的用户才能使用 **ftp** 命令登录 FTP 服务器，进入 FTP 客户端视图，执行目录、文件等命令，但命令能否执行成功，还将受 FTP 服务器端的授权限制。

1.2.1 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。源地址可以通过配置源接口（建议使用 Loopback 接口）或源 IP 地址来实现，源接口下配置的主 IP 地址或源 IP 地址即为发送报文的源地址。

FTP 客户端在与 FTP 服务器通信的时候，发送报文的源地址选取遵循以下规则：

- 如果没有指定 FTP 客户端的源地址，则采用路由决定的源地址进行通信。
- 如果只用 **ftp client source** 或 **ftp** 命令指定了源地址，则采用该地址进行通信。
- 如果执行 **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。
- **ftp client source** 命令指定的源地址对所有的 FTP 连接有效，**ftp** 命令指定的源地址只对当前的 FTP 连接有效。

表1-3 建立 FTP 连接（IPv4 组网环境）

操作	命令	说明
进入系统视图	**system-view**	-
配置FTP客户端的源地址	**ftp client source** { **interface** *interface-type interface-number* | **ip** *source-ip-address* }	可选 缺省情况下，设备使用路由决定的源地址与FTP服务器通信
退回用户视图	**quit**	-
在用户视图下直接登录远程FTP服务器	**ftp** [*server-address* [*service-port*]] [**vpn-instance** *vpn-instance-name*] [**source** { **interface** *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远程FTP服务器	**ftp**	
	open *server-address* [*service-port*]	

说明

- 如果源接口下没有配置主地址，将导致 FTP 连接建立失败。
- 如果先后使用 **ftp client source** 命令配置了客户端 FTP 报文的源接口和源 IP，则新配置的源 IP 将覆盖现有的源接口配置。反之亦然。

表1-4 建立 FTP 连接（IPv6 组网环境）

操作	命令	说明
在用户视图下直接登录远程FTP服务器	**ftp ipv6** [*server-address* [*service-port*]] [**vpn-instance** *vpn-instance-name*] [**source 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 ipv6**命令在FTP客户端视图下执行
在FTP客户端视图下间接登录远程FTP服务器	**ftp ipv6**	
	open ipv6 *server-address* [*service-port*] [**-i** *interface-type interface-number*]	

1.2.2 配置FTP报文的DSCP优先级

用户可以对 FTP 报文的 DSCP 优先级进行配置。

表1-5 配置 FTP 和 TFTP 报文的 DSCP 优先级

操作	命令	说明
进入系统视图	**system-view**	-
配置IPv4 FTP客户端发送报文的DSCP优先级	**ftp client dscp** *dscp-value*	可选 缺省情况下，IPv4 FTP客户端发送报文的DSCP优先级为0
配置IPv6 FTP客户端发送报文的DSCP优先级	**ftp client ipv6 dscp** *dscp-value*	可选 缺省情况下，IPv6 FTP客户端发送报文的DSCP优先级为0

1.2.3 操作FTP服务器上的目录

当设备作为FTP客户端，与FTP服务器连接建立成功后（连接操作请参见 1.2.1 建立FTP连接），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
查看远程FTP服务器上的目录/文件的详细信息	**dir** [*remotefile* [*localfile*]]	可选
查询远程FTP服务器上的目录/文件	**ls** [*remotefile* [*localfile*]]	可选

操作	命令	说明
切换远程FTP服务器上的工作路径	**cd** { *directory* | **..** | */* }	可选
退出远程FTP服务器的当前目录，返回FTP服务器的上一级目录	**cdup**	可选
显示当前用户正在访问的远程FTP服务器上的路径	**pwd**	可选
在远程FTP服务器上创建目录	**mkdir** *directory*	可选
删除FTP服务器上指定的目录	**rmdir** *directory*	可选

1.2.4 操作FTP服务器上的文件

当设备作为FTP客户端，与FTP服务器连接建立成功后（连接操作请参见 1.2.1 建立FTP连接），在FTP服务器的授权目录下，用户可以通过以下操作，给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** 命令了解用户登录 FTP 服务器前在 FTP 客户端上的工作路径。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) 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
查看远程FTP服务器上的目录/文件的详细信息	**dir** [*remotefile* [*localfile*]]	可选 **ls**命令只能显示出目录/文件的名称，而**dir**命令可以查看与目录/文件相关的信息，如大小，创建日期等
查询远程FTP服务器上的目录/文件	**ls** [*remotefile* [*localfile*]]	可选 **ls**命令只能显示出目录/文件的名称，而**dir**命令可以查看与目录/文件相关的信息，如大小，创建日期等
彻底删除远程FTP服务器上的指定文件	**delete** *remotefile*	可选
设置FTP文件传输的模式为ASCII模式	**ascii**	可选 缺省情况下，文件传输模式为ASCII模式

操作	命令	说明
设置FTP文件传输的模式为二进制模式	**binary**	可选 缺省情况下，文件传输模式为ASCII模式
设置数据传输的方式为被动方式	**passive**	可选 缺省情况下，数据传输的方式为被动方式
获取FTP客户端本地的工作路径	**lcd**	可选
上传本地文件到远程FTP服务器	**put** *localfile* [*remotefile*]	可选
下载FTP服务器上的文件	**get** *remotefile* [*localfile*]	可选

1.2.5 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（连接操作请参见 1.2.1 建立FTP连接），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设备。

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*]	可选

1.2.6 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（连接操作请参见 1.2.1 建立FTP连接），通过以下命令，可以帮助定位和诊断FTP连接过程中出现的问题。

表1-9 FTP 客户端维护与调试

操作	命令	说明
显示远程FTP服务器支持的FTP相关协议命令的帮助信息	**remotehelp** [*protocol-command*]	可选
使能显示FTP服务器返回的详细信息	**verbose**	可选 缺省情况下，verbose开关为开启状态
当设备作为FTP客户端时，打开FTP调试信息开关	**debugging**	可选 缺省情况下，FTP客户端调试信息开关处于关闭状态

1.2.7 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（连接操作请参见 1.2.1 建立FTP连接），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**	可选 等效于**close**命令
不退出FTP客户端视图的前提下，断开与FTP服务器的连接	**close**	可选 等效于**disconnect**命令
断开与远程FTP服务器的连接，并退回到用户视图	**bye**	可选 在FTP客户端视图下执行，等效于**quit**命令
断开与远程FTP服务器的连接，并退回到用户视图	**quit**	可选 在FTP客户端视图下执行，等效于**bye**命令

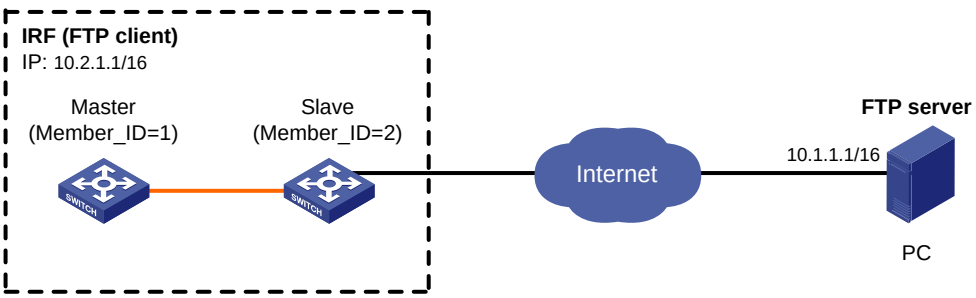
1.2.8 FTP客户端配置举例

1. 组网需求

- Master 和 Slave 两台成员设备组成 IRF。Master 的成员编号为 1，Slave 的成员编号为 2。
- IRF 作为 FTP 客户端，PC 作为 FTP 服务器。IP 地址如组网图所示，IRF 和 PC 之间路由可达。
- IRF 从 PC 上下载新的启动文件完成设备的升级，并将配置文件上传到 PC 进行备份。
- PC 上已设置设备登录 FTP 服务器的用户名为 abc，密码为 abc。设备以用户名 abc、密码 abc 登录 FTP 服务器。

2. 组网图

图1-2 利用 FTP 客户端功能实现平滑升级



说明：橙色的线表示IRF连接

3. 配置步骤

注意

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。

以 FTP 方式登录服务器。

```
<Sysname> ftp 10.1.1.1
Trying 10.1.1.1 ...
Connected to 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
```

将传输模式设置为 binary，以便传输启动文件。

```
[ftp] binary
200 Type set to I.
```

将启动文件 newest.bin 从 PC 下载到设备。

- 将启动文件 newest.bin 从 PC 下载到 Master 存储介质的根目录下。

```
[ftp] get newest.bin
```

- 将启动文件 newest.bin 从 PC 下载到 Slave（成员编号为 2）存储介质的根目录下。

```
[ftp] get newest.bin slot2#flash:/newest.bin
```

将本机的配置文件 config.cfg 上传到服务器进行备份。

```
[ftp] ascii
[ftp] put config.cfg back-config.cfg
227 Entering Passive Mode (10,1,1,1,4,2).
125 ASCII mode data connection already open, transfer starting for /config.cfg.
226 Transfer complete.
FTP: 3494 byte(s) sent in 5.646 second(s), 618.00 byte(s)/sec.
[ftp] bye
```

将 newest.bin 指定为所有成员设备的主用下次启动文件。

```
<Sysname> boot-loader file newest.bin slot all main
  This command will set the boot file of the specified board. Continue? [Y/N]:y
  The specified file will be used as the main boot file at the next reboot on slot 1!
  The specified file will be used as the main boot file at the next reboot on slot 2!
```

重启设备，完成设备软件升级。

```
<Sysname> reboot
```

注意

下次启动文件必须存放在存储介质的根目录下。可使用文件的拷贝或移动操作来调整文件的路径为根目录。关于 **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”。

1.3 配置FTP服务器

当设备作为 FTP 服务器时，可以进行如下配置。

1.3.1 FTP服务器的基本配置

用户登录到 FTP 服务器，使用 **put** 命令上传文件的过程中，FTP 服务器中文件的更新有两种方式，快速更新方式与普通更新方式。

- 快速更新方式，即 FTP 服务器先将上传文件接收到内存中，全部接收完后，再将文件内容写入存储设备。采用这种方式，即使文件传送过程发生断电等异常情况，也不会损坏 FTP 服务器上的现有文件。
- 普通更新方式，即 FTP 服务器一边接收用户的文件，一边将其写入存储设备。采用这种方式，可能会因为断电等异常情况致使 FTP 服务器上的现有文件被损坏。与快速更新方式相比，普通更新方式需要的空闲内存较少。

表1-11 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**	必选 缺省情况下，FTP服务器功能处于关闭状态
配置IPv4 FTP服务器发送报文的DSCP优先级	**ftp server dscp** *dscp-value*	可选 缺省情况下，IPv4 FTP服务器发送报文的DSCP优先级为0
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*	可选 缺省情况下，没有使用ACL限制FTP客户端
配置FTP服务器的连接空闲时间	**ftp timeout** *minutes*	可选 缺省情况下，连接空闲时间为30分钟 如果在连接空闲时间内，FTP服务器和客户端没有消息交互，则断开它们之间的连接
设置在上传过程中，FTP服务器更新文件的方式	**ftp update** { **fast** | **normal** }	可选 缺省情况下，在给FTP服务器上传文件的过程中，FTP服务器采用**normal**方式更新文件
退回到用户视图	**quit**	-
强制释放通过指定用户名建立的FTP连接	**free ftp user** *username*	可选

1.3.2 配置FTP服务器的验证和授权

FTP 服务器的授权信息包含提供给 FTP 用户的工作目录的路径。只有验证通过和授权成功的用户，才能得到 FTP 服务器的服务。

以下配置为 FTP 服务器在本地对 FTP 客户端身份进行验证的时候的步骤，如果要对 FTP 客户端进行远程认证，则不需要配置本地用户，但需要配置 AAA（Authentication, Authorization and Accounting，认证、授权和计费）认证方案，详细配置请参见“安全配置指导”中的“AAA”。（本地认证是指在设备上验证用户输入的用户名/密码是否与设备上配置的用户名/密码匹配；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，由服务器来验证用户名/密码是否匹配）

表1-12 配置 FTP 服务器的验证和授权

操作	命令	说明
进入系统视图	**system-view**	-
进入本地用户视图	**local-user** *user-name*	必选 如果指定的本地用户不存在，则先完成本地用户的创建，再进入该用户的视图 缺省情况下，系统中没有任何授权FTP服务的本地用户，系统不支持FTP匿名用户访问
设置当前本地用户的密码	**password** [[**hash**] **cipher** | **simple** } *password*]	必选
设置用户可以使用的服务类型为FTP	**service-type ftp**	必选 缺省情况下，系统不支持FTP匿名用户访问，不对用户授权任何服务；若授权FTP服务，缺省授权使用设备的根目录
配置用户的属性	**authorization-attribute** { **acl** *acl-number* | **callback-number** *callback-number* | **idle-cut** *minute* | **level** *level* | **user-profile** *profile-name* | **user-role** { **guest** | **guest-manager** | **security-audit** } | **vlan** *vlan-id* | **work-directory** *directory-name* } *	可选 缺省情况下，FTP用户可以访问设备的根目录，用户的级别为0。可以使用该命令进行修改

说明

- **local-user**、**password**、**service-type ftp** 和 **authorization-attribute** 命令的详细介绍，请参见“安全命令参考”中的“AAA”。
- 设备作为 FTP 服务器时，对客户端的访问操作有级别限制：如果要对设备的文件系统执行写操作（比如上传、删除、创建/删除文件夹），则必须将 FTP 登录用户的级别设置为 3；如果执行其它操作（比如普通的查看操作），则 FTP 登录用户的级别不受限制，可以为 0～3 中的任意级别。

1.3.3 配置FTP服务与SSL服务器端策略关联

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

说明

- 仅 Release 5206 及以上版本支持此特性。
- 配置此特性前，请先创建 SSL 服务器端策略，并关闭 FTP 服务器功能。

表1-13 配置 FTP 服务与 SSL 服务器端策略关联

操作	命令	说明
进入系统视图	**system-view**	-
配置FTP服务与SSL服务器端策略关联	**ftp server ssl-server-policy** *policy-name*	可选 缺省情况下，没有配置FTP服务与SSL服务器端策略关联

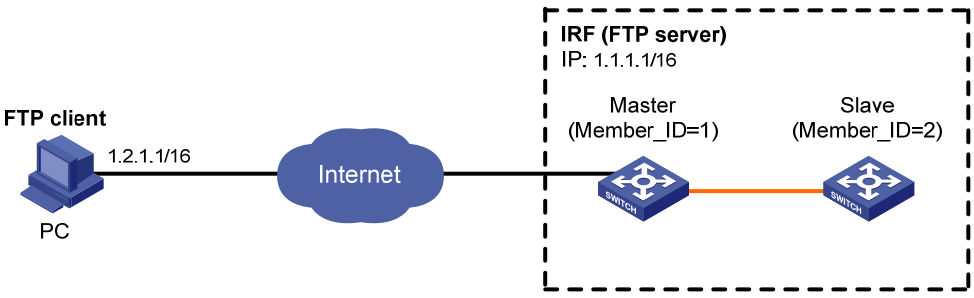
1.3.4 FTP服务器配置举例

1. 组网需求

- Master 和 Slave 两台成员设备组成 IRF。Master 的成员编号为 1，Slave 的成员编号为 2。
- IRF 作为 FTP 服务器，PC 作为 FTP 客户端。IP 地址如组网图所示，IRF 和 PC 之间路由可达。
- IRF 最新版本的启动文件存储在 PC 上，请使用 FTP 功能实现 IRF 的升级以及 IRF 配置文件的备份。
- 客户端登录 FTP 服务器的用户名为 abc，密码为 abc。

2. 组网图

图1-3 利用 FTP 服务器功能实现升级



说明：橙色的线表示IRF连接

3. 配置步骤

注意

如果 Master 和 Slave 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。

(1) IRF（FTP Server）上的配置

在 IRF 上添加一个本地用户 abc，并设置其认证密码为 abc，用户级别为 3 管理级，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
[Sysname-luser-abc] password simple abc
[Sysname-luser-abc] authorization-attribute level 3
[Sysname-luser-abc] authorization-attribute work-directory flash:/
```

如果要直接访问 Slave（成员编号为 2） Flash 的根目录，需要将“authorization-attribute work-directory flash:/”配置中的“flash:/”替换成“slot2#flash:/”。

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

启动 IRF 的 FTP 服务。

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

(2) PC（FTP Client）的配置

以 FTP 方式登录 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 IRF 的配置文件 config.cfg 下载到 PC 本地进行备份。

```
ftp> get config.cfg back-config.cfg
```

上传启动文件 newest.bin 到 Master 存储介质的根目录下。

```
ftp> put newest.bin
200 Port command okay.
150 Opening ASCII mode data connection for /newest.bin.
226 Transfer complete.
ftp> bye
221 Server closing.

c:\>
```

说明

- 利用 FTP 功能升级配置文件时，操作步骤与上述介绍基本相同，需要注意的是获取后的配置文件同样要放在存储介质的根目录下。
- 利用 FTP 远程升级 Bootrom 程序，文件传送完成后需要再执行 **bootrom update** 命令来升级 Bootrom。

(3) 升级 IRF

将启动文件 newest.bin 拷贝到 Slave（成员编号为 2）存储介质的根目录下。

```
<Sysname> copy newest.bin slot2#flash:/
```

将 newest.bin 指定为所有成员设备的主用下次启动文件。

```
<Sysname> boot-loader file newest.bin slot all main
  This command will set the boot file of the specified board. Continue? [Y/N]:y
  The specified file will be used as the main boot file at the next reboot on slot 1!
  The specified file will be used as the main boot file at the next reboot on slot 2!
```

重启设备，完成 IRF 软件升级。

