H3C MSR 系列路由器

基础配置指导(V7)

新华三技术有限公司
http://www.h3c.com

资料版本：6W204-20190110
产品版本：MSR-CMW710-R0615

前 言

本配置指导主要介绍命令行接口配置、如何登录设备、FTP 和 TFTP 配置、文件系统管理、配置文件管理、设备管理和软件升级。

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

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。
	该图标及其相关描述文字代表无线控制器、无线控制器业务板和有线无线一体化交换机的无线控制引擎设备。
	该图标及其相关描述文字代表无线接入点设备。
	该图标及其相关描述文字代表无线终结单元。
	该图标及其相关描述文字代表无线终结者。
	该图标及其相关描述文字代表无线Mesh设备。
	该图标代表发散的无线射频信号。
	该图标代表点到点的无线射频信号。
	该图标及其相关描述文字代表防火墙、UTM、多业务安全网关、负载均衡等安全设备。
	该图标及其相关描述文字代表防火墙插卡、负载均衡插卡、NetStream插卡、SSL VPN插卡、IPS插卡、ACG插卡等安全插卡。

5. 示例约定

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

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

资料意见反馈

如果您在使用过程中发现产品资料的任何问题，可以通过以下方式反馈：

E-mail：info@h3c.com

感谢您的反馈，让我们做得更好！

目 录

1 CLI

1.1 命令行接口简介

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

设备支持多种方式进入命令行接口界面，比如通过 Console 口/Telnet/SSH 登录设备后进入命令行接口界面等，各方式的详细描述请参见“基础配置指导”中的“登录设备”。设备的命令行接口界面如下所示。

```
******************************************************************************
* Copyright (c) 2004-2018 New H3C Technologies Co., Ltd. All rights reserved.*
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************

<Sysname>
```

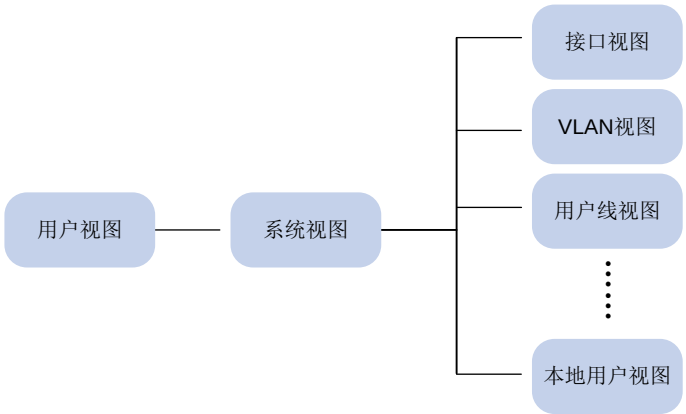
1.2 命令视图

1.2.1 命令视图简介

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

命令视图采用分层结构，如图 1-1 所示。

图1-1 命令视图示意图



- 用户登录设备后，直接进入用户视图。此时屏幕显示的提示符是：<*设备名*>。用户视图下可执行的操作主要包括查看操作、调试操作、文件管理操作、设置系统时间、重启设备、FTP 和 Telnet 操作等。
- 从用户视图可以进入系统视图，此时屏幕显示的提示符是：[*设备名*]。系统视图下能对设备运行参数以及部分功能进行配置，比如配置夏令时、配置欢迎信息、配置快捷键等。
- 在系统视图下输入特定命令，可以进入相应的功能视图，完成相应功能的配置，比如：进入接口视图配置接口参数、进入 VLAN 视图给 VLAN 添加端口、进入用户线视图配置登录用户的属性、创建本地用户并进入本地用户视图配置本地用户的属性等。功能视图下可能还包含子视图，比如 BGP 视图下还包含 BGP IPv4 单播实例视图和 BGP-VPN IPv4 单播实例视图等，请参见各功能模块的详细描述。

想要了解某命令视图下支持哪些命令，请在该命令视图提示符后输入<?>。

说明

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

1.2.2 进入系统视图

表1-1 进入系统视图

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

1.2.3 返回上一级视图

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

- 用户视图下执行 **quit** 命令会中断用户终端与设备之间的当前连接。
- 公共密钥视图下请使用 **peer-public-key end** 命令返回系统视图。

表1-2 返回上一级视图

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

1.2.4 返回用户视图

本命令为用户提供了一种从任意的非用户视图返回到用户视图的快捷方式，而不需要多次执行 **quit** 命令逐级返回。用户也可以直接按组合键<Ctrl+Z>从当前视图返回用户视图。

表1-3 返回用户视图

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

1.3 使用命令行在线帮助

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

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

```
<Sysname> ?
User view commands:
  archive             Archive configuration
  backup              Backup operation
  boot-loader         Software image file management
  bootrom             Update/read/backup/restore bootrom
  cd                  Change current directory
……略……
```