```
<Sysname> reboot
```

注意

下次启动文件必须存放在存储介质的根目录下。可使用文件的拷贝或移动操作来调整文件的路径为根目录。关于 **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”。

1.4 FTP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 FTP 的运行情况，通过查看显示信息验证配置的效果。

表1-14 FTP 显示和维护

操作	命令
查看FTP客户端的当前配置	**display ftp client configuration** [**|** { **begin** | **exclude** | **include** } *regular-expression*]
查看FTP服务器的配置情况	**display ftp-server** [**|** { **begin** | **exclude** | **include** } *regular-expression*]
查看FTP登录用户的详细情况	**display ftp-user** [**|** { **begin** | **exclude** | **include** } *regular-expression*]

2 TFTP

说明

FIPS 模式下不支持 TFTP。

2.1 TFTP简介

2.1.1 TFTP概述

TFTP（Trivial File Transfer Protocol，简单文件传输协议）也是用于在远端服务器和本地主机之间传输文件的，相对于 FTP，TFTP 没有复杂的交互存取接口和认证控制，适用于客户端和服务器之间不需要复杂交互的环境。TFTP 协议的运行基于 UDP 协议，使用 UDP 端口建立连接、收/发数据报文。TFTP 协议基本操作在 RFC1350 中进行了描述。

TFTP 协议传输是由客户端发起的：

- 当 TFTP 客户端需要从服务器下载文件时，由客户端向 TFTP 服务器发送读请求包，然后从服务器接收数据，并向服务器发送确认；
- 当 TFTP 客户端需要向服务器上传文件时，由客户端向 TFTP 服务器发送写请求包，然后向服务器发送数据，并接收服务器的确认。

TFTP 传输文件有两种模式：

- 二进制模式，用于传输程序文件（比如后缀名.bin 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）。

2.1.2 TFTP的实现

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 配置示意图

使用 TFTP 之前，网络管理员需要配置好 TFTP 客户端和服务器的 IP 地址，并且确保客户端和服务器之间的路由可达。

设备作为 TFTP 客户端时，需要进行如下配置：

表2-1 设备作为 TFTP 客户端时的配置

设备	操作	说明
Device（作为TFTP客户端）	• 进行 IP 地址和路由功能配置，确保设备和 TFTP 服务器之间路由可达 • 直接使用 TFTP 命令登录远端的 TFTP 服务器上传或者下载文件	-
PC（作为TFTP服务器）	启动TFTP服务器，并配置TFTP工作目录	-

2.2 配置TFTP客户端

当设备作为 TFTP 客户端时，可以把本设备的文件上传到 TFTP 服务器，还可以从 TFTP 服务器下载文件到本地设备。下载又分为两种：

- 普通下载。在这种方式下，设备将获取的远端文件直接写到存储设备中。如果下载时将远端文件保存在设备上使用的文件名是 *destination-filename*，而设备已经存在同名文件，则在下载时，系统会先将设备上已有的 *destination-filename* 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。
- 安全下载。在这种方式下，设备将获取的远端文件先保存到内存中，等用户文件全部接收完毕，才将它写到存储设备中。如果下载时将远端文件保存在设备上使用的文件名是 *destination-filename*，设备已经存在同名文件，此时，即便下载失败（如网络断开等原因），因为原文件没有被覆盖，仍能使用。这种方法安全系数较高，但需要较大的内存空间。

当操作启动文件或配置文件等重要文件时，建议采用安全下载或者非覆盖性下载（即下载时使用一个当前目录下不存在的文件名作为目标文件名）。

在使用 **tftp** 命令建立 TFTP 连接时，还可以进行源地址绑定。源地址可以通过配置源接口（建议使用 Loopback 接口）或源 IP 地址来实现，源接口下配置的主 IP 地址或源 IP 地址即为发送报文的源地址。

TFTP 客户端在与 TFTP 服务器通信的时候，发送报文的源地址选取遵循以下规则：

- 如果没有指定 TFTP 客户端的源地址，则采用路由决定的源地址进行通信。
- 如果只用 **tftp client source** 或 **tftp** 命令指定了源地址，则采用该地址进行通信。
- 如果执行 **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。
- **tftp client source** 命令指定的源地址对所有的 **tftp** 传输有效，**tftp** 命令指定的源地址只对当前的 **tftp** 传输有效。

表2-2 配置 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** [**ipv6**] **acl** *acl-number*	可选 缺省情况下，没有使用ACL限制TFTP服务器

操作	命令	说明
配置TFTP客户端的源地址	**tftp client source** { **interface** *interface-type interface-number* | **ip** *source-ip-address* }	可选 缺省情况下，设备使用路由决定的源地址与TFTP服务器通信
配置IPv4 TFTP客户端发送报文的DSCP优先级	**tftp client dscp** *dscp-value*	可选 缺省情况下，IPv4 TFTP客户端发送报文的DSCP优先级为0
配置IPv6 TFTP客户端发送报文的DSCP优先级	**tftp client ipv6 dscp** *dscp-value*	可选 缺省情况下，IPv6 TFTP客户端发送报文的DSCP优先级为0
退回用户视图	**quit**	-
在IPv4网络，用TFTP下载/上传/安全下载文件	**tftp** *server-address* { **get** | **put** | **sget** } *source-filename* [*destination-filename*] [**vpn-instance** *vpn-instance-name*] [**source** { **interface** *interface-type interface-number* | **ip** *source-ip-address* }]	可选 该命令在用户视图下执行
在IPv6网络，用TFTP下载/上传文件	**tftp ipv6** *tftp-ipv6-server* [**-i** *interface-type interface-number*] { **get** | **put** } *source-filename* [*destination-filename*] [**vpn-instance** *vpn-instance-name*]	可选 该命令在用户视图下执行

说明

- 如果源接口下没有配置主地址，将导致 TFTP 传输失败。
- 如果先后配置了客户端 TFTP 报文的源接口和源 IP，则新配置的源 IP 将覆盖现有的源接口配置。反之亦然。

2.3 TFTP客户端显示和维护

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 TFTP 客户端的情况，通过查看显示信息验证配置的效果。

表2-3 TFTP 客户端显示和维护

操作	命令
查看TFTP客户端的当前配置	**display tftp client configuration** [**|** { **begin** | **exclude** | **include** } *regular-expression*]

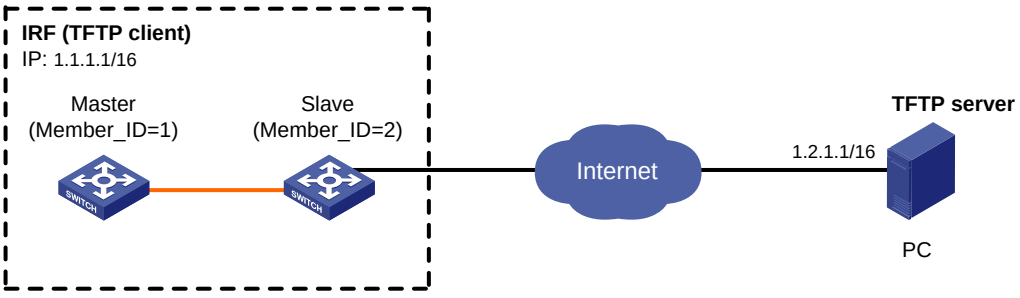
2.4 TFTP客户端配置举例

1. 组网需求

- Master 和 Slave 两台成员设备组成 IRF。Master 的成员编号为 1，Slave 的成员编号为 2。
- IRF 作为 TFTP 客户端，PC 作为 TFTP 服务器。IP 地址如组网图所示，IRF 和 PC 之间路由可达。
- IRF 通过 TFTP 协议从 PC 上下载最新启动文件完成 IRF 升级，同时将配置文件 config.cfg 上传到 PC 实现备份。

2. 组网图

图2-2 利用 TFTP 客户端功能实现平滑升级



说明：橙色的线表示IRF连接

3. 配置步骤

(1) PC（TFTP 服务器）的配置（具体配置步骤略）

- 在 PC 上启动 TFTP 服务器功能；
- 配置 TFTP 服务器的工作目录。

(2) IRF（TFTP 客户端）上的配置

注意

如果 Master 和 Slave 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。

将启动文件 newest.bin 从 PC 下载到 Master 和 Slave。

- 将启动文件 newest.bin 从 PC 下载到 Master 存储介质的根目录下。

```
<Sysname> tftp 1.2.1.1 get newest.bin
```

- 将启动文件 newest.bin 从 PC 下载到 Slave（成员编号为 2）存储介质的根目录下。

```
<Sysname> tftp 1.2.1.1 get newest.bin slot2#flash:/newest.bin
```

将 IRF 的配置文件 config.cfg 上传到 TFTP 服务器。

```
<Sysname> tftp 1.2.1.1 put config.cfg configback.cfg
```

将 newest.bin 指定为所有成员设备的主用下次启动文件。

```
<Sysname> boot-loader file newest.bin slot all main
  This command will set the boot file of the specified board. Continue? [Y/N]:y
```

```
  The specified file will be used as the main boot file at the next reboot on slot 1!
  The specified file will be used as the main boot file at the next reboot on slot 2!
```

重启 IRF，完成 IRF 软件升级。

```
<Sysname> reboot
```

注意

下次启动文件必须存放在存储介质的根目录下。可使用文件的拷贝或移动操作来调整文件的路径为根目录。关于 **boot-loader** 命令的详细描述请参见“基础配置命令参考”中的“软件升级”。

目 录

1 文件系统管理

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）保存在设备的存储设备中，为了方便用户对存储设备进行有效的管理，设备以文件系统的方式对这些文件进行管理。

文件系统操作包括：文件操作、目录操作、存储设备操作、批处理操作等。

1.1.2 文件名参数输入规则

在设备上执行文件系统操作时，文件名参数的输入方式需要遵循下表。

表1-1 设备文件名参数输入规则

格式	说明	长度	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	1～91个字符	a.cfg表示当前目录下的a.cfg文件，如果当前工作路径在Master，则a.cfg表示Master上的a.cfg文件；如果当前工作路径在Slave，则a.cfg表示Slave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	1～135个字符	test/a.cfg表示当前路径下test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，Master上的存储介质表示为flash；Slave上的存储介质表示为slotX#flash，X为设备的成员编号，如：slot2#flash。可以使用**display irf**命令查看设备与成员编号的对应关系	1～135个字符	flash:/test/a.cfg表示Master上Flash根目录下test文件夹下的a.cfg文件 如果要读写Slave（编号为2）上Flash根目录下的a.cfg文件时，命令行文件名参数需要输入slot2#flash:/a.cfg

1.2 文件操作

文件操作包括显示指定目录或文件信息、显示文件的内容、重命名文件、拷贝文件、移动文件、删除文件、恢复删除的文件、彻底删除文件。

说明

创建文件可以通过拷贝、下载操作或 **save** 命令来辅助完成。

1.2.1 显示文件信息

表1-2 显示文件信息

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

1.2.2 显示文件内容

表1-3 显示文件内容

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

1.2.3 重命名文件

表1-4 重命名文件

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

1.2.4 拷贝文件

表1-5 拷贝文件

操作	命令	说明
拷贝文件	**copy** *fileurl-source fileurl-dest*	必选 该命令在用户视图下执行

1.2.5 移动文件

表1-6 移动文件

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

1.2.6 删除文件

表1-7 删除文件

操作	命令	说明
删除文件	**delete** [**/unreserved**] *file-url*	必选 该命令在用户视图下执行

注意

- 使用 **delete** *file-url* 命令删除文件，被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某个废弃文件，必须在该文件的原目录下执行 **reset recycle-bin** 命令，才可以回收存储空间。
- 使用 **delete /unreserved** *file-url* 命令删除文件，被删除的文件被彻底删除，不能再恢复。效果等同于执行 **delete** *file-url* 命令后，再在同一目录下执行了 **reset recycle-bin** 命令。

1.2.7 恢复删除文件

表1-8 恢复删除文件

操作	命令	说明
恢复删除文件	**undelete** *file-url*	必选 该命令在用户视图下执行

1.2.8 彻底删除回收站中的文件

表1-9 彻底删除回收站中的文件

操作	命令	说明
进入要删除文件的原路径	**cd** { *directory* | **..** | **/** }	可选 如果要删除的文件的原路径不是当前路径，则该步骤必选 该命令在用户视图下执行
彻底删除当前目录下、处于回收站中的文件	**reset recycle-bin** [**/force**]	必选 该命令在用户视图下执行

1.2.9 验证文件的正确性和完整性

使用指定的摘要算法对指定的文件计算摘要值，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1-10 验证文件的正确性和完整性

操作	命令	说明
验证文件的正确性和完整性配置	**crypto-digest sha256 file** *file-url*	必选 该命令在用户视图下执行

1.3 目录操作

目录操作包括创建/删除目录、显示当前的工作路径以及显示指定目录或文件信息等。

1.3.1 显示目录信息

表1-11 显示目录信息

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

1.3.2 显示当前的工作路径

表1-12 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**	必选 该命令在用户视图下执行

1.3.3 改变当前的工作路径

表1-13 改变当前的工作路径

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

1.3.4 创建目录

表1-14 创建目录

操作	命令	说明
创建目录	**mkdir** *directory*	必选 该命令在用户视图下执行

1.3.5 删除目录

表1-15 删除目录

操作	命令	说明
删除目录	**rmdir** *directory*	必选 该命令在用户视图下执行

说明

- 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。文件的删除请参见 **delete** 命令，子目录的删除请参见 **rmdir** 命令）。
- 成功执行 **rmdir** 后，回收站中原来属于该文件夹的文件会自动被彻底删除。

1.4 存储设备操作

1.4.1 管理存储设备的存储空间

由于异常操作等原因，存储设备的某些空间可能不可用，用户可以通过 **fixdisk** 命令来恢复存储设备的空间。如果使用 **format** 命令则会格式化指定的存储设备，该存储设备上的所有数据将被删除。

表1-16 管理存储设备的存储空间

操作	命令	说明
恢复存储设备的空间	**fixdisk** *device*	可选 该命令在用户视图下执行
格式化存储设备	**format** *device*	可选 该命令在用户视图下执行

注意

格式化操作将导致存储设备上的所有文件丢失，并且不可恢复；尤其需要注意的是，如果存储设备上有启动配置文件，格式化该存储设备，将丢失启动配置文件。

1.4.2 Nand Flash显示和维护

Nand Flash 存储器因为具有大容量、低价格、写速率快的优势，已逐渐成为新产品的首选存储器。Nand Flash 的物理空间被逻辑划分为多个块（Block），每个块又由多个页（page）组成。Nand Flash 的基本擦除单位是块，而基本读写单位是页，文件系统在分配存储空间的时候也是以页为单位的。

1. 坏块的显示和修复

Nand Flash 出厂时可能出现坏块，不同厂家出现的坏块比率不一样，并且在使用过程中，如果频繁使用某个区域，则容易造成该区域内块的损坏。坏块是不能用于存储数据的，文件系统在为文件分配存储空间的时候，需要跳过坏块。因此，设备提供了命令行帮助用户随时了解坏块分布信息以及修复坏块。

表1-17 坏块的显示和修复

配置	命令	说明
显示Nand Flash存储器的坏块分布信息	**display nandflash badblock-location** [**|** { **begin** | **exclude** | **include** } *regular-expression*]	必选 该命令在任意视图下执行
修复坏块	**fixdisk** *device*	必选 该命令在用户视图下执行

2. 文件检错

文件写操作成功后，结合使用下面两条命令可以检查保存到存储介质中的文件内容是否正确。

表1-18 文件检错

操作	命令
显示指定文件在存储介质上的空间分布信息	**display nandflash file-location** *filename* [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示指定物理页面的数据	**display nandflash page-data** *page-value* [**|** { **begin** | **exclude** | **include** } *regular-expression*]

1.5 批处理操作

批处理文件是可执行命令的集合，批处理功能用于自动执行批处理文件里的命令，执行过程相当于手工逐条执行这些命令。

执行批处理操作之前，首先需要在 PC 上编辑批处理文件，然后将批处理文件下载到设备上，文件名的后缀可以是任何格式，比如.bat、.txt 等。

表1-19 执行批处理操作

操作	命令	说明
进入系统视图	**system-view**	-
执行批处理文件	**execute** *filename*	必选

注意

批处理命令不保证每一条命令的执行，比如某命令设置错误或者该命令执行的条件不成熟，本命令将执行失败，系统会跳过该命令转到下一条。

1.6 设置文件系统的提示方式

用户可以通过命令修改当前文件系统的提示方式。文件系统支持两种提示方式：

- **alert**：当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。
- **quiet**：当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 设置文件系统的提示方式

操作	命令	说明
进入系统视图	**system-view**	-
设置文件系统的提示方式	**file prompt** { **alert** | **quiet** }	可选 缺省情况下，文件系统的提示方式为**alert**

1.7 文件系统应用举例

查看当前目录下的文件及子目录。

```
<Sysname> dir
Directory of flash:/

   0     -rw-  13308645  Mar 22 2011 11:34:07   main.bin
   1     -rw-      7380  Mar 25 2011 10:47:36   patch-package.bin
   2     -rw-       228  Mar 25 2011 10:50:39   patchstate
   3     -rw-      3921  Apr 01 2011 17:56:30   startup.cfg
   4     -rw-       151  Apr 01 2011 17:56:24   system.xml

515712 KB total (2521 KB free)
```

进入 test 目录，并创建新文件夹 mytest。

```
<Sysname> cd test
<Sysname> mkdir mytest
```

```
%Created dir flash:/test/mytest.
```
显示当前的工作路径。
```
<Sysname> pwd
flash:/test
```
查看 test 目录下的文件及子目录。
```
<Sysname> dir
Directory of flash:/test/

   0   drw-         -  Apr 01 2011 18:28:14   mytest

515712 KB total (2519 KB free)
```
返回上一级目录。
```
<Sysname> cd ..
```
显示当前的工作路径。
```
<Sysname> pwd
flash:
```

目 录

1 配置文件管理

配置文件管理是设备提供的用于管理配置文件的一项功能。它具有较好的命令行接口，方便用户对配置文件进行管理。

1.1 配置文件简介

配置文件是命令行的集合。用户将当前配置（一条条命令行）保存到配置文件中，以便设备重启后，这些配置能够继续生效。另外，通过配置文件，用户可以非常方便地查阅配置信息也可以将配置文件上传/下载到别的设备，来实现设备的批量配置。

1.1.1 配置文件类型介绍

1. 软件功能缺省值&空配置

软件版本中所有的软件功能都被赋了一个初始值（软件功能缺省值），这些初始值的集合被称为“空配置”。

说明

- 软件功能的缺省值可以是具体数值、功能开启/关闭状态、也可以为空值（为空值代表用户使用该功能时，需根据需要进行赋值）。
- 软件功能缺省值无法通过命令行直接进行查看，用户可通过查看产品当前软件版本的命令手册，了解各软件功能的缺省值。

2. 软件功能出厂值&缺省配置文件

为方便客户的使用，软件版本出厂时某些软件功能会被赋一个与初始值不一样的取值（软件功能出厂值），软件出厂值将被统一保存在一个文件中，该文件称为“缺省配置文件”。

说明

- 软件功能出厂值与软件功能缺省值不同，不同型号的设备可以根据需要定制各自的出厂配置。
- 缺省配置文件被集成到了软件包*.bin 中，用户可以通过 **display default-configuration** 命令查看当前软件版本中软件功能的出厂值。

3. 软件功能当前值&配置文件

设备中正在运行的软件功能的取值称为软件功能当前值（可以与软件功能缺省值一致，也可能通过配置后与软件功能缺省值不一致）。对软件功能进行配置、并对配置结果进行保存后，所有软件功能的取值都将被统一保存在一个文件中，该文件称为“配置文件”。

设备的 flash 中可以同时存在多个配置文件，用户可以根据需要选择下次启动时采用哪个配置文件。根据配置文件的使用情况，可以分为如下几类。

- 当前配置文件：设备当前使用的配置文件。
- 下次主用启动配置文件：设备下次启动时优先使用的配置文件，
- 下次备用启动配置文件：设备下次启动时如果主用配置文件不可用，作为备用的启动配置文件。
- 其它配置文件：flash 中除上述三类外的其它.cfg 文件。

窍门

用户可以将设备在多个使用环境下的配置保存成多个配置文件。当设备在网络中移动时，通过指定下次启动配置文件并重启设备，可以使设备以新的配置迅速适应切换后的网络环境，节省重新配置的工作量。而且多配置文件可以方便用户的备份、修改、恢复等操作，提高设备的可靠性。

说明

配置文件的后缀为.cfg，用户可以通过 **display saved-configuration** 命令查看设备下次启动配置文件中的具体软件功能配置：

- 软件功能缺省值，不会体现在配置文件中。
- 已进行了配置、但没有通过 **save** 命令进行保存的配置，不会体现在配置文件中。

说明

用户可以通过 **display current-configuration** 命令查看设备中当前运行的配置：

- 软件功能当前值中，与软件功能缺省值一致的部分不会显示，与软件功能缺省值不一致的部分能够显示。
- 即使当前配置未通过 **save** 命令保存到配置文件中，也可以显示。

1.1.2 配置文件的内容与格式

配置文件为一个文本文件，其保存规则如下：

- 配置文件的内容为命令行的完整形式；
- 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，节与节之间通常用空行或注释行隔开（以#开始的为注释行，空行或注释行可以是一行或多行）；
- 文件中各节的安排顺序通常为：系统配置、接口配置、各种协议配置和用户界面配置；
- 以 return 结束。

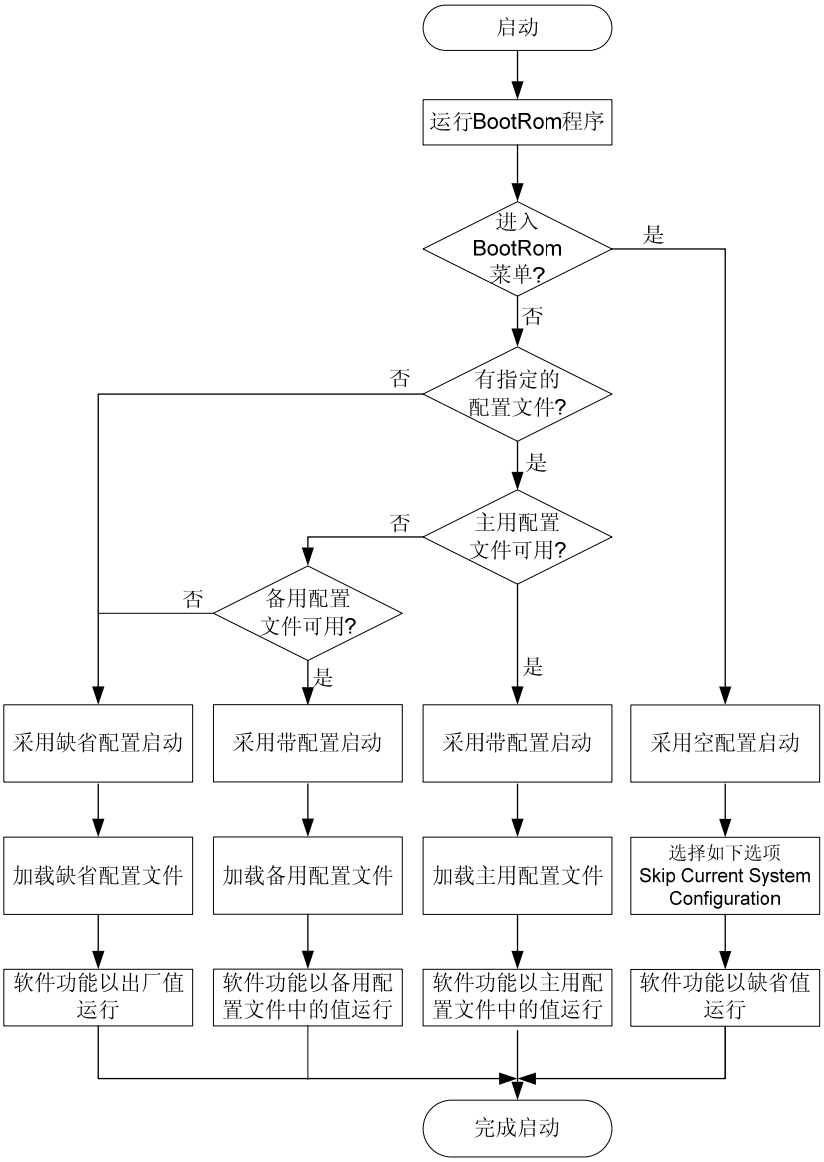
说明

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，不要随意手工修改配置文件。（执行 **save** 命令，设备会将当前配置自动生成配置文件）

1.1.3 设备启动过程中配置文件的选择

1. 设备启动过程中配置文件的选择流程

图1-1 设备启动过程中配置文件的选择流程



2. 采用空配置启动

设备启动时，若用户进入 BootRom 菜单并选择了 Skip Current System Configuration 选项，设备将采用软件的空配置方式进行启动。启动完成后，所有软件功能都将采用软件功能缺省值。

3. 采用缺省配置启动

设备启动时，若既没有选择采用空配置进行启动、也没有指定的配置文件，则设备会采用缺省配置方式进行启动。启动完成后，缺省配置文件中赋了值的软件功能将采用软件功能出厂值，其它软件功能都将采用软件功能缺省值。

说明

缺省配置文件被集成到了软件包*.bin 中，用户可以通过 **display default-configuration** 命令查看当前软件版本中软件功能的出厂值。

4. 采用带配置启动

设备启动时，若没有选择采用空配置进行启动、且有指定的配置文件，则设备会采用带配置方式进行启动。启动完成后，软件功能都将采用当前配置文件中的值。

- 如果采用带配置方式进行启动时存在主用配置文件，则设备启动运行时将采用主用配置文件中的值运行。
- 如果采用带配置方式进行启动时主用配置文件不可用，则设备启动运行时将采用备用配置文件中的值运行。
- 如果采用带配置方式进行启动时主备用配置文件均不可用，则设备将采用软件的缺省配置方式进行启动。

说明

用户可以通过 **display current-configuration** 命令查看设备中当前运行的配置：

- 软件功能当前值中，与软件功能缺省值一致的部分不会显示，与软件功能缺省值不一致的部分能够显示。
- 即使当前配置未通过 **save** 命令保存到配置文件中，也可以显示。

1.2 保存当前配置

1.2.1 保存当前配置任务简介

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重启时仍然有效，在重启设备前，需要将当前配置保存到配置文件中。

表1-1 保存当前配置任务简介

配置任务	说明	详细配置
使能配置文件同步保存功能	可选	1.2.2
保存当前配置	必选	1.2.3

1.2.2 使能配置文件同步保存功能

- 使能配置文件同步保存功能后，当用户执行“**save** [**safely**] [**backup** | **main**] [**force**]”或者“**save** *filename* **all**”操作保存当前配置时，Master 和 Slave 会同时自动把当前配置保存到指定的配置文件中，并将该文件配置为设备的下次启动文件，以保证 Master 和 Slave 配置文件内容的一致；

- 如果没有使能配置文件同步保存功能，则当用户执行“**save** [**safely**] [**backup** | **main**] [**force**]”或者“**save** *filename* **all**”操作保存当前配置时，只有 Master 自动把当前配置保存到指定的配置文件中，并将该文件配置为 Master 的下次启动文件，Slave 不会执行保存操作，也不会重新设置 Slave 的下次启动文件。

表1-2 使能配置文件同步保存功能

操作	命令	说明
进入系统视图	**system-view**	-
使能配置文件同步保存功能	**slave auto-update config**	可选 缺省情况下，配置文件同步保存功能处于使能状态

1.2.3 保存当前配置

1. 配置的保存方式

配置的保存方式有两种：

- 快速保存方式，执行不带 **safely** 参数的 **save** 命令。这种方式保存速度快，但是保存过程中如果出现设备重启、断电等问题，原有配置文件可能会丢失。
- 安全方式，执行带 **safely** 参数的 **save** 命令。这种方式保存速度慢，即使保存过程中出现设备重启、断电等问题，原有配置文件仍然会保存到设备中，不会丢失。

在电源稳定程度较好的环境中，推荐用户使用快速保存方式保存配置文件；在电源环境恶劣或者远程维护等情况，推荐用户使用安全模式保存配置文件。

表1-3 保存当前配置

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*]	二者必选其一 该命令可在任意视图下执行
将当前配置保存到所有成员设备存储介质的根目录下，并将该文件设置为下次启动配置文件	**save** [**safely**] [**backup** | **main**] [**force**]	

说明

- 配置文件名后缀必须为“.cfg”。
- 执行“**save** [**safely**] [**backup** | **main**] [**force**]”或者“**save** *filename* **all**”操作，是对所有成员设备同时生效还是只对Master生效，与配置文件的同步保存功能是否使能有关，详细介绍请参见“1.2.2 使能配置文件同步保存功能”。
- **save** [**safely**]和 **save** [**safely**] **main** 命令执行效果相同：都会在保存当前配置的同时，将指定文件设置为主用下次启动配置文件。
- 执行**save** [**backup** | **main**]命令时，如果出现设备重启、断电等问题，可能会造成下次启动配置文件丢失，这时，设备将以出厂配置启动。设备启动后，用户需要重新设置下次启动配置文件（请参见“1.4 设置下次启动配置文件”）。

2. 采用安全方式保存注意事项

设备采用新软件版本启动时，默认会采用升级前的下次启动配置文件。如果下次启动配置文件为老软件版本的配置文件，当用户使用新软件版本完成了若干配置，并对当前版本的最新配置进行首次保存时，若在 Master 上执行“**save** [**safely**] [**backup** | **main**] [**force**]”命令，此时设备会检查新配置信息与当前配置文件的兼容性。若二者不兼容，新配置信息无法写入当前使用的老配置文件中，此时设备上会提示如下信息：

```
The configuration file flash:/config.cfg will be automatically backed up as
flash:/_config_bak.cfg for a future version downgrading.
```

此时设备将进行如下操作：

- 对设备当前正在使用的老配置文件自动进行备份，以备版本降级时恢复设备的原有配置（例如，当前的配置文件名称为 config.cfg，则设备将该文件自动备份为名称为_config_bak.cfg 的文件，并将备份后的文件保存在 Master 及各 Subordinate 的 Flash 中）。
- 采用当前运行的配置生成新的配置文件，并用新配置文件直接覆盖当前正在使用的配置文件

注意

如果当前配置文件自动备份的过程中，出现 IRF 中某成员设备备份失败（其他成员设备备份不受影响）。设备将提示用户选择后续的操作方式。

- 放弃保存新版本上的所有配置：选择此操作方式，则所有成员设备不会保存当前运行的所有配置。
- 采用当前运行的配置生成新的配置文件，并用新配置文件直接覆盖当前正在使用的配置文件：选择此操作方式，升级前的老软件版本的配置文件将丢失。此时需要手工将 Master 上备份的老配置文件_XXX_bak.cfg 拷贝到该成员设备的 flash 中，以确保后续该成员设备也能够顺利的降级回老版本。

在保存配置文件时请确保各成员设备 Flash 有足够的空间并且自动备份文件名长度小于最大文件名长度（91 个字符），否则会导致老版本配置文件备份失败。

注意

- 如果设备需从当前的新软件版本降级回老软件版本时，首先要检查各成员设备上是否存在老版本的配置文件_XXX_bak.cfg。如果存在，需在降级之前手工指定各成员的下次启动配置文件采用老版本的配置文件，否则下次启动配置文件不会采用老版本的配置文件。
- 若执行 **save** filename [**all** | **slot**]命令保存当前配置时，设备不会备份老版本的配置文件。

1.3 配置回滚

1.3.1 配置回滚简介

配置回滚是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。配置回滚主要应用于：

- 当前配置错误，但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的状态。

配置回滚的基本步骤如下：

(1) 用户必须先设置备份配置文件的路径和文件名前缀；

(2) 系统将当前配置以指定的文件名（前缀+序号）备份到指定路径。这个备份有两种方式：一种是系统按照一定的时间周期自动备份，另一种是用户用命令行在必要时手工触发备份；

(3) 将当前配置回滚到指定配置文件的状态。配置回滚时，系统会比较、处理当前配置和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，回滚操作将不做处理；
- 对于在当前配置但不在回滚配置文件的命令，回滚操作将取消当前配置中的配置命令，即执行相应的 **undo** 命令；
- 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。


说明

当前配置只会备份到 Master。

1.3.2 配置回滚配置任务简介

表1-4 配置回滚配置任务简介

配置任务	说明	详细配置
设置备份参数	必选	1.3.3
自动备份当前配置	二者至少选其一	1.3.4
手工备份当前配置		1.3.5
配置回滚	必选	1.3.6

1.3.3 设置备份参数

自动或手动备份当前配置前必须设置备份配置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）保存到指定的路径。备份配置文件名形如20080620archive_1.cfg、20080620archive_2.cfg，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。修改备份配置的保存路径、文件名前缀，或设备重启后，备份序号也会从 1 开始重新自动编号，备份配置文件将重新计数，原路径下的备份配置文件将被视为普通配置文件，不再作为备份配置文件处理，查看备份配置文件时将不会显示此类文件的信息。

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

表1-5 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*	必选 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，也不会定时备份配置
系统允许保存的备份配置文件的最大数	**archive configuration max** *file-number*	可选 缺省情况下，系统最多允许保存5个备份配置文件

说明

- 为了 Master 变更后，配置回滚功能能在新 Master 上继续生效，请确保 **archive configuration location** 命令中指定的路径必须在 Master 和 Slave 上均存在，且路径参数中不能包含成员编号。
- 执行 undo archive configuration location 命令后，用户将不能进行手工备份当前配置，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，已保存的备份配置文件记录也会被清除。
- *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。

1.3.4 自动备份当前配置

用户可以使用本特性按照一定的时间间隔自动备份当前配置，使用 **display archive configuration** 命令可以查看到备份配置文件的名称和备份时间，以便用户可以将当前配置回退到某一历史时刻。

使用本特性时应根据设备存储介质的性能和修改配置的频繁程度来设置自动备份的时间间隔：

- 对于不会频繁修改配置的设备，建议按需手动备份当前配置；
- 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）；

表1-6 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*	可选 缺省情况下，系统不会自动备份当前配置

说明

设置自动备份配置时间间隔前必须指定备份配置文件的保存路径和文件名前缀。

1.3.5 手工备份当前配置

因为自动备份当前配置需要占用一定的系统资源，如果备份频率较高，对系统性能的影响也较大。因此，在设备维护过程中配置比较稳定（即不会频繁修改配置）的情况下，建议关闭自动备份功能，使用手工备份。

另外，自动备份是按照一定的时间周期进行的，手工备份能立即备份当前配置。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。

表1-7 手工备份当前配置

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

说明

手工保存备份配置前必须指定备份配置的保存路径和文件名前缀，否则备份失败。

1.3.6 配置回滚

表1-8 配置回滚

操作	命令	说明
进入系统视图	**system-view**	-
配置回滚	**configuration replace file** *filename*	必选

注意

配置回滚期间（即系统在执行 **configuration replace file** 命令时）不能重启成员设备，否则可能会造成配置回滚失败。另外，命令能否回滚成功还由命令的具体处理决定，存在以下情况时，回滚可能失败（若某条命令回滚失败，则会跳过该命令，直接处理下一条命令）：

- 配置命令不支持完整 **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。
- 若使用的配置文件不是由 **save** 命令或 **archive configuration** 命令生成的完整文件，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。
- **configuration replace file** *filename* 命令中指定的配置文件只能是明文配置文件，不能是被加密的配置文件。否则，会导致配置回滚出错。

1.4 设置下次启动配置文件

下次启动配置文件是指设备下次启动时使用的配置文件。设置下次启动配置文件有两种方式：

- 使用 **save** 命令。将当前配置保存到指定配置文件时，使用交互方式，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。
- 使用专用命令，请参见下表。

表1-9 设置下次启动配置文件

操作	命令	说明
配置所有成员设备的下次启动配置文件	**startup saved-configuration** *cfgfile* [**backup** | **main**]	必选 该命令在用户视图下执行

注意

配置文件必须以“.cfg”作为扩展名，启动配置文件必须存放在存储设备的根目录下。

1.5 备份下次启动配置文件

备份下次启动配置文件特性用于将设备下次启动配置文件备份至 TFTP 服务器上。

备份操作的对象是主用下次启动配置文件。

表1-10 备份下次启动配置文件

操作	命令	说明
将设备的下次启动配置文件备份到指定的TFTP服务器	**backup startup-configuration to** *dest-addr* [*dest-filename*]	必选 该命令在用户视图下执行

说明

在执行配置文件的备份操作前，请：

- 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。
- 在用户视图下使用 **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。若下次启动配置文件设置为 NULL，或者所设置的配置文件不存在，备份操作将会失败。
- FIPS 模式下不支持该命令。

1.6 删除设备中的下次启动配置文件

用户通过命令可以删除设备中的下次启动配置文件。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，但如果当前设备的主备用下次启动配置文件相同，仅执行一次删除操作，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。

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：

- 在设备软件升级之后，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）。

下次启动配置文件被删除后，设备下次上电时，系统将采用出厂配置进行初始化。

表1-11 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]**	必选 该命令在用户视图下执行

注意

本特性会将下次启动配置文件从所有成员设备上彻底删除，所以请慎用该命令。

1.7 恢复下次启动配置文件

恢复下次启动配置文件特性用于将 TFTP 服务器上保存的指定配置文件下载到所有成员设备存储介质的根目录下，并设置为所有成员设备的下次启动配置文件。

表1-12 恢复下次启动配置文件

操作	命令	说明
恢复主用下次启动配置文件	**restore startup-configuration from** *src-addr src-filename*	必选 该命令在用户视图下执行

说明

- 在执行配置文件的恢复操作前，请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，执行恢复操作的客户端设备已获得了相应的读写权限。
- 该命令执行成功后，用户可以在用户视图下使用 **display startup** 命令查看设备下次启动配置文件名是否与 *filename* 参数保持一致。
- FIPS 模式下不支持该命令。

1.8 配置文件显示和维护

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1-13 设备配置显示和维护

操作	命令
显示配置回滚功能的相关信息	**display archive configuration** [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示当前配置	**display current-configuration** [[**configuration** [*configuration*] | **interface** [*interface-type*] [*interface-number*] | **exclude** *modules*] [**by-linenum**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]]
显示出厂配置	**display default-configuration** [**|** { **begin** | **exclude** | **include** } *regular-expression*]
查看设备存储介质中保存的下次启动配置文件的内容	**display saved-configuration** [**by-linenum**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示用于本次及下次启动的配置文件名	**display startup** [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示当前视图下生效的配置	**display this** [**by-linenum**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

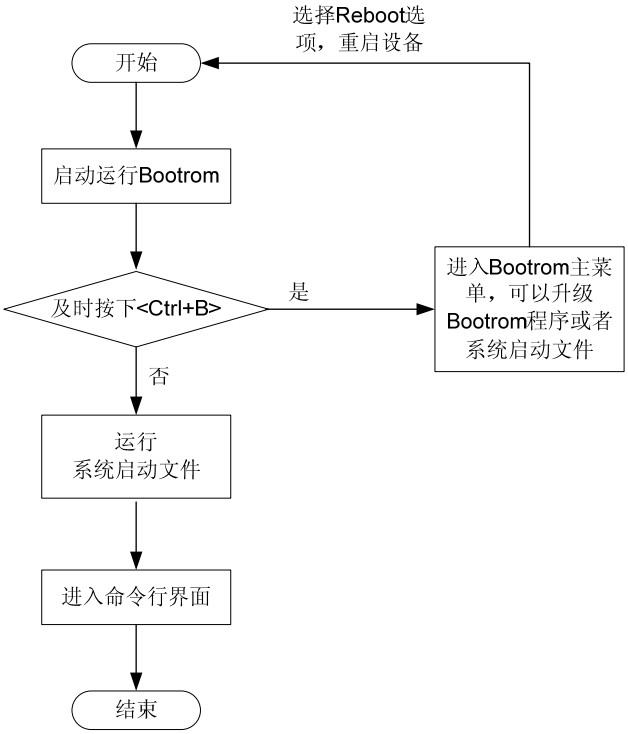
目 录

1 软件升级配置

1.1 设备软件简介

设备软件主要包括Bootrom程序和系统启动文件。设备上电后，先运行Bootrom程序，初始化硬件并显示设备的硬件参数，然后运行系统启动文件；启动文件一方面提供对硬件的驱动和适配功能，另一方面实现了业务特性。Bootrom程序与系统启动文件是设备启动、运行的必备软件，为整个设备提供支撑、管理、业务等功能，它们的关系如 图 1-1 所示。

图1-1 Bootrom 程序与系统启动文件关系示意图



1.2 升级方法简介

Bootrom 程序和系统启动文件都可以通过 Bootrom 菜单和命令行两种方式来升级，本文只介绍命令行升级方式，通过 Bootrom 菜单升级的具体操作请参见设备的版本说明书。

即便都是通过命令行，但因为实现原理不同，命令行下的软件升级方式又可以细分为以下几类：

升级方式及介绍	可升级的设备软件	各种升级方式对比说明
通过整机重启方式升级软件	Bootrom、启动文件	• 该方式通过重启设备来实现设备软件的升级，设备重启完成后，直接使用新版本软件运行 • 使用该方式升级设备软件时会导致当前业务中断

升级方式及介绍	可升级的设备软件	各种升级方式对比说明
通过热补丁方式升级启动文件	启动文件	• 热补丁是一种快速、低成本修复启动文件缺陷的方式 • 与通过整机重启升级启动文件相比，热补丁的优势是在升级过程中不会中断设备当前正在运行的业务 • 补丁文件与启动文件的版本一一对应，使用热补丁升级启动文件时，只能修复与补丁文件对应启动文件的缺陷，不涉及功能的添加及删除
通过ISSU（In-Service Software Upgrade，不中断业务升级）方式升级启动文件	启动文件	• 通过 ISSU 方式升级启动文件是一种简便、快速升级启动文件的方式 • 通过主备倒换机制完成启动文件的升级，ISSU 方式能够保证设备在升级过程中业务不中断 • 关于 ISSU 的详细描述，请参见“基本配置指导”中的“ISSU 配置”

1.3 通过整机重启方式升级软件

1.3.1 通过整机重启方式升级Bootrom

请按以下步骤升级 Bootrom：

(1) 使用 FTP 或者 TFTP，将 Bootrom 程序拷贝到设备存储介质的根目录下。

(2) 使用命令行升级 Bootrom 程序。

(3) 重启设备，使新的 Bootrom 程序生效。

IRF 系统中，由于不同成员设备的 Bootrom 可能各不相同，用户容易混淆，从而导致 Bootrom 升级错误。通过启动 Bootrom 升级时的合法性检查功能，设备就能够对 Bootrom 升级文件的正确性、版本配套性等进行严格的检查，保证升级成功。

表1-1 升级 Bootrom

操作	命令	说明
进入系统视图	**system-view**	-
启动升级时的合法性检查功能	**bootrom-update security-check enable**	可选 缺省情况下，Bootrom升级时的合法性检查功能是开启的
返回用户视图	**quit**	-
升级指定成员设备的Bootrom程序	**bootrom update file** *file-url* **slot** *slot-number-list*	必选 该命令在用户视图下执行

注意

必须先将 Bootrom 文件保存到相应成员设备存储介质的根目录下，**bootrom** 命令才能执行成功。

1.3.2 通过整机重启方式升级启动文件（方法一）

采用本特性升级启动文件时，请按以下步骤进行：

(1) 使用 FTP、TFTP 或者其它方式将启动文件下载保存到 Master 设备存储介质的根目录下。

(2) 将新的启动文件拷贝到 Slave 设备存储介质的根目录下。

(3) 使用命令行分别指定 Master 设备和 Slave 设备下次启动时使用的启动文件（以下简称为下次启动文件）。

(4) 重启设备，使新的启动文件生效。

表1-2 指定下次启动文件

操作	命令	说明
指定成员设备的下次启动文件	**boot-loader file** *file-url* **slot** { **all** | *slot-number* } { **main** | **backup** }	必选 该命令在用户视图下执行

注意

- 下次启动文件必须存放在设备存储介质的根目录下。可使用文件的拷贝或移动操作来调整文件的路径为根目录。
- 必须先将下次启动文件保存到相应成员设备存储介质的根目录下，**boot-loader** 命令才能执行成功。
- Master 和 Slave 的下次启动文件名称可以不同，但是版本必须一致，否则，Slave 会使用 Master 的启动文件重新启动加入 IRF。

1.3.3 通过整机重启方式升级启动文件（方法二）

使用本特性升级设备等效于 1.3.2 通过整机重启方式升级启动文件（方法一），但缩减了升级步骤。它通过一条命令可以完成将指定文件拷贝到指定成员设备，并设置为该成员设备下次启动配置文件的功能。使用本特性升级IRF时，因为IRF中通常存在多个成员设备，能简化升级步骤。

采用本特性升级启动文件时，请按以下步骤进行：

(1) 使用 FTP、TFTP 或者其它方式将启动文件下载保存到 Master 存储介质的根目录下。

(2) 同步升级启动文件。

(3) 重启指定成员设备或者整个 IRF 系统，使新的启动文件生效。

表1-3 同步升级启动文件

操作	命令	说明
同步升级指定成员设备或者所有成员设备的启动文件	**boot-loader update file** *file-url* **slot** { *slot-number* | **all** } { **main** | **backup** }	必选 该命令在用户视图下执行

1.4 通过热补丁方式升级启动文件

热补丁是一种快速、低成本修复产品软件版本缺陷的方式。和升级软件版本相比，热补丁的主要优势是不会使设备当前正在运行的业务中断，即在不重启设备的情况下，可以对设备当前软件版本的缺陷进行修复。

1.4.1 热补丁基本概念

1. 补丁和补丁文件

补丁（又被称为补丁单元）是用来修复某个缺陷的程序包，通常以补丁文件的形式发布，一个补丁文件可能包含一个或多个补丁，不同的补丁具有不同的功能。当补丁文件被用户从存储介质加载到内存补丁区中时，补丁文件中的补丁将被分配一个在此内存补丁区中唯一的单元序号，用于标志、管理、操作各补丁，补丁的单元序号从 1 开始顺序编号，如某补丁文件中有 3 个补丁单元，那合法的补丁单元号为 1、2 和 3。

2. 增量补丁

所谓增量补丁，是指各补丁单元和其前面的补丁单元有依赖性。比如，补丁文件中有 3 个补丁单元，则 3 号补丁必须在 1 号和 2 号补丁生效之后才能运行，而不能直接单独运行 3 号补丁。

当前发布补丁文件中的补丁均为增量补丁。

3. 正式补丁和临时补丁

- 正式补丁（Common patches）是通过版本发布流程发布的补丁。
- 临时补丁（Temporary patches）是未通过版本发布流程发布，用于临时解决紧急问题和需求的补丁。

正式补丁总会包含前面临时补丁的功能，从而替代前面的临时补丁。补丁的类型只对补丁加载（Load）过程产生影响——系统在加载正式补丁之前会先将系统中所有临时补丁删除。

4. 补丁包文件

补丁包文件是将设备需要的同期发布的多个补丁文件打包生成的文件。补丁包文件升级方式是补丁文件升级方式的改良。

使用补丁文件升级时，产品对补丁文件的名称进行了严格定义，指定类型的硬件会有对应的补丁文件，该文件的名称是固定的，用户不能随便定义。当某个部件需要软件升级时，用户必须先下载该部件对应的补丁文件，并将补丁文件重命名为指定的名称，如果命名错误，会造成该部件升级失败。如果要同时升级多个部件，则需要多次重复上述操作。

使用补丁包文件升级时，用户只需下载该补丁包文件，执行一次命令，就可以完成设备所有部件的软件升级，从而简化了补丁操作及补丁版本管理。

说明

本系列交换机发布补丁包文件，不单独发布单个补丁文件，补丁包文件以.hpk 为后缀。

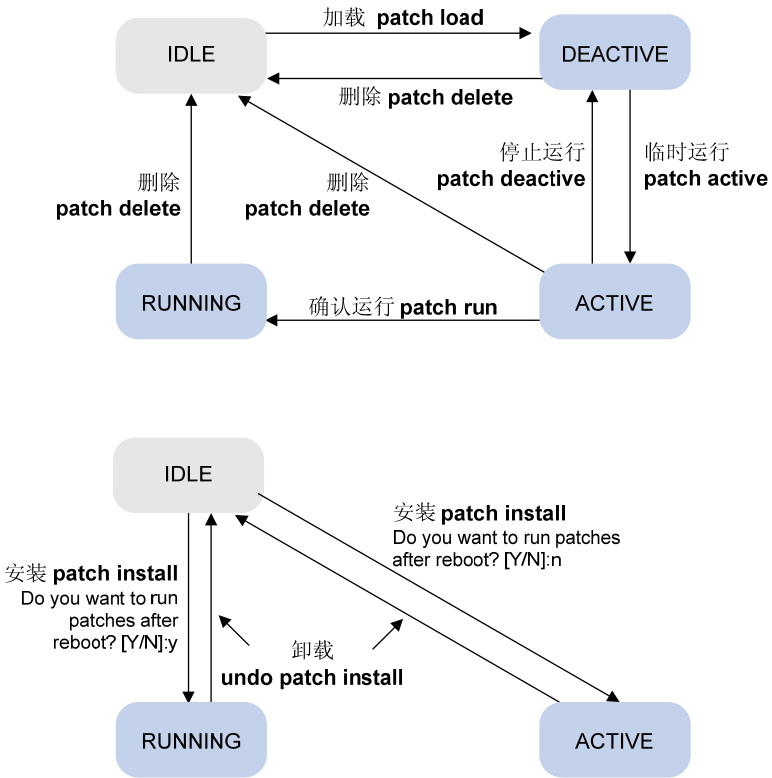
1.4.2 补丁状态

每个补丁都有自身的状态，只有在用户命令行的干预下才能发生切换。补丁状态切换与命令操作关系如 图 1-2 所示，其中：

- IDLE、DEACTIVE、ACTIVE 和 RUNNING 表示补丁的不同状态；
- 加载、临时运行、确认运行、停止运行、删除、安装、卸载表示补丁操作，分别对应命令 **patch load**、**patch active**、**patch run**、**patch deactive**、**patch delete**、**patch install** 和 **undo patch install**；
- 箭头方向表示状态的转变方向。

比如对 DEACTIVE 状态的补丁执行 **patch active** 操作，补丁的状态就会变为 ACTIVE。

图1-2 补丁状态切换与命令操作关系图



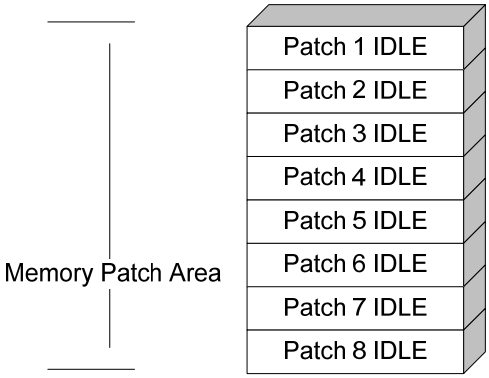
说明

补丁文件的状态信息内容保存在 Flash 中的 patchstate 文件里，建议用户不要对该文件进行操作。

1. 初始状态（IDLE）

表示尚未加载补丁，无法进行安装、运行等补丁操作，如 图 1-3 所示（假设系统补丁区中最多可以加载 8 个补丁）。

图1-3 补丁未加载



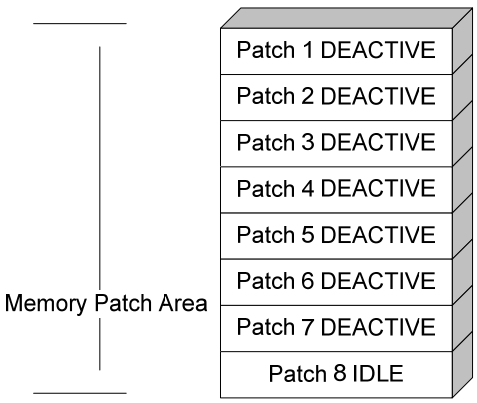
说明

当前内存补丁区中支持的最大补丁数为 200 个。

2. 未激活状态（DEACTIVE）

表示补丁已经被加载到内存补丁区，但尚未运行。假设用户将加载的补丁文件包含 7 个补丁，则这 7 个补丁将在经过版本校验及CRC校验之后被加载到内存补丁区，加载成功的补丁处于DEACTIVE状态，此时系统中补丁状态如 图 1-4 所示。

图1-4 补丁文件被加载

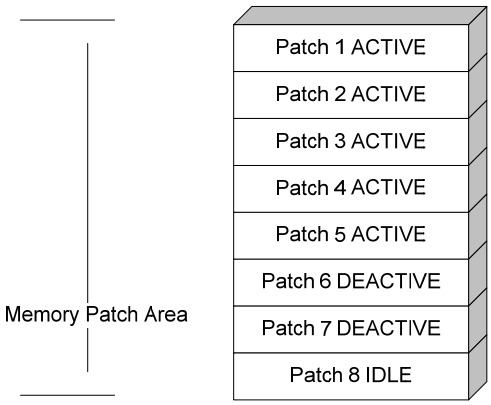


3. 激活状态（ACTIVE）

表示补丁已经被临时运行，即该补丁在设备重启之后不再生效。对于 图 1-4 中 7 个处于DEACTIVE状态的补丁，用户如果激活前 5 个补丁，则前 5 个补丁的状态将由DEACTIVE状态变成ACTIVE状态，此时系统中补丁状态如 图 1-5 所示。

系统重启后，所有处于 ACTIVE 状态的补丁将变成 DEACTIVE 状态。

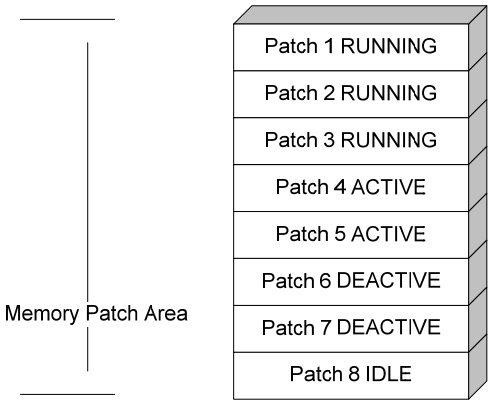
图1-5 补丁被激活



4. 确认运行状态（RUNNING）

表示补丁已经被永久运行，即该补丁在设备重启之后会继续生效。对于 图 1-5 中 5 个处于ACTIVE状态的补丁，用户确认运行前3个补丁后，前3个补丁的状态将由ACTIVE状态变成RUNNING状态，此时系统中补丁状态如 图 1-6 所示。

图1-6 补丁被确认运行



系统重启后，所有处于 RUNNING 状态的补丁仍保持为 RUNNING 状态。

1.4.3 热补丁配置任务简介

表1-4 热补丁配置任务简介

配置任务		说明	详细配置
安装补丁	一步式安装补丁	二者任选其一	1.4.5
	分步安装补丁	一步式配置和分步配置效果等同，分步配置时用户可以控制安装过程中的各个状态	1.4.6
分步卸载补丁		可选	1.4.7

1.4.4 配置准备

补丁包是根据安装补丁的设备类型按需发布。在进行安装补丁包操作前，需要通过 FTP/TFTP 等方式将补丁包保存到设备的存储介质上，保存时请注意补丁包版本必须与设备型号、设备的软件版本相匹配。如果不匹配，则会造成安装补丁包操作失败。

说明

加载和安装操作的对象是所有成员设备，所以，执行加载和安装操作前，请将补丁包保存到所有成员设备存储介质的根目录下，所有成员设备上补丁包必须一致（包括补丁包的名称和内容）。

1.4.5 一步式安装补丁

用户可以通过执行 **patch install** 命令来一步式安装补丁。执行该命令同时，需要指定补丁文件的来源，目前设备上可支持指定补丁文件的加载路径和从指定补丁包文件两种方式。

在执行 **patch install** 命令时，系统会提示“Do you want to continue running patches after reboot? [Y/N]:”：

- 如果输入<Y>或者<y>，则会安装指定路径下的所有补丁，设备重启后这些补丁继续生效，补丁状态从 IDLE 转换到 RUNNING。
- 如果输入<N>或者<n>，则会安装指定路径下的所有补丁，设备重启后这些补丁不再继续生效，补丁状态从 IDLE 转换到 ACTIVE。

表1-5 一步式安装补丁

操作	命令	说明
进入系统视图	**system-view**	-
一步式完成补丁的安装	**patch install** { *patch-location* | **file** *patch-package* }	必选 • *patch-location*：表示补丁文件所在的路径，该参数用于安装没有经过打包的补丁文件。 • **file** *patch-package*：表示补丁包文件的名称，该参数用于安装补丁包文件。

说明

- 指定路径下的补丁必须与设备的型号和版本匹配，否则系统不能正确识别补丁文件。
- 如果设备以前安装过补丁，必须先将历史补丁卸载，才能安装新补丁。用户可以使用 **display patch information** 显示设备的补丁信息。
- 如果通过指定补丁文件的加载路径来安装补丁，则执行补丁安装操作后，系统会将补丁文件的加载路径（**patch location**）修改成“**patch install** *patch-location*”中 *patch-location* 参数所指向的位置；如果通过指定补丁包文件来安装补丁，则执行补丁安装操作后系统不会改变补丁文件的加载路径。
- 如果要一步式卸载设备上所有已安装的补丁，请直接执行命令**undo patch install**。执行该命令等效于 1.4.7 分步卸载补丁。在搭建IRF环境下，推荐使用**undo patch install**命令一步式卸载补丁。

1.4.6 分步安装补丁

用户可以通过执行多条命令分步式安装补丁，该方式便于用户控制补丁安装过程中的各个状态。

1. 配置任务简介

表1-6 分步安装补丁配置任务简介

配置任务	说明	详细配置
设置补丁文件的加载路径	可选 如果是要安装补丁包，则无需设置补丁文件的加载路径	2.
加载补丁文件	必选	3.
激活补丁	必选	4.
确认运行补丁	可选	5.

2. 设置补丁文件的加载路径

表1-7 设置补丁文件的加载路径

操作	命令	说明
进入系统视图	**system-view**	-
设置补丁文件的加载路径	**patch location** *patch-location*	可选 缺省情况下，补丁文件的加载路径为flash:

说明

- 为了保证加载补丁过程的安全可靠，建议用户将补丁文件保存到 Flash 的根目录下。
- *patch-location* 参数指定的路径必须在所有成员设备上都存在，如果某成员设备上不存在该路径，则该命令在该成员设备上不生效。
- 通过指定补丁文件的加载路径来安装补丁文件的情况下，用户执行 **patch install** 命令后系统会自动修改补丁文件的加载路径。比如，先配置了 **patch location** xxx，再执行 **patch install** yyy，此时系统会自动将补丁文件的加载路径从 xxx 改为 yyy。

3. 加载补丁文件

只有正确加载补丁文件后才能进行补丁状态的管理。

- 如果要从补丁文件中安装补丁，则系统默认从 Flash 中读取补丁文件。
- 如果要从补丁包中安装补丁，则系统从指定的补丁包文件中查找补丁文件并进行加载操作。

注意

当使用 FTP 或 TFTP 方式将补丁文件上传/下载到设备的 Flash 中前，请将文件传输的模式设置为二进制模式，以免不能正确解析补丁文件。

表1-8 加载补丁文件

操作	命令	说明
进入系统视图	**system-view**	-
将补丁文件从存储介质（Flash）加载到指定的内存补丁区中	**patch load slot** *slot-number* [**file** *patch-package*]	必选

4. 激活补丁

激活补丁后，补丁会立即生效，处于试运行阶段。设备复位或重启后，该补丁不再生效，需要重新激活。

补丁的激活状态主要是提供一个缓冲带，如果补丁本身有问题，可以重启设备，以消除该补丁的作用，从而防止因为补丁错误而导致系统连续运行故障。

表1-9 激活补丁

操作	命令	说明
进入系统视图	**system-view**	-
激活补丁	**patch active** [*patch-number*] **slot** *slot-number*	必选

5. 确认运行补丁

确认运行补丁后，补丁的状态将变为 RUNNING，处于正式运行阶段。设备复位或重启后，该补丁会继续生效。

表1-10 确认运行补丁

操作	命令	说明
进入系统视图	**system-view**	-
确认运行补丁	**patch run** [*patch-number*] [**slot** *slot-number*]	必选

说明

该操作只对处于激活状态的补丁有效，对于处于其它状态的补丁，该操作无效。

1.4.7 分步卸载补丁

1. 配置任务简介

表1-11 分步卸载补丁配置任务简介

配置任务	说明	详细配置
停止运行补丁	必选	2.
删除补丁	必选	3.

2. 停止运行补丁

停止运行补丁后，补丁将进入未激活状态（DEACTIVE）。系统按打补丁前的特性运行。

表1-12 停止运行补丁

操作	命令	说明
进入系统视图	**system-view**	-
停止运行补丁	**patch deactive** [*patch-number*] **slot** *slot-number*	必选

3. 删除补丁

执行该操作，只是将补丁从内存补丁区中删除，并不会将补丁从存储介质中删除，补丁回到初始状态（IDLE）。补丁删除后，系统按打补丁前的特性运行。

表1-13 删除补丁

操作	命令	说明
进入系统视图	**system-view**	-

操作	命令	说明
将补丁从内存补丁区中删除	**patch delete** [*patch-number*] **slot** *slot-number*	必选

说明

搭建 IRF 环境下，推荐使用 **undo patch install** 命令一步式卸载补丁。

1.5 软件升级显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示软件升级的当前状态，通过查看显示信息验证配置的效果。

表1-14 软件升级显示和维护

操作	命令
显示启动文件信息	**display boot-loader** [**slot** *slot-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示补丁包信息	**display patch** [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示热补丁的信息	**display patch information** [**|** { **begin** | **exclude** | **include** } *regular-expression*]

1.6 软件升级典型配置举例

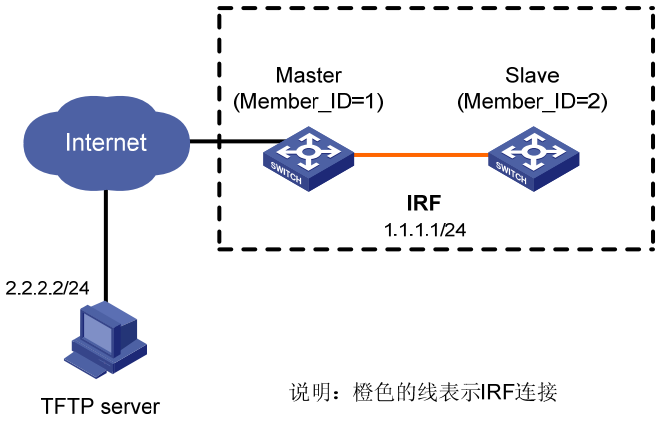
1.6.1 通过整机重启方式升级启动文件典型配置举例

1. 组网需求

- Master 和 Slave 两台成员设备组成 IRF。Master 的成员编号为 1，Slave 的成员编号为 2。
- IRF 当前的软件版本为 soft-version1，通过远程操作，将 IRF 系统的软件版本升级到 soft-version2，配置文件升级到 new-config；
- 最新版本的应用程序 soft-version2.bin 和最新配置文件 new-config.cfg 都保存在 TFTP server 上；
- IRF 的 IP 地址为 1.1.1.1/24，由 Master（成员编号为 1）和 Slave（成员编号为 2）两台成员设备组成。TFTP server 的 IP 地址为 2.2.2.2/24。IRF 与 TFTP server 之间路由可达。

2. 组网图

图1-7 通过整机重启方式升级启动文件组网图



3. 配置步骤

(1) TFTP server 的配置（注意：不同的服务器类型配置可能不同）

通过合法渠道（比如 H3C 官方网站或者代理商、技术支援人员）获取正确版本的启动文件和配置文件，并将该文件存储到 TFTP server 的工作路径，以便 TFTP client 可以访问。

(2) IRF 的配置

将 new-config.cfg 下载到 Master 上（注意：不同的服务器类型显示信息可能不同）。