(2) 输入一条命令的关键字，后接以空格分隔的<?>。

如果<?>位置为关键字，则列出全部关键字及其简单描述。例如：

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

如果<?>位置为参数，则列出有关的参数描述。例如：

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

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

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

```
<Sysname> a?
  archive  Archive configuration
<Sysname> display ftp?
  ftp         FTP module
  ftp-server  FTP server information
  ftp-user    FTP user information
```

1.4 命令的undo形式

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

1.5 命令行输入

1.5.1 编辑命令行

编辑命令行时，系统支持如表 1-4 所示的单个按键和如表 1-9 所示的组合键。

表1-4 编辑功能表

按键	功能
普通按键	若编辑缓冲区未满，则插入到当前光标位置，并向右移动光标（命令行下发前会暂时缓存在编辑缓冲区，缓冲区的大小为511个字符，如果编辑缓冲区满，则后续输入的字符无效）
退格键<Backspace>	删除光标位置的前一个字符，光标前移
左光标键<←>	光标向左移动一个字符位置
右光标键<→>	光标向右移动一个字符位置
上光标键<↑>	访问上一条历史命令
下光标键<↓>	访问下一条历史命令
<Tab>键	输入不完整的关键字后按下<Tab>键，系统自动补全关键字： • 如果与之匹配的关键字唯一，则系统用此完整的关键字替代原输入并换行显示 • 如果与之匹配的关键字不唯一，则多次按<Tab>键，系统会循环显示所有以输入字符串开头的关键字 • 如果没有与之匹配的关键字，系统会不作任何修改，重新换行显示原输入

用户通过键盘输入命令行后，按<Enter>键执行该命令。

用户输入的命令行总长度不能超过 512 个字符，包括空格，关键字或特殊符号等。

在配置文件中，存在#和 Version 7.1.064, ESS 0401L13 这样的特殊命令行配置信息。#用于将两段配置信息隔开；Version 7.1.064, ESS 0401L13 用于记录设备正在运行的软件包的版本信息。这样的命令行不支持在线帮助，但可以在任意视图下执行# xxx 或者 **version** xxx（比如执行# abc 或者 **version** abc），执行后系统不会提示错误信息，也不会修改这些行的值。这样的命令行用户没有必要使用，因此在命令手册中不再描述。

1.5.2 STRING和TEXT类型参数的输入

如果命令行中的参数为 STRING 类型，则建议输入除“?”、“"”、“\”、空格之外的可见字符（可见字符对应的 ASCII 码区间为 32～126），以免设备将该参数传递给其它网络设备时，对端设备无法解析。如果 STRING 类型的参数中需要包含字符“"”、“\”，则必须使用转义字符“\”辅助输入，

即实际应输入“\””、“\\”；如需输入空格，则需要将整个字符串包含在双引号中，例如，若要配置字符串参数为“my device”，则实际应输入“"my device"”。

如果命令行中的参数是 TEXT 类型的，则除了“?”外的其他字符都可输入。

1.5.3 接口类型的输入

输入接口类型时，设备支持使用接口类型的全称和简称。使用接口类型的全称时，支持不完整的字符输入；使用接口类型简称时，必须输入完整的简称。两种方式输入的接口类型均不区分大小写。例如在输入 **interface gigabitethernet 1/0/1** 时，可以使用接口类型全称的不完整字符 **interface g 1/0/1**，也可以使用接口类型简称 **interface ge 1/0/1**。接口类型和接口编号之间无论输入空格与否，都可以成功进入接口视图。关于接口全名与简名的对应关系，如表 1-5 所示。

表1-5 接口类型的全称和简称对应表

接口类型全称	接口类型简称
Route-Aggregation	RAGG
Dialer	Dia
LoopBack	Loop
GigabitEthernet	GE
Ten-GigabitEthernet	XGE
Virtual-Ethernet	VEth
M-GigabitEthernet	MGE
MP-group	MP
Serial	Ser
Tunnel	Tun
Vlan-interface	Vlan-int
Virtual-Template	VT
Bridge-Aggregation	BAGG
Route-Aggregation	RAGG
FortyGigE	FGE
Virtual-PPP	VPPP
HDLC-bundle	HDLC-B
Tunnel-Bundle	Tunnel-B
VE-L2VPN	L2VE
VE-L3VPN	L3VE

1.5.4 快速输入命令行

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

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

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

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

1.5.5 配置命令字符串的别名

通过本命令用户可以为命令行指定一个或多个别名，也可以为命令行开头的一个或多个关键字配置多个别名，使其符合用户的使用习惯。使用本特性，只有当命令行第一个关键字或者 undo 命令的第二个关键字是别名时，才按照别名命令替换执行，否则按照非别名命令执行。比如：