```
<IRF> tftp 2.2.2.2 get new-config.cfg
  ..
  File will be transferred in binary mode
  Downloading file from remote TFTP server, please wait.....
  TFTP:      917 bytes received in 1 second(s)

  File downloaded successfully.
```

将 new-config.cfg 下载到 Slave（成员编号为 2）上。

```
<IRF> tftp 2.2.2.2 get new-config.cfg slot2#flash:/new-config.cfg
```

将启动文件 soft-version2.bin 下载到 Master 和 Slave 上。

```
<IRF> tftp 2.2.2.2 get soft-version2.bin
  ...
  File will be transferred in binary mode
  Downloading file from remote TFTP server, please wait............
  TFTP: 10058752 bytes received in 141 second(s)

  File downloaded successfully.
<IRF> tftp 2.2.2.2 get soft-version2.bin slot2#flash:/soft-version2.bin
```

将所有成员设备的下次启动配置文件指定为 new-config.cfg。

```
<IRF> startup saved-configuration new-config.cfg main
Please wait ...
Setting the master board ...
... Done!
Setting the slave board ...
```

```
Slot 2:
 Set next configuration file successfully
```

将所有成员设备的下次启动文件指定为 soft-version2.bin。

```
<IRF> boot-loader file soft-version2.bin slot all main
  This command will set the boot file of the specified board. Continue? [Y/N]:y
  The specified file will be used as the main boot file at the next reboot on slot 1!
  The specified file will be used as the main boot file at the next reboot on slot 2!
```

重启所有成员设备完成升级。

```
<IRF> reboot
```

设备重启后可以使用 **display version** 命令验证升级是否成功。

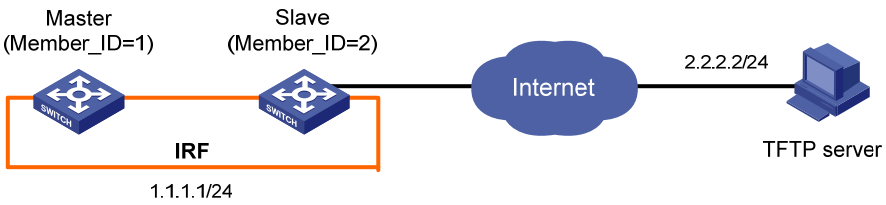
1.6.2 补丁包典型配置举例

1. 组网需求

- IRF（IRF 是整个 IRF 的统称，在本举例中包括 Matser 和 Slave 两台成员设备）当前的软件版本存在一些缺陷，需要使用补丁包进行修复。
- 补丁包 s5500hi-cmw520-r5206p02h01.hpk 保存在 TFTP server 上。
- IRF 的 IP 地址为 1.1.1.1/24，TFTP server 的 IP 地址为 2.2.2.2/24，IRF 与 TFTP server 之间路由可达。

2. 组网图

图1-8 补丁包升级组网图



说明：橙色的线表示IRF专用线缆

3. 配置步骤

(1) TFTP server 的配置（不同应用程序的配置方式不同，具体步骤略）

- 启动 TFTP server 功能。
- 将 s5500hi-cmw520-r5206p02h01.hpk 补丁包放到 TFTP server 的工作路径。

(2) IRF 的配置

注意

配置前需确认设备 Flash 有足够的剩余空间来存储补丁包文件。

开始升级前，执行 **save** 命令保存当前配置（配置步骤略）。

将 TFTP server 上的补丁包 s5500hi-cmw520-r5206p02h01.hpk 下载到 Master 存储介质的根目录下。

```
<IRF> tftp 2.2.2.2 get s5500hi-cmw520-r5206p02h01.hpk
```
将 TFTP server 上的补丁包 s5500hi-cmw520-r5206p02h01.hpk 下载到 Slave 存储介质的根目录下。
```
<IRF> tftp 2.2.2.2 get s5500hi-cmw520-r5206p02h01.hpk slot2#flash:/s5500hi-cmw520-r5206p02h01.hpk
```
安装补丁包。
```
<IRF> system-view
[IRF] patch install file flash:/s5500hi-cmw520-r5206p02h01.hpk
Patches will be installed. Continue? [Y/N]:y
Do you want to continue running patches after reboot? [Y/N]:y
Installing patches........
```
安装完成后，可以使用 **display patch information** 命令验证补丁包安装是否成功。

目 录

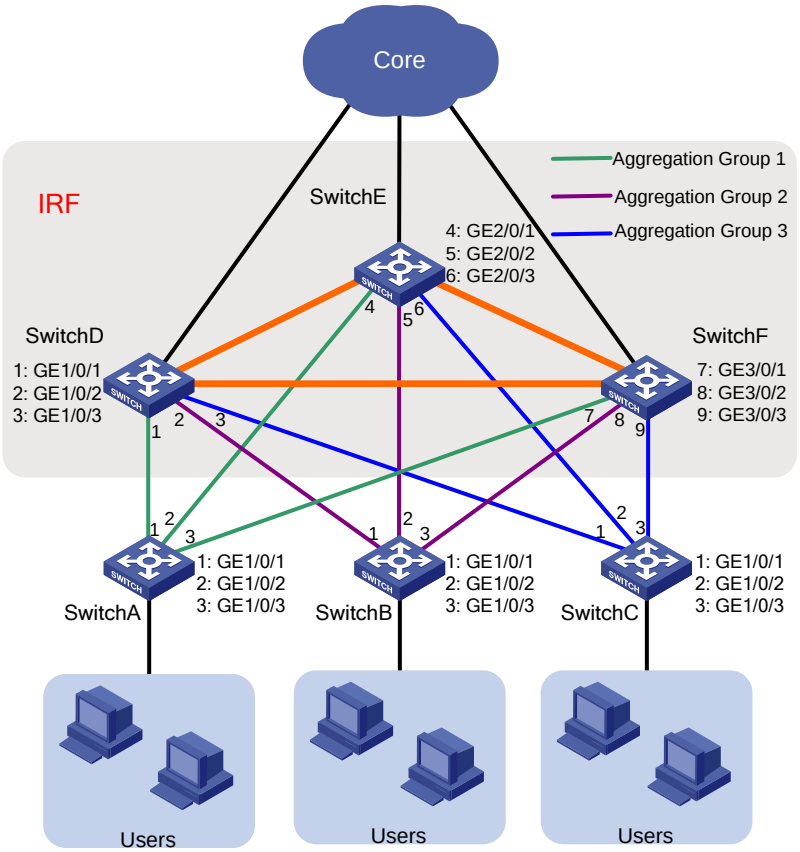
1 ISSU

1.1 ISSU简介

1.1.1 ISSU功能介绍

ISSU（In-Service Software Upgrade，不中断业务升级）是一种高可靠性升级设备启动文件的方式。如 图 1-1 所示。在IRF中为了保证用户网络的高可靠性，处于汇聚层的IRF成员设备间进行了跨设备链路聚合，使IRF各成员设备与每台接入层交换机之间的 3 条物理链路捆绑在一起成为一条逻辑链路。在这种情况下，如果要对IRF中各成员设备的启动文件进行升级、可通过ISSU方式逐一完成对每个成员设备启动文件的升级，从而保证IRF中各成员设备软件的升级过程中、接入层设备SwitchA、SwitchB、SwitchC下用户的数据业务转发不中断、或中断时间很短。

图1-1 IRF 组网图

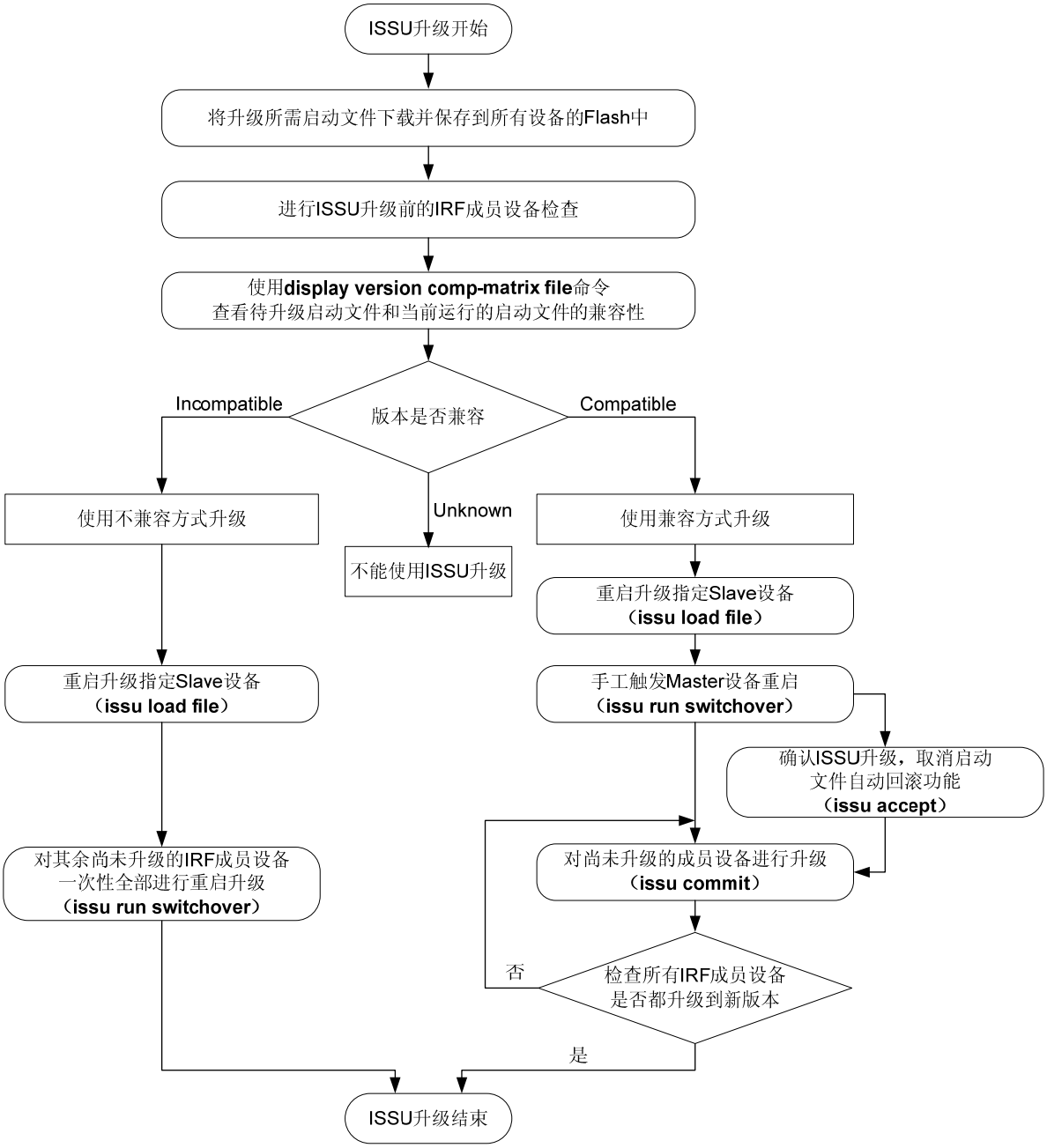


1.1.2 ISSU升级过程

1. ISSU升级过程介绍

ISSU升级由一系列步骤组成，升级过程中有严格的步骤要求，具体请参见 图 1-2。

图1-2 ISSU 升级流程图



说明

- ISSU 升级过程中请不要修改 IRF 系统的当前配置、插拔 IRF 端口的物理连线、删除/修改启动文件等操作，否则可能引起升级错误。
- 通过 ISSU 方式对成员设备的启动文件进行升级时，IRF 中各成员设备之间必须使用环形拓扑连接。

2. 查看ISSU升级状态

在 ISSU 升级过程中，管理员可通过 **display issu state** 命令查看当前 IRF 进行 ISSU 升级所处的状态（包括：新启动文件版本和原启动文件版本是否兼容，具体采用的 ISSU 升级方式等相关信息），以便管理员确定下一步需执行的操作。

ISSU升级过程中可能经历多个状态，具体请参见 表 1-1。

表1-1 ISSU 状态描述表

状态	说明
Init（初始状态）	表示还没有开始ISSU升级或者此次ISSU升级已完成
Load（加载状态）	表示Slave设备正在进行升级或者已经完成升级（此时如需终止版本加载，可通过自动/手动回滚方式使启动文件回滚恢复到原始版本）
Switchover（倒换状态）	表示已手工触发Master设备重启
Accept（已确认状态）	表示已经确认要执行新启动文件的ISSU加载（取消了启动文件的自动回滚功能，此时如需终止版本加载只能通过手动回滚方式使启动文件回滚恢复到原始版本）
Commit	表示IRF系统中至少还有一台成员设备没有完成启动文件升级，（此时不能通过自动/手动回滚方式使启动文件回滚恢复到原始版本）

1.1.3 ISSU升级过程中启动文件的版本回滚

用户在进行 IRF 系统的启动文件升级过程中，可能会由于某种原因（如新的启动文件被损坏）需要取消本次 ISSU 升级。交换机提供了 ISSU 升级过程中启动文件的版本回滚功能，能够使管理员根据需要将处于 ISSU 升级过程中的 IRF 成员设备的启动文件恢复到升级前的版本。

交换机在进行 ISSU 升级过程中，支持两种版本回滚方式。

1. 自动回滚方式：

用户在重启指定 Slave 设备时（已执行 **issu load** 命令），系统会自动创建一个版本回滚定时器。

- 在进行兼容方式的升级时：如果直到版本回滚定时器超时（用户可根据需求，通过命令行指定版本回滚定时器的取值），用户还没有确认 ISSU 升级（未执行 **issu accept**）或还没有对其它成员设备进行启动文件升级（未执行 **issu commit** 命令），则系统会自动将已升级 IRF 成员设备的启动文件回滚恢复到升级前的版本。
- 在进行不兼容方式的升级时：如果直到版本回滚定时器超时，用户还没有对其余尚未升级的 IRF 成员设备一次性全部进行重启升级（未执行 **issu run switchover** 命令），系统会自动将已升级 IRF 成员设备的启动文件回滚恢复到升级前的版本。

2. 手动回滚方式：

用户需要进行启动文件版本回滚时，可采用手动回滚方式进行IRF成员设备的启动文件回滚（是否能够采用手动回滚方式、取决于ISSU状态，具体请参见 表 1-1），用户都可以使用**issu rollback**命令手动将已升级IRF成员设备的启动文件回滚恢复到升级前的版本。

1.2 ISSU配置

1.2.1 ISSU配置任务简介

表1-2 ISSU 配置任务简介

配置任务		说明	详细配置
将升级所需的启动文件下载并保存到IRF所有成员设备的Flash中		必选	-
ISSU升级前IRF成员设备检查		必选	1.2.2
启动文件版本兼容性检查		必选	1.2.3
ISSU升级	兼容版本	必选 二者选其一	1.2.4 1.
	不兼容版本		1.2.4 2.

配置任务	说明	详细配置
配置ISSU的版本回滚方式	可选	1.2.5
ISSU功能的显示和维护	可选	1.2.6

1.2.2 ISSU升级前IRF成员设备检查

表1-3 ISSU 升级前的准备

操作	命令	说明
保存当前配置	**save**	必选 ISSU升级前，要确保IRF当前配置已保存到配置文件中
检查各成员设备的运行状态	**display device**	必选 ISSU升级前，要确保IRF中所有成员设备都处于正常运行状态
查看启动文件信息	**display boot-loader**	必选 ISSU升级前，要确保各成员设备当前使用的启动文件相同（文件的版本、名称及路径均应相同）
查看IRF中各成员设备的角色	**display irf**	必选
查看flash存储文件	**dir**	必选 ISSU升级前，要确保待升级的启动文件和原启动文件在各成员设备的Flash上同时存在，且存储路径相同

1.2.3 启动文件版本兼容性检查

通过 ISSU 方式进行 IRF 系统的启动文件升级前，需要进行启动文件新老版本间的兼容性检查，从而确定是否能够采用 ISSU 方式进行升级、以及该采用何种方式升级。

完成新版本启动文件的下载及保存后，可以根据启动文件版本兼容性检查结果选择不同的升级方式。

- 兼容版本（Compatible）：检查结果为兼容版本，表示设备当前运行的启动文件版本与新启动文件版本兼容。可采用ISSU兼容方式进行IRF系统的启动文件升级，具体请参见 1.2.4 1. 兼容版本的ISSU升级配置。
- 不兼容版本（Incompatible）：检查结果为不兼容版本，表示设备当前运行的启动文件版本与新启动文件版本不兼容。可采用ISSU不兼容方式进行IRF系统的启动文件升级，具体请参见 1.2.4 2. 不兼容版本的ISSU升级配置。
- 未知兼容性版本（Unknown）：检查结果为未知兼容性版本，表示指定的启动文件版本不支持 ISSU 功能、或者不能通过 ISSU 功能来进行启动文件的升级。不能采用 ISSU 方式进行 IRF 系统的启动文件升级。

表1-4 进行启动文件版本兼容性检查

操作	命令	说明
进入系统视图	**system-view**	-
检查新的启动文件与设备当前的启动文件版本是否兼容	**display version comp-matrix file** *upgrading-filename*	必选

1.2.4 配置ISSU升级

1. 兼容版本的ISSU升级配置

通过**display version comp-matrix file** *upgrading-filename*命令检查新启动文件与当前启动文件的版本后，若显示新启动文件与当前启动文件版本兼容（Compatible），则使用 表 1-5 中的步骤进行升级。

注意

在进行兼容版本的 ISSU 升级配置前，请确保当前 IRF 系统中的 Master 设备和升级结束后的新 Master 设备（通过 **issu load** 命令指定的 Slave 设备，ISSU 升级完成后，此设备 IRF 角色变为新的 Master）的优先级高于其它成员设备的优先级（否则请使用 **irf member** *member-id* **priority** *priority* 命令修改当前 Master 设备和新 Master 设备的优先级）。

表1-5 兼容版本的 ISSU 配置

操作	命令	说明
进入系统视图	**system-view**	-
升级指定的Slave设备（升级结束后的新Master）	**issu load file** *upgrading-filename* **slot** *slot-number*	必选 *slot-number*为指定的Slave设备的成员编号 执行此命令以后，指定Slave设备将使用新的启动文件进行自动重启 需要注意的是：请在重启过程完成以后，再执行下一步操作
手工触发原Master设备重启	**issu run switchover slot** *slot-number*	必选 执行此命令后： • 原 Master 设备使用原版本启动文件重新启动，重启完成后该设备的 IRF 角色改变为 Slave • IRF 中的 Slave 设备重新进行 IRF 选举，选举获胜者（通过 **issu load** 命令指定的 Slave 设备）倒换为新的 Master 设备 需要注意的是： • 本命令中指定的 *slot-number* 参数值必须和 **issu load** 命令中指定的值相同 • 请在重启过程完成以后，再执行下一步操作
确认ISSU升级，取消启动文件版本的自动回滚功能	**issu accept slot** *slot-number*	可选 缺省情况下，版本回滚定时器的超时时长为45分（即**issu load file**命令执行45分钟后，若还未执行**issu commit**命令对IRF系统中尚未升级的成员设备进行ISSU升级、或未通过**issu accept**命令取消自动回滚功能，则设备将自动终止ISSU升级操作，启动文件将恢复到升级前的版本） 需要注意的是： • 本命令中指定的 *slot-number* 参数值必须和 **issu load** 命令中指定的值相同 • 执行此命令后，启动文件的版本回滚定时器失效（即，启动文件不能再进行自动回滚）

操作	命令	说明
对IRF系统中尚未进行ISSU升级的成员设备进行升级	**issu commit slot** *slot-number*	必选 • 此命令一次只能指定一台成员设备，当IRF 系统中有三台或三台以上成员设备时，您需要多次执行此命令、逐一完成各成员设备的升级 • 所有 IRF 成员设备都使用新版本启动文件重启后，ISSU 升级结束

说明

- ISSU 升级结束后，IRF 中成员设备的角色会发生变化。
- 执行 issu commit 命令后，用户不能通过执行 issu rollback 命令将启动文件从当前版本 BB 回滚到 ISSU 升级前的版本 AA。此时用户如果想将启动文件从版本 BB 恢复到 ISSU 升级前的版本 AA，请将原 AA 版本启动文件版本作为新启动文件版本，对 IRF 系统进行再一次 ISSU 升级。

2. 不兼容版本的ISSU升级配置

通过**display version comp-matrix file** *upgrading-filename*命令检查新启动文件与当前启动文件的版本兼容性后，若显示不兼容（Incompatible），则使用 表 1-6 中的步骤进行升级。

注意

在进行 ISSU 不兼容版本升级前，请把升级指定的 Slave 设备（即升级结束后的新 Master）的优先级设置为最高并保存配置，然后再进行 ISSU 升级，否则可能导致操作失败。

表1-6 不兼容版本的 ISSU 配置

操作	命令	说明
进入系统视图	**system-view**	-
升级指定的Slave设备（升级结束后的新Master）	**issu load file** *upgrading-filename* **slot** *slot-number* **force**	必选 *slot-number*为指定的Slave设备的成员编号 执行此命令以后，指定的Slave设备（升级结束后的新Master）将使用新的启动文件进行自动重启，重启完成后该设备处于Recover状态 需要注意的是：请在重启过程完成以后，再执行下一步操作
对其余尚未升级的IRF成员设备一次性全部进行重启升级	**issu run switchover slot** *slot-number*	必选 需要注意的是：本命令中指定的*slot-number*参数值必须和**issu load**命令中指定的值相同 执行本命令以后，除了指定的Slave设备（新Master），其余IRF成员设备将使用新版本启动文件进行一次性全部重启升级，重启完成后ISSU升级结束

1.2.5 配置ISSU的版本回滚

表1-7 配置版本回滚定时器的超时时长

操作	命令	说明
进入系统视图	**system-view**	-
设置版本回滚定时器的超时时长	**issu rollback-timer** *minutes*	可选 缺省情况下，版本回滚定时器的超时时长为45分钟（即**issu load file**命令执行45分钟后，若还未执行**issu commit**命令对IRF系统中尚未升级的成员设备进行ISSU升级、或未通过**issu accept**命令取消自动回滚功能，则设备将自动终止ISSU升级操作，启动文件将恢复到升级前的版本）

表1-8 配置采用手动回滚方式进行启动文件的版本回滚

操作	命令	说明
进入系统视图	**system-view**	-
配置ISSU升级过程中采用手动回滚方式进行启动文件的版本回滚	**issu rollback slot** *slot-number*	可选 缺省情况下，系统采用自动回滚方式进行启动文件的版本回滚 本命令中指定的*slot-number*参数值必须和**issu load**命令中的值相同

说明

在进行 ISSU 升级过程中，当执行了 **issu load** 命令以后，如果再修改版本回滚定时器的超时时长，修改后的超时时长对此次 ISSU 升级无效。

1.2.6 ISSU功能的显示和维护

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

表1-9 ISSU 显示和维护

操作	命令
显示版本回滚定时器相关信息	**display issu rollback-timer** [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示ISSU升级状态	**display issu state** [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示版本兼容信息	**display version comp-matrix** [**file** *upgrading-filename*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

2 ISSU典型配置举例

2.1 网络现状及需求分析

2.1.1 组网现状

用户当前组网如 图 2-1 所示：

(1) SwitchA、SwitchB 和 SwitchC 为三台接入交换机，下面连接各自的用户网络。

(2) SwitchD、SwitchE 和 SwitchF 为三台汇聚交换机，这三台交换机组成 IRF（Master 设备的成员编号为 1；Slave 设备的成员编号为 2 和 3）。

(3) 为了保证用户网络的高可靠性，处于汇聚层的 IRF 成员设备间进行了跨设备链路聚合，使 IRF 各成员设备与每台接入层交换机之间的 3 条物理链路捆绑在一起成为一条逻辑链路。

- IRF 上：创建 3 个动态聚合组，聚合组 1 中的端口与 Switch A 相连，聚合组 2 中的端口与 Switch B 相连，聚合组 3 中的端口与 Switch C 相连。
- SwitchA 上：创建聚合组 1，与 IRF 上的聚合组 1 对应。
- SwitchB 上：创建聚合组 2，与 IRF 上的聚合组 2 对应。
- SwitchC 上：创建聚合组 3，与 IRF 上的聚合组 3 对应。

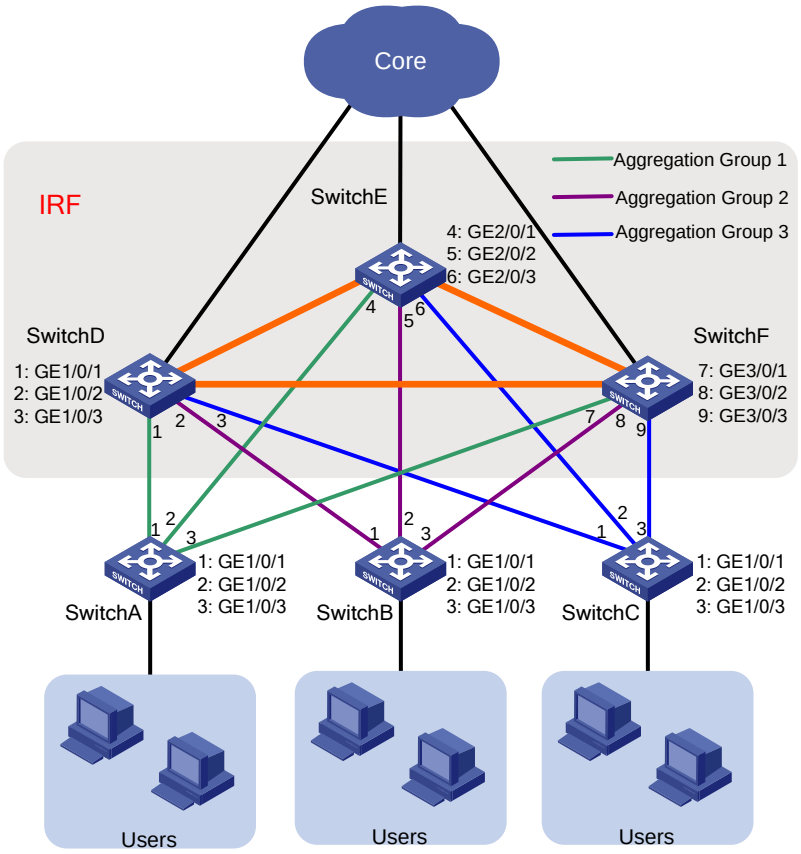
2.1.2 组网需求

现在用户需要在确保接入层交换机 SwitchA、SwitchB 和 SwitchC 下连的用户网络业务流量不中断的情况下，升级 IRF 中各成员设备的启动文件。

- 已知 IRF 当前的启动文件为 soft-version1.bin，希望通过远程操作进行 IRF 系统的启动文件升级（最新版本的启动文件 soft-version2.bin 保存在 TFTP server 上）。
- 已知 IRF 系统的 IP 地址为 1.1.1.1/24；TFTP server 的 IP 地址为 2.2.2.2/24。IRF 与 TFTP server 之间路由可达。

2.1.3 组网图

图2-1 用户网络示意图



2.2 ISSU升级配置

2.2.1 ISSU升级前提

1. IRF中进行了跨设备链路聚合

(1) IRF 上的配置

创建 3 个动态聚合组（聚合组 1 中的端口与 Switch A 相连，聚合组 2 中的端口与 Switch B 相连，聚合组 3 中的端口与 Switch C 相连）。