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

使用本特性时需要注意：

- 用户成功执行的带别名的命令将以系统原始的命令形式被显示或存储，而不会以别名的形式。
- 当用户在执行别名命令时，如果别名命令中定义了参数，则参数必须输入完全，设备才会按照替换后的命令执行相关操作；否则设备将会返回命令输入不完整的提示信息，并显示出当前别名代表的命令字符串。
- 为了方便用户使用，系统定义了部分常用的关键字作为缺省别名，如表 1-6 所示。

表1-6 系统定义的缺省别名

缺省别名	命令
access-list	**acl**
end	**return**
erase	**delete**
exit	**quit**
hostname	**sysname**
logging	**info-center**
no	**undo**
show	**display**
write	**save**

表1-7 配置命令字符串的别名

操作	命令	说明
进入系统视图	**system-view**	-
给指定的命令字符串配置别名	**alias** *alias command*	系统定义的缺省别名命令，请参见表1-6

操作	命令	说明
（可选）显示命令字符串别名功能的相关配置	**display alias** [*alias*]	该命令可在任意视图下执行

1.5.6 配置命令行的快捷键

为便于用户对常用命令进行快捷操作，系统提供了一系列的快捷键。其中用户可自定义的快捷键有五个，配置步骤见表 1-8，其他快捷键（见表 1-9）为系统保留的，不能通过命令行配置。

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

表1-8 配置命令行的快捷键

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

表1-9 系统保留的快捷键

快捷键	功能
<Ctrl+A>	将光标移动到当前行的开头
<Ctrl+B>	将光标向左移动一个字符
<Ctrl+C>	停止当前正在执行的功能
<Ctrl+D>	删除当前光标所在位置的字符
<Ctrl+E>	将光标移动到当前行的末尾
<Ctrl+F>	将光标向右移动一个字符
<Ctrl+H>	删除光标左侧的一个字符
<Ctrl+K>	终止呼出的连接
<Ctrl+N>	显示历史缓冲区中的下一条命令（暂不支持）

快捷键	功能
<Ctrl+P>	显示历史缓冲区中的上一条命令
<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>	删除光标所在位置及其右侧所有的字符
<Ctrl+Z>	退回到用户视图
<Ctrl+]>	终止当前连接
<Esc+B>	将光标移动到左侧连续字符串的首字符处
<Esc+D>	删除光标所在位置及其右侧连续字符串内的所有字符
<Esc+F>	将光标向右移到下一个连续字符串之前
<Esc+N>	将光标向下移动一行（输入回车前有效）（暂不支持）
<Esc+P>	将光标向上移动一行（输入回车前有效）（暂不支持）
<Esc+<>	（暂不支持）将光标所在位置指定为剪贴板的开始位置
<Esc+>>	（暂不支持）将光标所在位置指定为剪贴板的结束位置

1.5.7 命令行输入回显功能

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

表1-10 配置命令行输入回显功能

操作	命令	说明
进入系统视图	**system-view**	-
打开命令行输入回显功能	**info-center synchronous**	缺省情况下，命令行输入回显功能处于关闭状态 本命令的详细介绍请参见“网络管理和监控命令参考”中的“信息中心”

1.6 解读输入错误提示信息

命令行输入完毕后，请按<Enter>键执行该命令。设备执行命令的过程中，首先会对命令行进行语法检查。如果通过语法检查，则正确执行；否则，输出错误信息，常见的错误信息如表 1-11 所示。

表1-11 命令行常见错误信息表

英文错误信息	错误原因
% Unrecognized command found at '^' position.	命令无法解析，符号“^”指示位置出错

英文错误信息	错误原因
% Incomplete command found at '^' position.	符号“^”指示位置的参数输入不完整
% Ambiguous command found at '^' position.	符号“^”指示位置的关键字不明确，存在二义性
% Too many parameters.	输入参数太多
% Wrong parameter found at '^' position.	在符号“^”指示位置的参数错误

1.7 使用历史命令

用户在设备上成功执行的命令，会同时保存到用户独享的历史命令缓冲区和所有用户共享的历史命令缓冲区。两缓冲区的详细描述请参见表 1-12。

表1-12 历史命令缓冲区描述表

历史命令缓冲区	是否可查看	是否可调用	退出登录后，历史命令是否继续保存	大小是否可调
独享历史命令缓冲区，每个用户线对应一个独享历史命令缓冲区	可通过**display history-command**来查看	• 使用上光标键↑并回车，可调用上一条历史命令 • 使用下光标键↓并回车，可调用下一条历史命令	不保存	可通过**history-command max-size** *size-value*命令来配置（该命令的详细介绍请参见“基础配置命令参考”中的“登录设备”）。缺省情况下，可存放10条历史命令；如果将*size-value*设置为0，则不会缓存历史命令；如果当前历史命令缓冲区满且有新的命令需要缓存，则自动删除最早的记录，来保存新命令
共享历史命令缓冲区，所有用户线共用一个共享历史命令缓冲区	可通过**display history-command all**来查看	不能调用	保存	为固定大小1024条。如果当前历史命令缓冲区满且有新的命令需要缓存，则自动删除最早的记录，来保存新命令

设备保存历史命令时，遵循下列原则：

- 如果用户使用了命令的不完整形式，保存的历史命令也是不完整形式；如果用户使用了命令字符串的别名形式，保存的历史命令是原始命令形式。
- 如果用户连续多次执行同一条命令，设备的历史命令中只保留一次。但如果执行时输入的形式不同，将作为不同的命令对待。例如：连续多次执行 **display current-configuration** 命令，设备只保存一条历史命令；如果分别执行 **display current-configuration** 命令和它的不完整形式 **display cu**，设备将保存为两条历史命令。

1.8 重复执行历史记录命令

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

在执行 **repeat** 命令时需要注意：

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

表1-13 重复执行历史记录命令

操作	命令	说明
重复执行历史记录命令	**repeat** [*number*] [**count** *times*] [**delay** *seconds*]	该命令可以在任意视图下执行

1.9 便捷地查看显示信息

1.9.1 分屏显示

1. 控制分屏显示

当显示信息较多并超过一屏时，系统会将信息分屏显示，并在屏间显示“----more----”信息，表示这一屏信息已经显示完毕，自动暂停，方便查看显示信息。

这时用户可以使用表 1-14 所示的按键来选择下一步操作。

表1-14 分屏显示功能表

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

缺省情况下，一屏显示 24 行信息，也可以使用 **screen-length** 命令设置用户线下一屏显示的行数（**screen-length** 命令的详细介绍请参见“基础配置命令参考”中的“登录设备”）。

2. 关闭分屏显示功能

可以通过以下配置关闭当前登录用户的分屏显示功能。分屏显示功能处于关闭状态时，会一次显示所有信息，如果信息较多，则会连续刷屏，不方便查看。

表1-15 关闭分屏显示

操作	命令	说明
关闭当前用户的分屏显示功能	**screen-length disable**	缺省情况下，用户登录后将遵循用户线下的**screen-length**设置 该操作在用户视图下执行，仅对当前用户本次登录有效，用户重新登录后将恢复到缺省情况

1.9.2 查看带行号的显示信息

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

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

表1-16 查看带行号的显示信息

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

下面将通过举例示意如何查看带行号的显示信息。

显示 VLAN 999 信息的同时显示行号。

```
<Sysname> display vlan 999 | by-linenum
    1:  VLAN ID: 999
    2:  VLAN type: Static
    3:  Route interface: Configured
    4:  IPv4 address: 192.168.2.1
    5:  IPv4 subnet mask: 255.255.255.0
    6:  Description: For LAN Access
    7:  Name: VLAN 0999
    8:  Tagged ports:   None
    9:  Untagged ports:
   10:      GigabitEthernet1/0/1
```

1.9.3 使用正则表达式过滤显示信息

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

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

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

正则表达式（*regular-expression*）为 1～256 个字符的字符串，区分大小写，它支持多种特殊字符，特殊字符的匹配规则如表 1-17 所示。正则表达式的执行时间和正则表达式的复杂程度成正比，对于复杂的正则表达式，执行时间会比较长，如有需要，可按<CTRL+C>键终止。