```
<IRF> system-view
[IRF] interface bridge-aggregation 1
[IRF-Bridge-Aggregation1] link-aggregation mode dynamic
[IRF-Bridge-Aggregation1] quit
[IRF] interface bridge-aggregation 2
[IRF-Bridge-Aggregation2] link-aggregation mode dynamic
[IRF-Bridge-Aggregation2] quit
[IRF] interface bridge-aggregation 3
[IRF-Bridge-Aggregation3] link-aggregation mode dynamic
[IRF-Bridge-Aggregation3] quit
```

将与 Switch A 相连的端口 GigabitEthernet1/0/1、GigabitEthernet2/0/1 和 GigabitEthernet3/0/1 加入该聚合组 1 中。

```
[IRF] interface GigabitEthernet 1/0/1
[IRF-GigabitEthernet1/0/1] port link-aggregation group 1
[IRF-GigabitEthernet1/0/1] quit
```

```
[IRF] interface GigabitEthernet 2/0/1
[IRF-GigabitEthernet2/0/1] port link-aggregation group 1
[IRF-GigabitEthernet2/0/1] quit
[IRF] interface GigabitEthernet 3/0/1
[IRF-GigabitEthernet3/0/1] port link-aggregation group 1
[IRF-GigabitEthernet3/0/1] quit
```

将与 Switch B 相连的端口 GigabitEthernet1/0/2、GigabitEthernet2/0/2 和 GigabitEthernet3/0/2 加入该聚合组 2 中。

```
[IRF] interface GigabitEthernet 1/0/2
[IRF-GigabitEthernet1/0/2] port link-aggregation group 2
[IRF-GigabitEthernet1/0/2] quit
[IRF] interface GigabitEthernet 2/0/2
[IRF-GigabitEthernet2/0/2] port link-aggregation group 2
[IRF-GigabitEthernet2/0/2] quit
[IRF] interface GigabitEthernet 3/0/2
[IRF-GigabitEthernet3/0/2] port link-aggregation group 2
[IRF-GigabitEthernet3/0/2] quit
```

将 IRF 中与 Switch C 相连的端口 GigabitEthernet1/0/3、GigabitEthernet2/0/3 和 GigabitEthernet3/0/3 加入该聚合组 3 中。

```
[IRF] interface GigabitEthernet 1/0/3
[IRF-GigabitEthernet1/0/3] port link-aggregation group 3
[IRF-GigabitEthernet1/0/3] quit
[IRF] interface GigabitEthernet 2/0/3
[IRF-GigabitEthernet2/0/3] port link-aggregation group 3
[IRF-GigabitEthernet2/0/3] quit
[IRF] interface GigabitEthernet 3/0/3
[IRF-GigabitEthernet3/0/3] port link-aggregation group 3
[IRF-GigabitEthernet3/0/3] quit
```

(2) Switch A 上的配置

创建动态聚合接口 1。

```
<SwitchA> system-view
[SwitchA] interface bridge-aggregation 1
[SwitchA-Bridge-Aggregation1] link-aggregation mode dynamic
[SwitchA-Bridge-Aggregation1] quit
```

#将 SwitchA 上与 IRF 各成员设备相连的端口 GigabitEthernet1/0/1、GigabitEthernet1/0/2 和 GigabitEthernet1/0/3 加入聚合组 1 中。

```
[SwitchA] interface GigabitEthernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] port link-aggregation group 1
[SwitchA-GigabitEthernet1/0/1] quit
[SwitchA] interface GigabitEthernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] port link-aggregation group 1
[SwitchA-GigabitEthernet1/0/2] quit
[SwitchA] interface GigabitEthernet 1/0/3
[SwitchA-GigabitEthernet1/0/3] port link-aggregation group 1
[SwitchA-GigabitEthernet1/0/3] quit
```

(3) Switch B 上的配置

创建动态聚合接口 2。

```
<SwitchB> system-view
[SwitchB] interface bridge-aggregation 2
[SwitchB-Bridge-Aggregation2] link-aggregation mode dynamic
[SwitchB-Bridge-Aggregation2] quit
```

#将 SwitchB 上与 IRF 各成员设备相连的端口 GigabitEthernet1/0/1、GigabitEthernet1/0/2 和 GigabitEthernet1/0/3 加入聚合组 2 中。

```
[SwitchB] interface GigabitEthernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] port link-aggregation group 2
[SwitchB-GigabitEthernet1/0/1] quit
[SwitchB] interface GigabitEthernet 1/0/2
[SwitchB-GigabitEthernet1/0/2] port link-aggregation group 2
[SwitchB-GigabitEthernet1/0/2] quit
[SwitchB] interface GigabitEthernet 1/0/3
[SwitchB-GigabitEthernet1/0/3] port link-aggregation group 2
[SwitchB-GigabitEthernet1/0/3] quit
```

(4) Switch C 上的配置

创建动态聚合接口 3。

```
<SwitchC> system-view
[SwitchC] interface bridge-aggregation 3
[SwitchC-Bridge-Aggregation3] link-aggregation mode dynamic
[SwitchB-Bridge-Aggregation3] quit
```

将 SwitchC 上与 IRF 各成员设备相连的端口 GigabitEthernet1/0/1、GigabitEthernet1/0/2 和 GigabitEthernet1/0/3 加入聚合组 3 中。

```
[SwitchC] interface GigabitEthernet 1/0/1
[SwitchC-GigabitEthernet1/0/1] port link-aggregation group 3
[SwitchC-GigabitEthernet1/0/1] quit
[SwitchC] interface GigabitEthernet 1/0/2
[SwitchC-GigabitEthernet1/0/2] port link-aggregation group 3
[SwitchC-GigabitEthernet1/0/2] quit
[SwitchC] interface GigabitEthernet 1/0/3
[SwitchC-GigabitEthernet1/0/3] port link-aggregation group 3
[SwitchC-GigabitEthernet1/0/3] quit
```

2. 完成了TFTP server的配置

通过合法渠道获取正确版本的升级启动文件，并将该文件存储到 TFTP server 的工作路径（不同类型的服务器配置可能不同），以便 TFTP client 可以访问。

2.2.2 ISSU升级准备

1. 将新启动文件soft-version2.bin下载保存到IRF中所有成员设备的Flash根目录中

```
<IRF> tftp 2.2.2.2 get soft-version2.bin
 File will be transferred in binary mode
 Downloading file from remote TFTP server, please wait……
 TFTP: 10058752 bytes received in 141 second(s)
 File downloaded successfully.
<IRF> copy soft-version2.bin slot2#flash:/
<IRF> copy soft-version2.bin slot3#flash:/
```

2. ISSU升级前进行IRF成员设备检查

(1) 检查各成员设备的运行状态是否正常（如不正常，则不能采用 ISSU 方式进行启动文件升级）。

```
<IRF> display device
Slot 1
SubSNo PortNum PCBVer  FPGAVer CPLDVer BootRomVer AddrLM Type       State
0      30      REV.B   NULL    001      107        IVL    MAIN       Normal
Slot 2
SubSNo PortNum PCBVer  FPGAVer CPLDVer BootRomVer AddrLM Type       State
```

```
0      30      REV.B   NULL    001      107       IVL    MAIN       Normal
Slot 3
SubSNo PortNum PCBVer  FPGAVer CPLDVer BootRomVer AddrLM Type       State
0      30      REV.B   NULL    001      107       IVL    MAIN       Normal
```

以上显示信息中，State 字段显示为 Normal，表示 IRF 中各成员设备均正常运行。

(2) 查看 IRF 系统中所有成员设备的当前运行的启动文件是否相同（如果不同，则不能采用 ISSU 方式进行启动文件升级）。

```
<IRF> display boot-loader
Slot 1
The current boot app is:  flash:/soft-version1.bin
The main boot app is:     flash:/soft-version1.bin
The backup boot app is:   flash:/
Slot 2
The current boot app is:  flash:/soft-version1.bin
The main boot app is:     flash:/soft-version1.bin
The backup boot app is:   flash:/
Slot 3
The current boot app is:  flash:/soft-version1.bin
The main boot app is:     flash:/soft-version1.bin
The backup boot app is:   flash:/
```

通过以上信息可以看到，IRF 中各成员设备当前运行的启动文件都是 soft-version1.bin。

(3) 逐一查看待升级的启动文件是否已保存到所有 IRF 成员设备的 Flash 中（如未保存，则不能采用 ISSU 方式进行启动文件升级）。

查看待升级的启动文件 soft-version2.bin 已保存到 Master 设备的 Flash 中。

```
<IRF> dir
Directory of flash:/

   0     -rw-      6085  May 29 2010 11:38:45   config.cfg
   1     -rw-     10518  Apr 26 2011 12:45:05   logfile.log
   2     -rw-  19057904  Apr 26 2011 14:24:11   soft-version1.bin
   3     -rw-  19077744  Apr 26 2011 14:13:46   soft-version2.bin
   4     drw-         -  Apr 26 2011 12:00:33   seclog
   5     -rw-       287  Apr 26 2011 12:19:52   system.xml

515712 KB total (479308 KB free)
```

通过以上信息可以看出，待升级的启动文件 soft-version2.bin 已保存到 Master 设备的 Flash 中。

查看待升级的启动文件 soft-version2.bin 已保存到 Slave2 的 Flash 中。

```
<IRF> dir slot2#flash:/
Directory of slot2#flash:/

   0     -rw-      6085  May 29 2010 11:38:45   config.cfg
   1     -rw-     10518  Apr 26 2011 12:45:05   logfile.log
   2     -rw-  19057904  Apr 26 2011 14:24:11   soft-version1.bin
   3     -rw-  19077744  Apr 26 2011 14:13:46   soft-version2.bin
   4     drw-         -  Apr 26 2011 12:00:33   seclog
   5     -rw-       287  Apr 26 2011 12:19:52   system.xml

515712 KB total (479308 KB free)
```

通过以上信息可以看出，待升级的启动文件 soft-version2.bin 已保存到 Slave2 的 Flash 中。

查看待升级的启动文件 soft-version2.bin 已保存到 Slave3 的 Flash 中。

```
<IRF> dir slot3#flash:/
Directory of slot3#flash:/

   0     -rw-      6085  May 29 2010 11:38:45   config.cfg
   1     -rw-     10518  Apr 26 2011 12:45:05   logfile.log
   2     -rw-  19057904  Apr 26 2011 14:24:11   soft-version1.bin
   3     -rw-  19077744  Apr 26 2011 14:13:46   soft-version2.bin
   4     drw-         -  Apr 26 2011 12:00:33   seclog
   5     -rw-       287  Apr 26 2011 12:19:52   system.xml

515712 KB total (479308 KB free)
```

通过以上信息可以看出，待升级的启动文件 soft-version2.bin 已保存到 Slave3 的 Flash 中。

(4) 逐一查看待升级的启动文件是否已保存到所有 IRF 成员设备的 Flash 中（如未保存，则不能采用 ISSU 方式进行启动文件升级）。

查看待升级的启动文件 soft-version2.bin 已保存到 Master 设备的 Flash 中。

```
<IRF> dir
Directory of flash:/

   0     -rw-      6085  May 29 2010 11:38:45   config.cfg
   1     -rw-     10518  Apr 26 2011 12:45:05   logfile.log
   2     -rw-  19701664  Apr 26 2011 14:24:11   soft-version1.bin
   3     -rw-  19728552  Apr 26 2011 14:13:46   soft-version2.bin
   4     drw-         -  Apr 26 2011 12:00:33   seclog
   5     -rw-       287  Apr 26 2011 12:19:52   system.xml

126592 KB total (86796 KB free)
```

通过以上信息可以看出，待升级的启动文件 soft-version2.bin 已保存到 Master 设备的 Flash 中。

查看待升级的启动文件 soft-version2.bin 已保存到 Slave2 的 Flash 中。

```
<IRF> dir slot2#flash:/
Directory of slot2#flash:/

   0     -rw-      6085  May 29 2010 11:38:45   config.cfg
   1     -rw-     10518  Apr 26 2011 12:45:05   logfile.log
   2     -rw-  19701664  Apr 26 2011 14:24:11   soft-version1.bin
   3     -rw-  19728552  Apr 26 2011 14:13:46   soft-version2.bin
   4     drw-         -  Apr 26 2011 12:00:33   seclog
   5     -rw-       287  Apr 26 2011 12:19:52   system.xml

126592 KB total (86796 KB free)
```

通过以上信息可以看出，待升级的启动文件 soft-version2.bin 已保存到 Slave2 的 Flash 中。

查看待升级的启动文件 soft-version2.bin 已保存到 Slave3 的 Flash 中。

```
<IRF> dir slot3#flash:/
Directory of slot3#flash:/

   0     -rw-      6085  May 29 2010 11:38:45   config.cfg
   1     -rw-     10518  Apr 26 2011 12:45:05   logfile.log
   2     -rw-  19701664  Apr 26 2011 14:24:11   soft-version1.bin
   3     -rw-  19728552  Apr 26 2011 14:13:46   soft-version2.bin
   4     drw-         -  Apr 26 2011 12:00:33   seclog
   5     -rw-       287  Apr 26 2011 12:19:52   system.xml
```

```
126592 KB total (86796 KB free)
```

通过以上信息可以看出，待升级的启动文件 soft-version2.bin 已保存到 Slave3 的 Flash 中。

(5) 保存当前配置。

```
<IRF> save
The current configuration will be written to the device. Are you sure? [Y/N]:y
Please input the file name(*.cfg)[flash:/config.cfg]
(To leave the existing filename unchanged, press the enter key):
flash:/config.cfg exists, overwrite? [Y/N]:y
 Validating file. Please wait....
 Saved the current configuration to mainboard device successfully.
Slot 2:
 Save next configuration file successfully.
Slot 3:
 Save next configuration file successfully.
 Configuration is saved to device successfully.
```

通过以上显示信息可以看出，当前运行配置已成功保存到 IRF 各成员设备的配置文件中。

3. 查看新启动文件与当前启动文件的版本兼容情况

查看新启动文件 soft-version2.bin 与当前版本启动文件的版本兼容情况后，可确定具体采用何种 ISSU 升级方式。

```
<IRF> display version comp-matrix file soft-version2.bin
```

执行 **display version comp-matrix file** 命令后，显示信息如下，具体显示信息请以设备实际情况为准。

(1) 兼容版本的显示

```
Number of Matrices in Table = 1
Matrix for S5500-HI

Running Version: version1
Version Compatibility List:
version2 (Compatible)
```

以上显示信息表明，soft-version2.bin与当前版本完全兼容，需要使用兼容版本的升级步骤进行ISSU升级。具体配置请参见 2.2.3 兼容版本的ISSU升级。

(2) 不兼容版本的显示

```
Number of Matrices in Table = 1
Matrix for S5500-HI

Running Version: version1
Version Compatibility List:
Version2 (Incompatible)
```

以上显示信息表明，soft-version2.bin与当前版本不兼容，需要使用不兼容版本的升级步骤进行ISSU升级。具体配置请参见 2.2.4 不兼容版本的ISSU升级。

2.2.3 兼容版本的ISSU升级

开始 ISSU 升级，先升级指定 Slave 设备（升级结束后的新 Master，此例中为 Slave2）。

```
<IRF> system-view
[IRF] issu load file soft-version2.bin slot 2
This command will begin ISSU, and the specified board will reboot and be upgraded. Please
save the current running configuration first; otherwise, the configuration may be
lost.Continue? [Y/N]:y
```

Slave2 重启完成以后，查看 Slave2 的启动文件是否为 soft-version2.bin。

```
[IRF] display boot-loader
Slot 1
The current boot app is:  flash:/soft-version1.bin
The main boot app is:     flash:/soft-version1.bin
The backup boot app is:   flash:/
Slot 2
The current boot app is:  flash:/soft-version2.bin
The main boot app is:     flash:/soft-version2.bin
The backup boot app is:   flash:/
Slot 3
The current boot app is:  flash:/soft-version1.bin
The main boot app is:     flash:/soft-version1.bin
The backup boot app is:   flash:/
```

通过以上显示信息可以看出，Slave2 重启完成以后，启动文件已经升级为 soft-version2.bin。

手工触发 IRF 系统中 Master 设备重启。

```
[IRF] issu run switchover slot 2
Master will reboot, switch the specified board to master and update the line card. Continue?
[Y/N]:y
```

此例中 Master 的成员编号为 1，Master 设备重启完成以后（原 Master 设备在 IRF 系统中的角色变为 Slave），IRF 中的 Slave 设备重新进行 IRF 选举，Slave2 的优先级高于 Slave3，在 IRF 中选举获胜倒换为新的 Master 设备。

确认 ISSU 升级，取消启动文件的自动回滚功能。