表1-17 正则表达式中的特殊字符描述表

特殊字符	含义	举例
^	匹配以指定字符开始的行	^u只能匹配以u开始的行，不能匹配以Au开始的行
$	匹配以指定字符结束的行	u$只能匹配以u结尾的行，不能匹配以uA结尾的行
.	通配符，可代表任何一个字符	.s可以匹配as和bs等
*	匹配星号前面的字符或字符串零次或多次	• zo*可以匹配 z 以及 zoo • (zo)*可以匹配 zo 以及 zozo
+	匹配+前面的字符或字符串一次或多次	zo+可以匹配zo以及zoo，但不能匹配z
|	匹配|左边或右边的整个字符串	def|int只能匹配包含def或者int的字符串所在的行
( )	表示字符串，一般与“+”或“*”等符号一起使用	(123A)表示字符串123A；408(12)+可以匹配40812或408121212等字符串，但不能匹配408
\index	表示重复一次指定字符串，字符串是指\前用()括起来的字符串，index对应\前字符串的顺序号按从左至右的顺序从1开始编号：如果\前面只有一个字符串，则index只能为1；如果\前面有n个字符串，则index可以为1到n中的任意整数	(string)\1表示把string重复一次，匹配的字符串必须包含stringstring；(string1)(string2)\2表示把string2重复一次，匹配的字符串必须包含string1string2string2；(string1)(string2)\1\2表示先把string1重复一次，再重复一次string2，匹配的字符串必须包含string1string2string1string2
[ ]	表示字符选择范围，将以选择范围内的单个字符为条件进行匹配，只要字符串里包含该范围的某个字符就能匹配到	• [16A]表示可以匹配到的字符串只需要包含 1、6 或 A 中任意一个 • [1-36A] 表示可以匹配到的字符串只需要包含 1、2、3、6 或 A 中任意一个（-为连接符） 如果]需要作为普通字符出现在[ ]内时，必须把]写在[ ]中字符的最前面，形如[]string]，才能匹配到]。[没有这样的限制
[^]	表示选择范围外的字符，将以单个字符为条件进行匹配，只要字符串里包含该范围外的某个字符就能匹配到	[^16A]表示可匹配的字符串只需要包含1、6和A之外的任意字符，该字符串也可以包含字符1、6或A，但不能只包含这三个字符。比如[^16A]可以匹配abc、m16，不能匹配1、16、16A
{n}	n是一个非负整数，匹配n次	o{2}不能匹配Bob，但是能匹配food
{n,}	n是一个非负整数，至少匹配n次	o{2,}不能匹配Bob，但能匹配fooooood
{n,m}	m和n均为非负整数，其中n小于等于m。只要字符串里包含n到m个某字符就能匹配到	o{1,3}能匹配fod、food、foood、foooood，但不能匹配fd
\<	匹配包含指定字符串的字符串，字符串前面如果有字符则不能是数字、字母和下划线	\<do匹配单词domain，还可以匹配字符串doa
\>	匹配包含指定字符串的字符串，字符串后面如果有字符则不能是数字、字母和下划线	do\>匹配单词undo，还可以匹配字符串cdo
\b	匹配一个单词边界，也就是指单词和空格间的位置	er\b可以匹配never，但不能匹配verb \ber可以匹配erase，但不能匹配verb
\B	匹配非单词边界	er\B能匹配verb，但不能匹配never

特殊字符	含义	举例
\w	\w等效于[A-Za-z0-9_]，是数字、字母或下划线	v\w能匹配vlan，v\w还能匹配service
\W	\W等效于[^A-Za-z0-9_]，是除了数字、字母和下划线之外的任意字符	\Wa可以匹配-a，但是不能匹配2a和ba等
\	转义操作符，\后紧跟本表中罗列的单个特殊字符时，将去除特殊字符的特定含义	• \\可以匹配包含\的字符串 • \^可以匹配包含^的字符串 • \\b 可以匹配包含\b 的字符串

下面将通过举例示意如何使用正则表达式过滤显示信息。

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

```
<Sysname> display current-configuration | begin line
line class console
 user-role network-admin
#
line class tty
 user-role network-operator
#
line class vty
 user-role network-operator
#
line con 0
 user-role network-admin
#
line vty 0 63
 authentication-mode none
 user-role network-admin
 user-role network-operator
#
return
```

查看路由表中的非直连路由（该显示信息与设备型号以及用户的当前配置有关）。

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

Destinations : 12       Routes : 12

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
2.2.2.0/24          OSPF   10   2            1.1.2.2         GE1/0/1
```

查看 SNMP 相关配置（该显示信息与设备型号以及用户的当前配置有关）。

```
<Sysname> display current-configuration | include snmp
 snmp-agent
 snmp-agent community write private
 snmp-agent community read public
 snmp-agent sys-info version all
```

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

1.9.4 将显示信息保存到指定文件

display 命令显示的内容通常是统计信息、功能是否开启以及功能的相关参数配置，这些信息在设备运行过程中会随着时间或者用户的配置而改变。使用本配置可以将当前显示信息保存到指定文件，方便随时比对和查看。有两种方式将显示信息保存到文件中：

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

表1-18 将显示信息保存到指定文件

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

下面将通过举例示意如何将显示信息保存到指定文件以及保存效果。

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

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

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

```
<Sysname> more vlan.txt
VLAN ID: 1
 VLAN type: Static
 Route interface: Not configured
 Description: VLAN 0001
 Name: VLAN 0001
 Tagged ports:   None
 Untagged ports:
    GigabitEthernet1/0/2
```

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

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

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

```
<Sysname> more vlan.txt
VLAN ID: 1
 VLAN type: Static
 Route interface: Not configured
 Description: VLAN 0001
 Name: VLAN 0001
 Tagged ports:   None
 Untagged ports:
    GigabitEthernet1/0/2