```
[IRF] issu accept slot 2
```

对尚未升级的成员设备进行升级。（分别升级成员设备 1 和 3）

```
[IRF] issu commit slot 1
The specified board will reboot and be upgraded. Continue? [Y/N]:y
[IRF] issu commit slot 3
The specified board will reboot and be upgraded. Continue? [Y/N]:y
```

至此，IRF 中所有成员设备都使用新版本的启动文件运行，IRF 升级完成。

查看设备上当前使用的启动文件是否为 soft-version2.bin。

```
[IRF] display boot-loader
Slot 1
The current boot app is:  flash:/soft-version2.bin
The main boot app is:     flash:/soft-version2.bin
The backup boot app is:   flash:/
Slot 2
The current boot app is:  flash:/soft-version2.bin
The main boot app is:     flash:/soft-version2.bin
The backup boot app is:   flash:/
Slot 3
The current boot app is:  flash:/soft-version2.bin
The main boot app is:     flash:/soft-version2.bin
The backup boot app is:   flash:/
```

2.2.4 不兼容版本的ISSU升级

开始 ISSU 升级，先升级指定 Slave 设备（升级结束后的新 Master，此例中先升级 Slave2）。

```
<IRF> system-view
[IRF] issu load file soft-version2.bin slot 2 force
```

```
This command will begin ISSU, and the specified board will reboot and be upgraded. Please
save the current running configuration first; otherwise, the configuration may be
lost.Continue? [Y/N]: y
```

Slave2 重启完成以后，对其余尚未升级的 IRF 成员设备一次性全部进行重启升级。

```
[IRF] issu run switchover slot 2
Master will reboot, switch the specified board to master and update the line card. Continue?
[Y/N]:y
```

至此，ISSU 升级过程结束，IRF 升级完成。

查看设备上当前使用的启动文件是否为 soft-version2.bin。

```
[IRF] display boot-loader
Slot 1
The current boot app is:  flash:/soft-version2.bin
The main boot app is:     flash:/soft-version2.bin
The backup boot app is:   flash:/
Slot 2
The current boot app is:  flash:/soft-version2.bin
The main boot app is:     flash:/soft-version2.bin
The backup boot app is:   flash:/
Slot 3
The current boot app is:  flash:/soft-version2.bin
The main boot app is:     flash:/soft-version2.bin
The backup boot app is:   flash:/
```

目 录

1 设备管理

说明

本章节各配置任务互相独立，均为设备的可选配置，配置时没有先后顺序要求。

1.1 设备管理简介

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重启设备、定时重启设备、配置设备的温度告警门限等功能。

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*	可选 缺省情况下，设备名称为**H3C**

1.3 配置系统时间

1.3.1 系统时间的配置

系统时间是系统信息时间戳显示的时间。该时间由配置的相对时间、时区和夏令时三个参数运算之后联合决定，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。

表1-2 配置系统时间

操作	命令	说明
配置时间和日期	**clock datetime** *time date*	可选 该命令在用户视图下执行
进入系统视图	**system-view**	-

操作		命令	说明
配置系统所在的时区		**clock timezone** *zone-name* { **add** | **minus** } *zone-offset*	可选 缺省情况下，本地时区采用UTC（Coordinated Universal Time，国际协调时间）时区
配置夏令时	设置从“起始日期”的“起始时间”到“结束日期”的“结束时间”这个时间段内采用夏令时制，夏令时间要比设备的当前时间增加“*add-time*”	**clock summer-time** *zone-name* **one-off** *start-time start-date end-time end-date add-time*	二者选其一 缺省情况下，设备上没有配置夏令时，采用UTC时间
	设置设备重复采用夏令时制	**clock summer-time** *zone-name* **repeating** *start-time start-date end-time end-date add-time*	

注意

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。如果设备时间不正确，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。NTP 的配置请参见“网络管理和监控配置指导”中的“NTP”。

1.3.2 系统时间的配置效果

系统时间由**clock datetime**、**clock timezone**和**clock summer-time**三条命令联合决定。如果以上三条命令都不配置，则**display clock**命令显示的为原系统时间。如果把三条以上命令任意组合进行配置，配置后的系统时间请参见 表 1-3。表中配置列各参数的含义为：

- 1：表示执行 **clock datetime** 命令配置了时间 *date-time*；
- 2：表示执行 **clock timezone** 命令配置了时区参数，时间偏移量为 *zone-offset*；
- 3：表示执行 **clock summer-time** 命令配置了夏令时参数，时间偏移量为 *summer-offset*；
- [1]：表示 **clock datetime** 命令是可选配置，可执行也可不执行。

表中举例默认原系统时间为 2005/1/1 1:00:00。

表1-3 系统时间配置示例表

配置	配置后的系统时间	举例
1	*date-time*	配置：clock datetime 1:00 2007/1/1 配置后的系统时间：01:00:00 UTC Mon 01/01/2007
2	原系统时间±"*zone-offset*"	配置：clock timezone zone-time add 1 配置后的系统时间：02:00:00 zone-time Sat 01/01/2005
1、2	"*date-time*"±"*zone-offset*"	配置：clock datetime 2:00 2007/2/2和clock timezone zone-time add 1 配置后的系统时间：03:00:00 zone-time Fri 02/02/2007

配置	配置后的系统时间	举例
2、1	*date-time*	配置：clock timezone zone-time add 1和clock datetime 3:00 2007/3/3 配置后的系统时间：03:00:00 zone-time Sat 03/03/2007
3	原系统时间不在夏令时段内，则为原系统时间	配置：clock summer-time ss one-off 1:00 2006/1/1 1:00 2006/8/8 2 配置后的系统时间：01:00:00 UTC Sat 01/01/2005
	原系统时间在夏令时段内，则为原系统时间+”*summer-offset*”	配置：clock summer-time ss one-off 00:30 2005/1/1 1:00 2005/8/8 2 配置后的系统时间：03:00:00 ss Sat 01/01/2005 如果原系统时间+”*summer-offset*”不在夏令时段内，则配置后的系统时间为原系统时间。之后，若取消夏令时配置，则系统时间会被减少”*summer-offset*”
1、3	*date-time*不在夏令时段内，则为*date-time*	配置：clock datetime 1:00 2007/1/1和clock summer-time ss one-off 1:00 2006/1/1 1:00 2006/8/8 2 配置后的系统时间：01:00:00 UTC Mon 01/01/2007
	*date-time*在夏令时段内，则为“*date-time*”+”*summer-offset*”	配置：clock datetime 8:00 2007/1/1和clock summer-time ss one-off 1:00 2007/1/1 1:00 2007/8/8 2 配置后的系统时间：10:00:00 ss Mon 01/01/2007 如果“*date-time*”+”*summer-offset*”不在夏令时段内，则配置后的系统时间为“*date-time*”。之后，若取消夏令时配置，则系统时间会被减少”*summer-offset*”
[1]、3、1	*date-time*不在夏令时段内，则为*date-time*	配置：clock summer-time ss one-off 1:00 2007/1/1 1:00 2007/8/8 2和clock datetime 1:00 2008/1/1 配置后的系统时间：01:00:00 UTC Tue 01/01/2008
	*date-time*在夏令时段内，再根据“*date-time*”-”*summer-offset*”的值是否在夏令时段内来判断。如果该值不在夏令时段内，则为“*date-time*”-”*summer-offset*”；如果在夏令时段内，则为date-time	配置：clock summer-time ss one-off 1:00 2007/1/1 1:00 2007/8/8 2和clock datetime 1:30 2007/1/1 配置后的系统时间：23:30:00 UTC Sun 12/31/2006
		配置：clock summer-time ss one-off 1:00 2007/1/1 1:00 2007/8/8 2和clock datetime 3:00 2007/1/1 配置后的系统时间：03:00:00 ss Mon 01/01/2007
2、3或者 3、2	如果原系统时间±"*zone-offset*"的值不在夏令时段内，则为原系统时间±"*zone-offset*"	配置：clock timezone zone-time add 1和clock summer-time ss one-off 1:00 2007/1/1 1:00 2007/8/8 2 配置后的系统时间：02:00:00 zone-time Sat 01/01/2005
	如果原系统时间±"*zone-offset*"的值在夏令时段内，则为原系统时间±"*zone-offset*"+”*summer-offset*”	配置：clock timezone zone-time add 1和clock summer-time ss one-off 1:00 2005/1/1 1:00 2005/8/8 2 配置后的系统时间：04:00:00 ss Sat 01/01/2005
1、2、3或者1、3、2	如果"*date-time*"±"*zone-offset*"的值不在夏令时段内，则为"*date-time*"±"*zone-offset*"	配置：clock datetime 1:00 2007/1/1、clock timezone zone-time add 1和clock summer-time ss one-off 1:00 2008/1/1 1:00 2008/8/8 2 配置后的系统时间：02:00:00 zone-time Mon 01/01/2007

配置	配置后的系统时间	举例
	如果"*date-time*"±"*zone-offset*"的值在夏令时段内，则为"*date-time*"±"*zone-offset*"+"*summer-offset*"	配置：clock datetime 1:00 2007/1/1、clock timezone zone-time add 1和clock summer-time ss one-off 1:00 2007/1/1 1:00 2007/8/8 2 配置后的系统时间：04:00:00 ss Mon 01/01/2007
[1]、2、3、1或者[1]、3、2、1	*date-time*不在夏令时段内，则为*date-time*	配置：clock timezone zone-time add 1、clock summer-time ss one-off 1:00 2008/1/1 1:00 2008/8/8 2和clock datetime 1:00 2007/1/1 配置后的系统时间：01:00:00 zone-time Mon 01/01/2007
	*date-time*在夏令时段内，再根据“*date-time*”-”*summer-offset*”的值是否在夏令时段内来判断。如果不在夏令时段内，则为“*date-time*”-”*summer-offset*”；如果在夏令时段内，则为*date-time*	配置：clock timezone zone-time add 1、clock summer-time ss one-off 1:00 2008/1/1 1:00 2008/8/8 2和clock datetime 1:30 2008/1/1 配置后的系统时间：23:30:00 zone-time Mon 12/31/2007
		配置：clock timezone zone-time add 1、clock summer-time ss one-off 1:00 2008/1/1 1:00 2008/8/8 2和clock datetime 3:00 2008/1/1 配置后的系统时间：03:00:00 ss Tue 01/01/2008

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**	可选 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、进行登录验证以及开始交互配置时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：

(1) 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”，则退出认证或登录过程。“Y”和“N”不区分大小写。

(2) MOTD（Message Of The Day，每日提示）欢迎信息。在 legal 欢迎信息后，login 欢迎信息前显示。

(3) 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。

(4) 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 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**	-
配置登录进入用户视图时的欢迎信息（Modem登录方式适用）	**header incoming** *text*	可选
配置登录验证时的欢迎信息	**header login** *text*	可选
配置登录终端界面前的授权信息	**header legal** *text*	可选
配置登录进入用户视图时的欢迎信息	**header shell** *text*	可选
配置登录终端界面前的欢迎信息	**header motd** *text*	可选

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，输入内容的起始符和结束符必须相同，这两字符不作为欢迎信息的内容。此时包括命令关键字、起始符和结束符在内，一共可以输入 510 个字符。在该方式下输入欢迎信息时不能回车（按<Enter>键）。例如：用户要设置的欢迎信息为“Have a nice day.”：

```
<System> system-view
[System] header shell %Have a nice day.%
```

(2) 多行输入

该方式下，通过回车键可以将欢迎信息分多行输入，此时欢迎信息一共可以长达 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：用户要设置的欢迎信息为“Have a nice day. Please input the Password.”：

```
<System> system-view
[System] header shell
Please input banner content, and quit with the character '%'. ——系统提示
Have a nice day.
Please input the Password.%
```

- 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：用户要设置的欢迎信息为“Have a nice day. Please input the Password.”：

```
<System> system-view
[System] header shell A
Please input banner content, and quit with the character 'A'.——系统提示
Have a nice day.
Please input the Password.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：用户要设置的欢迎信息为“Have a nice day. Please input the Password.”：

```
<System> system-view
[System] header shell AHave a nice day.
Please input banner content, and quit with the character 'A'.——系统提示
Please input the Password.A
```

1.6 配置系统异常时的处理方式

当系统检测到设备软件运行异常时，支持两种处理方式：

- **reboot**：直接自动重启故障的设备来进行恢复。
- **maintain**：保持当前状态，系统不会自动采取任何恢复措施。此时需要手工进行恢复操作。某些系统异常可能较难复现，或者异常时打印的一些提示设备重启后会丢失，此时，使用该方式可以保持异常时的状态，以便进行问题定位和修复。但该方式需要手工修复，比如手工重启。

表1-6 配置系统异常时的处理方式

操作	命令	说明
进入系统视图	**system-view**	-
配置设备系统异常时的处理方式	**system-failure** { **maintain** | **reboot** }	可选 缺省情况下，系统异常时的处理方式为**reboot**

说明

在 IRF 系统中，系统异常处理方式仅对 Master 设备生效。

1.7 配置设备重启

当设备运行出现故障时，用户可以根据实际情况，通过重启设备来排除故障。

重启的方式有三种：

- 通过断电后重新上电立即重启设备（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或者硬件损坏。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，主要用于远程维护时，可以远程重启设备，而不需要到设备所在地进行断电/供电重启。

注意

- 重新启动会导致业务中断，请谨慎使用。
- 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。（**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”）

说明

- 当多次使用 **schedule reboot at** 或者 **schedule reboot delay** 命令配置不同的重启时间时，最新的配置生效。
- 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，或者断电后重新上电，系统将自动使用备用启动文件重启。
- 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。
- 在 Master 设备上使用 **reboot** 命令：当指定 **slot** 参数时，IRF 中相应编号的成员设备被重启；当不指定 **slot** 参数时，则会重启 IRF 中的所有设备。

表1-7 通过命令行立即重启设备

操作	命令	说明
立即重启指定设备或所有成员设备	**reboot** [**slot** *slot-number*]	必选 在IRF中，**slot**参数表示重启某个成员设备，如果不输入则默认重启整个IRF 该命令在用户视图下执行

表1-8 通过命令行定时重启设备

操作	命令	说明
开启所有成员设备定时重启功能，并指定重启的具体时间和日期	**schedule reboot at** *hh:mm* [*date*]	二者必选其一 缺省情况下，设备定时重启功能处于关闭状态 两命令均在用户视图下执行 使用该方式配置定时重启后，又执行**clock datetime**、**clock summer-time**或**clock timezone**命令调整了系统时间，则定时重启配置将自动取消
开启所有成员设备的定时重启功能，并设定等待时延	**schedule reboot delay** { *hh:mm* | *mm* }	

1.8 配置定时执行任务功能

1.8.1 定时执行任务功能简介

定时执行任务功能是指通过配置，设备可以在指定时刻或延迟指定时长以后，自动执行一个或一组命令的功能。启用此功能以后，设备能够在无人值守的情况下完成某些操作或配置。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。

当配置了定时执行任务之后，设备每分钟遍历一次已配置的任务列表，如果发现有任务的定时时间到了，设备将自动执行该任务。

1.8.2 配置定时执行任务

配置定时执行任务有以下两种方式：

对比项	配置定时执行任务（方式一）	配置定时执行任务（方式二）
配置复杂程度	简单 只涉及**schedule job**命令	复杂 涉及**job**、**view**、**time**三条命令
能否同时配置多个任务	不能	可以
同一任务中能否执行多条命令	不能 多次使用**schedule job**命令用来定时执行不同的命令时，最新的配置生效	可以 使用**time**命令可以指定在不同的时间点来执行不同的命令
支持的视图（*view-name*参数的取值）	只能是shell（表示用户视图）和system（表示系统视图）	系统支持的所有视图，其中用monitor表示用户视图

对比项	配置定时执行任务（方式一）	配置定时执行任务（方式二）
支持的命令范围（*command*参数的取值）	只能是用户视图或系统视图下的命令	对应*view-name*下的任意命令
是否支持循环执行	不支持	支持
是否支持配置保存	不支持	支持

说明

- 如果设备系统时间不正确，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”。
- *command* 表示的命令行必须是设备上可成功执行的命令行，并且要求命令行是 *view-name* 视图下的命令，由用户保证配置的正确性，否则，命令行不能自动被执行。
- 指定命令执行时不进行信息交互。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。
- 对于切换用户操作界面的命令（如 **telnet**、**ftp**、**ssh2** 等）、切换视图的命令（如 **system-view**、**quit** 等）以及修改执行命令用户状态的命令（如 **super** 命令等），自动执行命令后当前用户的操作界面、命令视图和用户状态不变。
- 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）。

1. 配置定时执行任务（方式一）

表1-9 配置定时执行任务（方式一）

操作	命令	说明
在指定时间执行指定命令	**schedule job at** *time* [*date*] **view** *view-name command*	二者必选其一 该命令在用户视图下执行 • 多次执行 **schedule job** 命令时，只有最新的配置生效 • 使用该方式配置定时执行功能后，又执行 **clock datetime**、**clock summer-time** 或 **clock timezone** 命令调整了系统时间，则定时执行配置将自动取消
在指定延时后执行指定命令	**schedule job delay** *time* **view** *view-name command*	

2. 配置定时执行任务（方式二）

表1-10 配置定时执行任务（方式二）

操作	命令	说明
进入系统视图	**system-view**	-
创建定时执行任务，并进入定时执行任务视图	**job** *job-name*	必选
配置执行指定命令所在的视图	**view** *view-name*	必选 每个定时执行任务只能指定一个视图
在指定时间点执行指定任务	**time** *time-id* **at** *time date* **command** *command*	二者必选其一 修改系统时间，不会影响该命令的配置和执行
	time *time-id* { **one-off** | **repeating** } **at** *time* [**month-date** *month-day* | **week-day** *week-daylist*] **command** *command*	
延迟指定时间执行指定任务	**time** *time-id* { **one-off** | **repeating** } **delay** *time* **command** *command*	

需要注意的是：

- 每个定时执行任务只能包含一个视图，该定时任务中所有命令都将在此视图下被执行。若多次执行 **view** 命令指定了不同的视图，则最新的配置生效。
- 视图必须是设备当前支持的视图，而且是视图的完整形式，不能使用缩写。常用的有：用户视图对应的 *view-name* 为 monitor，系统视图对应的 *view-name* 为 system，以太网接口视图对应的 *view-name* 为 GigabitEthernetX/X/X 或 Ten-GigabitEthernetX/X/X，VLAN 接口视图对应的 *view-name* 为 Vlan-interfacex 等。
- 一个定时执行任务中最多可以配置 10 条命令（对应 10 个 *time-id*）。如果多于 10 条，请把这个任务拆分为多个任务。
- *time-id* 在同一个任务中必须唯一。如果新执行的 time at 命令指定的 *time-id* 和已有配置的 *time-id* 值相同，则新配置会覆盖旧配置。

1.9 配置节能功能

1.9.1 使能节能功能

设备节能主要体现在两个方面：控制设备上指示灯亮/灭以及控制以太网接口的节能状态。

- 当没有使能节能功能时：设备上所有灯都正常亮、灭、闪烁，用户可以通过灯的亮、灭、闪烁来判断设备物理上是否存在故障；所有以太网接口的节能功能是否使能由设备上的当前配置来决定。
- 使能节能功能后：设备上指示灯的亮/灭将根据需要来控制，所有以太网接口的节能功能会自动使能，从而达到节能的效果。

表1-11 使能节能功能

操作	命令	说明

操作	命令	说明
进入系统视图	**system-view**	-
使能节能功能	**save-power enable**	必选 缺省情况下，节能功能处于关闭状态

1.9.2 切换节能状态

使能节能功能后，设备可能处于以下状态中的一种：

- 节能休眠状态（**sleep**）：处于该状态的设备会强制关闭除 SYS 灯以外的面板上的所有灯，并自动使能所有以太网端口的节能功能；
- 节能唤醒状态（**wake**）：处于该状态的设备上的所有灯仍然正常亮、灭、闪烁，只是自动使能所有以太网端口的节能功能。

节能状态的切换有两种触发方式：

- 自动方式。当设备处于节能休眠状态时，只要用户一按<Mode>按钮或者通过 Console 连接和设备之间有报文交互，则设备认为用户就在设备附近，需要恢复设备上指示灯的正常亮/灭以便用户了解设备的物理状态，从而设备会立即切换到节能唤醒状态；反之，当设备处于节能唤醒状态，且在 *time* 时间内（*time* 由 **save-power delay-timer** 命令设置）用户没有按<Mode>按钮并且没有通过 Console 连接和设备之间有报文交互，则设备会切换到节能休眠状态以便达到更节能的效果。
- 手动方式。使用该方式用户在不需要操作按钮也不需要等待 *time* 时间的情况下，可以通过命令行手工实现节能状态的快速切换。