 VLAN ID: 999
 VLAN type: Static
 Route interface: Configured
```

```
 IPv4 address: 192.168.2.1
 IPv4 subnet mask: 255.255.255.0
 Description: For LAN Access
 Name: VLAN 0999
 Tagged ports:    None
 Untagged ports:
    GigabitEthernet1/0/1
```

1.9.5 各种便捷查看方式的综合应用

执行 **display** 命令时，通过选择参数，可以同时实现“1.9.2 查看带行号的显示信息”、“1.9.3 使用正则表达式过滤显示信息”和“1.9.4 将显示信息保存到指定文件”。

表1-19 各种便捷查看方式的综合应用

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

下面将通过举例示意如何将各种便捷查看方式综合应用。

按行号将当前配置保存到文件 test.txt。

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

将 SNMP 的相关配置以追加方式保存到文件 test.txt。

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

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

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

1.10 保存当前配置

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

配置保存不涉及一次性执行命令，比如：**display** 命令（执行后即显示相关信息）和 **reset** 命令（执行后即清除相关信息）。**save** 命令的详细介绍请参见“基础配置命令参考”中的“配置文件管理”。

目 录

1 RBAC

说明

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

1.1 RBAC简介

RBAC（Role Based Access Control，基于角色的访问控制）通过建立“权限<->角色”的关联实现将权限赋予给角色，并通过建立“角色<->用户”的关联实现为用户指定角色，从而使用户获得相应角色所具有的权限。RBAC 的基本思想就是给用户指定角色，这些角色中定义了允许用户操作哪些系统功能以及资源对象。

由于权限与用户的分离，RBAC 具有以下优势：

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

1.1.1 用户角色

为一个用户角色赋予权限的具体实现包括以下两个方面：

- 定义用户角色规则：实现对系统功能的操作权限的控制。例如，定义用户角色规则允许用户配置 A 功能，或禁止用户配置 B 功能。
- 定义资源控制策略：实现对系统资源（接口、VLAN、VPN 实例、安全域）的操作权限的控制。例如，定义资源控制策略允许用户操作 VLAN 10，禁止用户操作接口 GigabitEthernet1/0/1。

1. 用户角色规则

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

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

- 读类型：本类型的命令仅能显示系统配置信息和维护信息，如显示命令 **display**、显示文件信息的命令 **dir**。
- 写类型：本类型的命令用于对系统进行配置，如使能信息中心功能的命令 **info-center enable**、配置调试信息开关的命令 **debugging**。
- 执行类型：本类型的命令用于执行特定的功能，如 **ping** 命令、与 FTP 服务器建立连接的命令 **ftp**。

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

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

(4) Web 菜单：通过 Web 对设备进行配置时，各配置页面以 Web 菜单的形式组织，按照层次关系，形成多级菜单的树形结构。

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

(6) OID：Object Identifier，对象标识符，SNMP 协议通过 OID 唯一标识一个被管理对象。

根据权限控制范围的不同，可以将用户角色规则分为如下几类：

(1) 基于命令的规则：用来控制一条命令或者与指定命令关键字相匹配的一类命令是否允许被执行。关于匹配的具体涵义，请参见 RBAC 配置命令。

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

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

(4) 基于 Web 菜单的规则：用来控制指定的 Web 菜单选项是否允许被操作。因为菜单项中的操作控件具有相应的读，写或执行属性，所以定义基于 Web 菜单的规则时，可以精细地控制菜单项中读、写或执行控件的操作。

(5) 基于 XML 元素的规则：用来控制指定的 XML 元素是否允许被执行。XML 元素也具有读，写或执行属性。

(6) 基于 OID 的规则：用来控制指定的 OID 是否允许被 SNMP 访问。OID 具有读，写和执行属性。

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

2. 资源控制策略

资源控制策略规定了用户对系统资源的操作权限。在用户角色中可定义四种类型的资源控制策略：接口策略、VLAN 策略、VPN 策略以及安全域策略，它们分别定义了用户允许操作的接口、VLAN、VPN 实例以及安全域。对接口/VLAN/VPN 实例/安全域的操作是指创建并进入接口视图/VLAN 视图/VPN 实例视图/安全域视图、删除和应用接口/VLAN/VPN 实例/安全域（在 **display** 命令中指定接口/VLAN/VPN 实例/安全域参数并不属于应用接口/VLAN/VPN 实例/安全域）。

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

为该用户角色定义规则允许用户执行创建 VLAN 命令，则用户即便拥有该 VLAN 资源的操作权限，也无法执行相关的命令。

1.1.2 缺省用户角色

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

表1-1 系统预定义的用户角色名和对应的权限

用户角色名	权限
network-admin	可操作系统所有功能和资源（除安全日志文件管理相关命令**display security-logfile summary**、**info-center security-logfile directory**、**security-logfile save**之外）