表1-12 自动切换节能状态

操作	命令	说明
设置设备从节能唤醒状态切换到节能休眠状态的时间间隔	**save-power delay-timer** *time*	可选 缺省情况下，设备从节能唤醒状态切换到节能休眠状态的时间间隔为15秒

表1-13 手动切换节能状态

操作	命令	说明
手工强制切换设备的节能状态	**save-power mode { sleep | wake }**	可选 本命令在用户视图下执行

1.10 配置端口状态检测定时器

某些协议模块在特定情况下会自动关闭某个端口，比如当使能了 BPDU 保护功能的端口收到配置消息时，生成树模块将自动关闭该端口。此时，可以配置一个端口状态检测定时器。当定时器超时，并且该端口仍处于关闭状态，协议模块则自动取消关闭动作，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*	可选 缺省情况下，端口状态检测定时器时长为30秒

1.11 配置设备的温度告警门限

通过以下配置任务，用户可以根据实际应用的需要设置不同的温度告警门限，来监控设备上不同位置温度传感器的温度。

设备支持以下几个温度告警门限：低温告警门限、一般级（Warning）高温告警门限、严重级（Alarm）高温告警门限、关断级（Shutdown）高温告警门限。

- 如果温度低于低温告警门限，系统会生成日志信息和告警信息提示用户，以便用户及时进行处理；
- 如果温度高于 Warning 高温门限，系统会生成日志信息和告警信息提示用户，以便用户及时进行处理；
- 如果温度高于 Alarm 高温门限，系统反复输出日志信息和告警信息提示用户；
- 如果温度高于（Shutdown）高温告警门限，系统会生成日志信息和告警信息提示用户并且设备会自动关闭。

说明

关断级（Shutdown）高温告警门限不支持用户配置。

表1-15 配置设备的温度告警门限

操作	命令	说明
进入系统视图	**system-view**	-
配置指定成员设备的各温度告警门限	**temperature-limit slot** *slot-number* { **hotspot** | **inflow** } *sensor-number lowerlimit warninglimit* [*alarmlimit*]	可选 缺省情况下，设备的温度告警门限值具体请参见表1-16 高温告警门限必须大于低温告警门限；Alarm高温告警门限必须大于Warning高温告警门限。

表1-16 设备温度告警门限缺省值

设备型号	传感器	低温告警值	一般级高温告警门限	严重级高温告警门限	关断级高温告警门限
S5500-28SC-HI/ S5500-52SC-HI	Inflow 1	0	55	65	N/A
	hotspot 1	0	55	65	N/A
S5500-34C-HI	Inflow 1	0	67	72	N/A
	hotspot 1	0	77	82	N/A
S5500-58C-HI	Inflow 1	0	59	64	N/A
	hotspot 1	0	74	79	N/A
S5500-34F-HI	Inflow 1	0	56	61	N/A
	hotspot 1	0	69	72	N/A
S5500-34C-PWR-HI	Inflow 1	0	62	66	N/A
	hotspot 1	0	76	80	N/A
	hotspot 2	0	115	130	N/A
S5500-58C-PWR-HI	Inflow 1	0	64	69	N/A
	hotspot 1	0	77	82	N/A
	hotspot 2	0	115	130	N/A

1.12 清除当前系统中不使用的16bit接口索引

NMS 软件要求设备能够提供统一的 16bit 的接口索引，同时要求接口索引稳定，即同一设备中接口的名字与接口的索引保持一一对应的关系。

为了尽量保证接口索引的稳定性，当删除逻辑接口时，系统会保存该接口的 16bit 接口索引，以保证重新创建该接口时其索引值不变。

创建或者删除大批量不同类型的逻辑口，可能会耗尽接口索引，导致创建接口失败。为了避免这种情况，用户可以在用户视图下执行以下操作，清除当前系统中保存的但不使用的 16bit 接口索引。

执行该操作后：

- 对于重新创建的接口，接口的新的索引不能保证与原来的索引一致。
- 对于系统中已经正常存在的接口，不会引起其索引值的改变。

表1-17 清除当前系统中不使用的 16bit 接口索引

操作	命令	说明
清除所有成员设备当前系统中保存的但不使用的16bit索引	**reset unused porttag**	必选 该命令在用户视图下执行

注意

执行该命令时需要得到用户的确认。若用户在 30 秒之内没有确认操作，或者用户输入字符“N”否定了本次操作，则本命令退出执行。

1.13 配置密码修复功能

当用户忘记用户级别切换密码（**super password** 命令中配置的密码）或者忘记登录认证密码，会导致无法操作或登录设备。为了保证用户能够对设备进行正常登录、配置，用户可进入 Bootrom 扩展段，设置设备下次启动时采取何种方式（跳过配置文件、删除 **super password** 命令中配置的密码或恢复设备的出厂配置）。密码修复功能与 Bootrom 菜单中选项的关系，具体请参见版本说明书。

在丢失密码的情况下，可通过如下操作进入 Bootrom 扩展段菜单：

- 通过 Console 口连接设备、并对设备进行断电重启。
- 在设备启动过程中，根据提示按<Ctrl+B>进入 Bootrom 菜单。

表1-18 配置密码修复功能

操作	命令	说明
进入系统视图	**system-view**	-
开启密码修复功能	**password-recovery enable**	可选 缺省情况下，密码修复功能处于开启状态
关闭密码修复功能	**undo password-recovery enable**	

1.14 可插拔接口模块的识别与诊断

说明

是否支持可插拔接口模块以及模块类型的支持情况与设备的型号有关，请以设备的实际情况为准。

1.14.1 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等，在模块调测（调试、测试）过程中被写入到存储器件中，包括序列号、调测日期、模块生产厂商名称等信息。

表1-19 识别可插拔接口模块信息

操作	命令
显示可插拔接口模块的主要特征参数	**display transceiver interface** [*interface-type interface-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示可插拔接口模块的电子标签信息	**display transceiver manuinfo interface** [*interface-type interface-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

说明

电子标签信息的显示与可插拔接口模块的支持情况有关，请以实际情况为准。

1.14.2 诊断可插拔接口模块

系统提供故障告警信息标志可插拔接口模块的故障来源，以便诊断和解决故障。同时，还提供了可插拔接口模块的数字诊断功能，其原理主要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1-20 诊断可插拔接口模块

操作	命令
显示可插拔接口模块的当前故障告警信息	**display transceiver alarm interface** [*interface-type interface-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示可插拔接口模块的数字诊断参数的当前测量值	**display transceiver diagnosis interface** [*interface-type interface-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

说明

数字诊断参数的显示与可插拔接口模块的支持情况有关，请以实际情况为准。

1.14.3 关闭可插拔模块告警信息开关

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1-21 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

1.15 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1-22 设备管理显示和维护

操作	命令
显示系统版本信息	**display version** [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示系统当前的时间和日期	**display clock** [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示或保存系统当前多个功能模块运行的统计信息	**display diagnostic-information** [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示CPU占用率的统计信息	**display cpu-usage** [**slot** *slot-number* [**cpu** *cpu-number*]] [**|** { **begin** | **exclude** | **include** } *regular-expression*] **display cpu-usage** *entry-number* [*offset*] [**verbose**] [**slot** *slot-number* [**cpu** *cpu-number*]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
以图形方式显示CPU占用率统计历史信息	**display cpu-usage history** [**task** *task-id*] [**slot** *slot-number* [**cpu** *cpu-number*]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示设备的硬件信息	**display device** [[**slot** *slot-number* [**subslot** *subslot-number*]] | **verbose**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示设备的电子标签信息	**display device manuinfo** [**slot** *slot-number* [**subslot** *subslot-number*]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示指定电源的电子标签信息	**display device manuinfo slot** *slot-number* **power** *power-id* [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示设备的温度信息	**display environment** [**slot** *slot-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示设备风扇模块的工作状态	**display fan** [**slot** *slot-number* [*fan-id*]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示设备的内存使用状态	**display memory** [**slot** *slot-number* [**cpu** *cpu-number*]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示设备的电源状态	**display power** [**slot** *slot-number* [*power-id*]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示设备的启动方式	**display reboot-type** [**slot** *slot-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示节能功能是否使能以及所处的节能状态	**display save-power** [**|** { **begin** | **exclude** | **include** } *regular-expression*]

操作	命令
查看定时执行功能的具体配置（针对**schedule job**配置方式）	**display schedule job** [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示设备的重启时间	**display schedule reboot** [**|** { **begin** | **exclude** | **include** } *regular-expression*]
查看定时执行功能的具体配置（针对**job**配置方式）	**display job** [*job-name*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示异常情况下系统的处理方式	**display system-failure** [**|** { **begin** | **exclude** | **include** } *regular-expression*]

在日常维护或系统出现故障时，为了便于问题定位，用户需要查看各个功能模块的运行信息。因为各个功能模块都有其对应的运行信息，所以一般情况下，用户需要逐条运行相应的 **display** 命令。为便于一次性收集更多信息，用户可以在任意视图下执行 **display diagnostic-information** 命令，显示或保存系统当前多个功能模块运行的统计信息。**display diagnostic-information** 命令一次性收集的信息等效于依次执行 **display clock**、**display version**、**display device**、**display current-configuration** 等命令后终端显示的信息。

目 录

1 自动配置

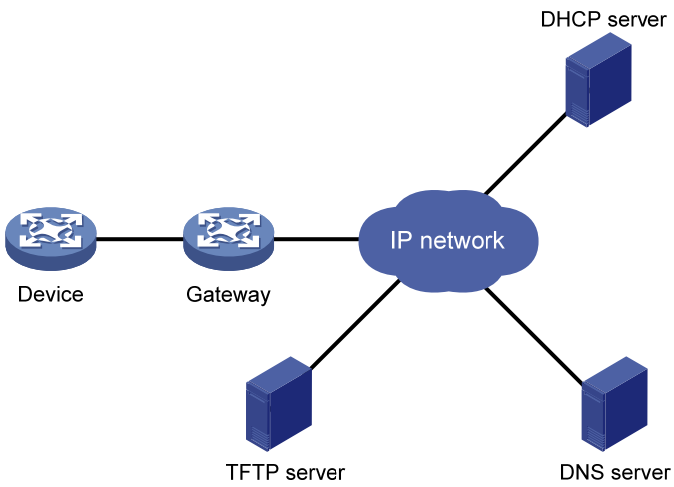
1.1 自动配置简介

自动配置功能是指在设备空配置启动时自动获取并执行配置文件的功能。

自动配置功能简化了网络配置，便于实现对设备的集中管理。目前，企业网面临着这样的问题：设备分布广，维护人员少，网络管理员在每一台设备上进行手工配置的代价巨大。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，从而大大降低了网络管理员的工作量。

1.2 自动配置的典型组网环境

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 IP 地址、DNS 服务器 IP 地址等信息。
- TFTP 服务器：用来保存自动配置过程中设备需要的文件。设备从 TFTP 服务器获取所需的文件，如保存主机 IP 地址和主机名映射关系的主机名文件、设备的配置文件等。
- 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 域名服务器将 TFTP 服务器的域名解析为 TFTP 服务器的 IP 地址。

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，还需要在网关设备上配置 DHCP 中继，并配置路由协议，使得各个服务器和设备之间路由可达。

1.3 自动配置的工作过程

自动配置的基本工作过程如下：

(1) 设备在空配置启动时，系统会自动将处于 up 状态的第一个接口（如果存在处于 up 状态的二层以太网接口，则为缺省 VLAN 对应的虚接口，否则为处于 up 状态的接口编号最小的三层以太网接口）配置为通过 DHCP 方式获得 IP 地址及后续获取配置文件所需要的信息（例如：配置文件名、TFTP 服务器的域名、TFTP 服务器的 IP 地址、DNS 服务器 IP 地址等信息）。

(2) 如果设备成功地从DHCP服务器获取到IP地址及配置文件名等相关信息，则发起TFTP请求，从指定的 TFTP 服务器获取配置文件。如果设备没有获取到相关信息，则在空配置文件的情况下正常启动。

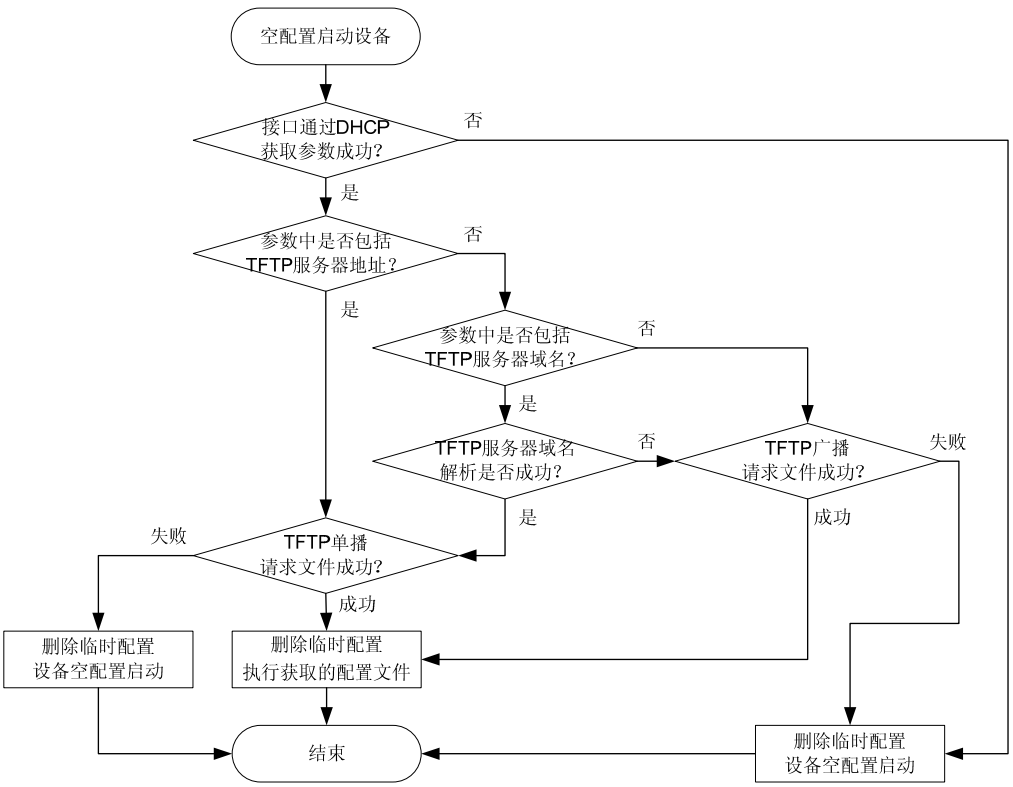
说明

- 自动配置功能在空配置启动的设备上不需要进行任何配置，但若要成功获得配置文件，则需在 DHCP 服务器、DNS 服务器和 TFTP 服务器上配置一些必需的参数。
- 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。

1.3.1 自动配置流程图

自动配置的流程如 图 1-2 所示。

图1-2 自动配置流程图



1.3.2 通过DHCP获取IP地址及相关信息

1. IP地址获取过程

设备在空配置启动时，系统会自动将处于 up 状态的第一个接口（如果存在处于 up 状态的二层以太网接口，则为缺省 VLAN 对应的虚接口，否则为处于 up 状态的接口编号最小的三层以太网接口）配置为通过 DHCP 方式获得 IP 地址，设备通过该接口以广播方式发送 DHCP 请求报文。DHCP 请求报文中的 Option 55 选项指明设备需要从 DHCP 服务器获得哪些信息（如获取自动配置文件需要的配置文件名、TFTP 服务器域名、TFTP 服务器 IP 地址、DNS 服务器 IP 地址等信息）。

经过 DHCP 请求成功获取到 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。

如果获取 IP 地址失败，则设备删除临时配置，在空配置文件的情况下启动。

说明

- 临时配置是指设备空配置启动时在执行自动配置的接口上进行的配置，以及执行的主机名文件中的 **ip host** 命令（**ip host** 命令的具体介绍请参见“三层技术-IP 业务命令参考”中的“IPv4 域名解析”）。删除临时配置就是按照相反顺序执行 **undo** 命令，取消临时配置。
- 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. DHCP服务器上地址池的选择

DHCP 服务器从地址池中选择为客户端分配的 IP 地址和其他网络配置参数。DHCP 的地址池分为两类：

- 动态分配的地址池：该类地址池中包括可供分配的 IP 地址范围，DHCP 服务器从中选取 IP 地址分配给客户端，同时为客户端分配该地址池中其他的网络配置参数。
- 静态绑定的地址池：通过将客户端的 IP 地址与客户端的 MAC 地址或客户端 ID 绑定，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。

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池：

- 不同设备的配置文件都相同时，可以在 DHCP 服务器上配置动态分配的地址池，通过该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 方式登录各个设备，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的地址池，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命令，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

配置静态绑定的地址池时需要指定静态绑定的客户端 ID（设备作为 DHCP 客户端时，采用客户端 ID 作为标识），因此需要首先通过下面的方法获取客户端 ID：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。

1.3.3 从TFTP服务器上获取配置文件

1. 文件类型

设备通过自动配置功能从 TFTP 服务器上获取的文件可以是：

- DHCP 应答报文中 Option 67 或 file 字段指定的配置文件。
- 主机名文件，文件名为“network.cfg”。主机名文件用来保存主机 IP 地址与主机名称的映射关系。主机 IP 地址与主机名称的映射关系使用以下格式进行定义：

ip host *hostname ip-address*

例如，主机名文件可以包括如下内容：

```
ip host host1 101.101.101.101
ip host host2 101.101.101.102
ip host client1 101.101.101.103
ip host client2 101.101.101.104
```

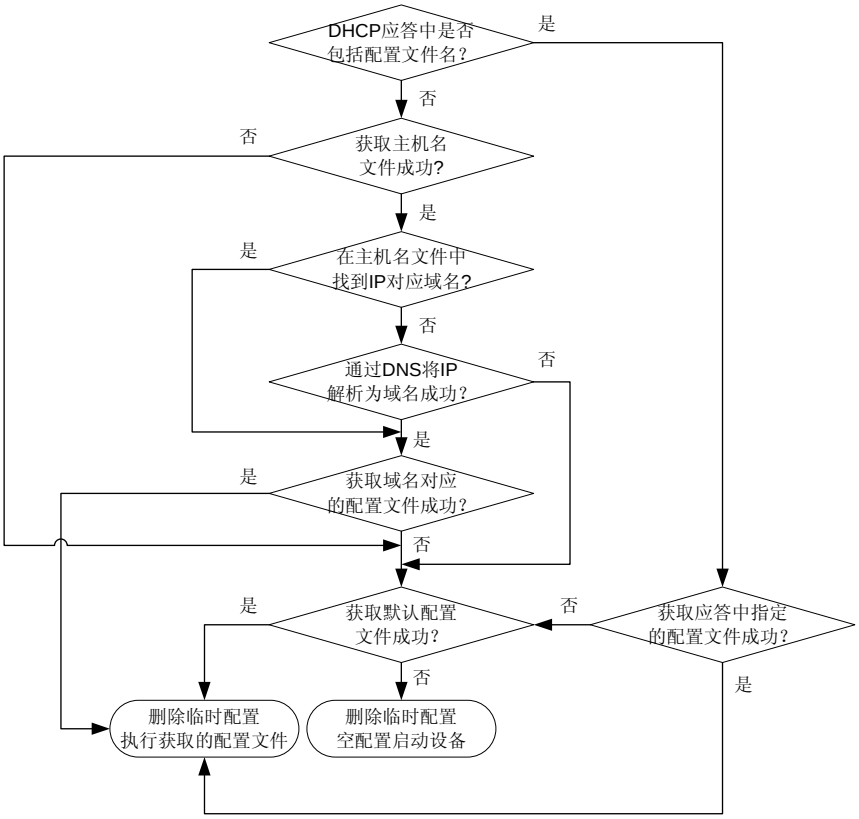
注意

- **ip host** 关键字前必须包括一个空格。
- 主机名文件中保存的主机名称是用户为了更好地管理自动配置而设定的，需要与主机的配置文件名保持一致。该主机名称区别于 DNS 服务器中记录的主机名称，两者可以相同，也可以不相同。

- 设备的主机名对应的配置文件，文件名为“主机名.cfg”。例如，设备的主机名为 aaa，则此配置文件名为“aaa.cfg”。
- 默认配置文件，文件名为“device.cfg”。

2. 获取配置文件

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：

- 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；
- 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，则通过 DNS 服务器获得设备 IP 地址对应的主机名；
- 如果获取指定的配置文件、设备主机名解析或获取主机名对应的配置文件失败，则向 TFTP 服务器请求默认的配置文件。

3. 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：

- 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；
- 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；

- 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。

说明

- 以广播方式发送 TFTP 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，如果该服务器上没有需要的配置文件，配置文件获取失败，设备将删除临时配置，在空配置文件的情况下正常启动。
- 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”。

1.3.4 执行配置文件

成功获得配置文件后，设备将删除临时配置，执行获取到的配置文件。如果获取配置文件失败，设备将删除临时配置，在空配置文件的情况下正常启动。

说明

- 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”。
- 如果配置文件中含有 IRF 相关配置的内容，设备在执行配置文件时，并不会执行这些内容。