network-operator	• 可执行系统所有功能和资源的相关 **display** 命令（除 **display history-command all**、**display security-logfile summary** 等命令，具体请通过 **display role** 命令查看） • 如果用户采用本地认证方式登录系统并被授予该角色，则可以修改自己的密码 • 可执行进入 XML 视图的命令 • 可允许用户操作所有读类型的 Web 菜单选项 • 可允许用户操作所有读类型的 XML 元素 • 可允许用户操作所有读类型的 OID
level-*n* (*n* = 0～15)	• level-0：可执行命令 **ping**、**tracert**、**ssh2**、**telnet** 和 **super**，且管理员可以为其配置权限 • level-1：具有 level-0 用户角色的权限，并且可执行系统所有功能和资源的相关 **display** 命令（除 **display history-command all** 之外），以及管理员可以为其配置权限 • level-2～level-8 和 level-10～level-14：无缺省权限，需要管理员为其配置权限 • level-9：可操作系统中绝大多数的功能和所有的资源，且管理员可以为其配置权限，但不能操作 **display history-command all** 命令、RBAC 的命令（Debug 命令除外）、文件管理、设备管理以及本地用户特性。对于本地用户，若用户登录系统并被授予该角色，可以修改自己的密码 • level-15：具有与 network-admin 角色相同的权限
security-audit	安全日志管理员，仅具有安全日志文件的读、写、执行权限，具体如下： • 可执行安全日志文件管理相关的命令（**display security-logfile summary**、**info-center security-logfile directory**、**security-logfile save**）。安全日志文件管理相关命令的介绍，请参见“网络管理与监控”中的“信息中心” • 可执行安全日志文件操作相关的命令，例如 **more** 显示安全日志文件内容；**dir**、**mkdir** 操作安全日志文件目录等，具体命令的介绍请参见“基础配置命令参考”中的“文件系统管理” 以上权限，仅安全日志管理员角色独有，其它任何角色均不具备 该角色不能被授权给从当前用户线登录系统的用户

用户角色名	权限
guest-manager	来宾用户管理员，只能查看和配置与来宾有关的web页面，没有控制命令行的权限

说明

- 用户以任意角色登录设备，均具有执行 **system-view**、**quit** 和 **exit** 命令的权限。
- 预定义的用户角色中，仅用户角色 level-0～level-14 可以通过自定义规则和资源控制策略调整自身的权限。需要注意的是，这种修改对于 **display history-command all** 命令不生效，即不能通过添加对应的规则来更改它的缺省执行权限。

注意

只有具有 network-admin 或者 level-15 用户角色的用户登录设备后才具有执行创建/修改/删除本地用户和本地用户组的权限；其它角色的用户，即使被授权本地用户和本地用户组的操作权限，也仅仅具有修改自身密码的权限，没有除此之外的对本地用户和本地用户组的任何操作权限。

1.1.3 为用户授权角色

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

(1) AAA 方式：用户登录时使用的认证方式为 **scheme**，用户登录设备后所拥有的用户角色由 AAA 功能进行授权。

- 若用户通过了本地授权，则由设备为其授权用户角色，授权的用户角色是在本地用户中设置的。
- 若用户通过了远程授权，则由远程 AAA 服务器为其授权用户角色，授权的用户角色是在远程 AAA 服务器（RADIUS 或 HWTACACS 服务器）上设置的。

(2) 非 AAA 方式：用户登录时使用的认证方式为 **none** 或者 **password**，用户登录后所拥有的用户角色是用户线下配置的用户角色。

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

说明

- AAA 相关内容的介绍请参见“安全配置指导”中的“AAA”。
- 用户线相关内容的介绍请参见“基础配置指导”中的“登录设备”。
- 通过 publickey 或 password-publickey 认证登录服务器的 SSH 用户将被授予同名的设备管理类本地用户视图下配置的授权用户角色。SSH 用户相关的介绍请参见“安全配置指导”中的“SSH”。

1.2 RBAC配置任务简介

表1-2 RBAC 配置任务简介

配置任务	说明	详细配置
创建用户角色	必选	1.3
配置用户角色规则	必选	1.4
配置特性组	可选	1.5
配置资源控制策略	必选	1.6
为用户授权角色	可选	1.7
切换用户角色	可选	1.8

1.3 创建用户角色

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

表1-3 创建用户角色

操作	命令	说明
进入系统视图	**system-view**	-
创建用户角色，并进入用户角色视图	**role name** *role-name*	缺省情况下，系统预定义的用户角色为network-admin、network-operator、level-*n*（*n*为0～15的整数）、security-audit、guest-manager。其中，仅用户角色level-0～level-14可以自定义规则、资源控制策略以及配置描述信息
（可选）配置用户角色描述信息	**description** *text*	缺省情况下，未定义用户角色描述信息

1.4 配置用户角色规则

用户角色规则分为以下几类，可根据权限控制需要配置一条或多条规则：

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

关于用户角色规则，存在以下配置限制：

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

表1-4 配置用户角色规则

操作	命令	说明
进入系统视图	**system-view**	-
进入用户角色视图	**role name** *role-name*	-
配置基于命令的规则	**rule** *number* { **deny** | **permit** } **command** *command-string*	至少选其一 缺省情况下，新创建的用户角色中未

操作	命令	说明
配置基于特性的规则	**rule** *number* { **deny** | **permit** } { **execute** | **read** | **write** } * **feature** [*feature-name*]	
配置基于特性组的规则	**rule** *number* { **deny** | **permit** } { **execute** | **read** | **write** } * **feature-group** *feature-group-name*	
配置基于Web菜单的规则	**rule** *number* { **deny** | **permit** } { **execute** | **read** | **write** } * **web-menu** [*web-string*]	
配置基于XML元素的规则	**rule** *number* { **deny** | **permit** } { **execute** | **read** | **write** } * **xml-element** [*xml-string*]	
配置基于OID的规则	**rule** *number* { **deny** | **permit** } { **execute** | **read** | **write** } * **oid** *oid-string*	

1.5 配置特性组

特性组中可以包含多个系统中的特性。配置特性组便于管理员为有相同权限需求的多个特性定义统一的用户角色规则。

表1-5 配置特性组

操作	命令	说明
进入系统视图	**system-view**	-
创建特性组，并进入特性组视图	**role feature-group name** *feature-group-name*	若要配置基于特性组的规则，则必选 缺省情况下，存在两个特性组，名称为L2和L3 除系统预定义的特性组L2和L3之外，系统中最多允许创建64个特性组 特性组L2和L3不能被修改和删除
向特性组中添加一个特性	**feature** *feature-name*	缺省情况下，自定义特性组中不包含任何特性

1.6 配置资源控制策略

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

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

表1-6 配置接口资源控制策略

操作	命令	说明
进入系统视图	**system-view**	-

操作	命令	说明
进入用户角色视图	**role name** *role-name*	-
进入接口策略视图	**interface policy deny**	缺省情况下，用户具有操作任何接口的权限 进入接口策略视图后，如果不配置允许操作的接口列表，则用户将没有操作任何接口的权限
（可选）配置允许操作的接口列表	**permit interface** *interface-list*	缺省情况下，未定义允许操作的接口列表，用户没有操作任何接口的权限 可以多次执行此命令向接口列表中添加允许操作的接口

表1-7 配置 VLAN 资源控制策略

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

表1-8 配置 VPN 资源控制策略

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

表1-9 配置安全域资源控制策略

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

1.7 为用户授权角色

说明

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

1.7.1 使能缺省用户角色授权功能

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

表1-10 使能缺省用户角色授权功能

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

1.7.2 为远程AAA认证用户授权角色

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

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

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

1.7.3 为本地AAA认证用户授权角色

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

需要注意的是：

- 由于本地用户缺省就拥有一个用户角色，如果要赋予本地用户新的用户角色，请确认是否需要保留这个缺省的用户角色，若不需要，请删除。
- 系统中的最后一个安全日志管理员角色的本地用户不可被删除。

安全日志管理员与其它用户角色互斥，因此在为本地用户授权用户角色时，有以下内容需要关注：

- 为一个本地用户授权安全日志管理员角色时，经过界面的交互式确认后，系统会自动删除当前用户的所有其它他用户角色。
- 如果已经为当前本地用户授权了安全日志管理员角色，再授权其它的用户角色时，经过界面的交互确认后，系统会自动删除当前用户的安全日志管理员角色。

表1-11 为本地用户授权用户角色

操作	命令	说明
进入系统视图	**system-view**	-
创建本地用户，并进入本地用户视图	**local-user** *user-name* **class** { **manage** | **network** }	-
为本地用户授权用户角色	**authorization-attribute user-role** *role-name*	缺省情况下，由用户角色为network-admin或level-15的用户创建的本地用户将被授权用户角色network-operator 可通过多次执行本命令，为本地用户授权多个用户角色，最多可授权64个

1.7.4 为非AAA认证用户授权角色

对于不使用 AAA 认证登录设备的非 SSH 用户，由用户线配置决定为其授权的用户角色。有关用户线相关配置的详细介绍请参见“基础配置指导”中的“登录设备”；通过 publickey 或 password-publickey 认证登录设备的 SSH 用户，由同名的设备管理类本地用户配置决定为其授权的用户角色。SSH 用户相关的介绍请参见“安全配置指导”中的“SSH”。

表1-12 为非 AAA 认证用户授权用户角色

操作	命令	说明
进入系统视图	**system-view**	-
进入用户线视图	**line** { *first-num1* [*last-num1*] | { **aux** | **console** | **tty** | **vty** } *first-num2* [*last-num2*] }	二者选其一 关于用户线和用户线视图下各属性生效情况和优先级的详细介绍，请参见“基础配置指导”中的“配置通过CLI登录设备”
进入用户线类视图	**line class** { **aux** | **console** | **tty** | **vty** }	
为从当前用户线登录系统的用户配置授权的用户角色	**user-role** *role-name*	缺省情况下，使用Console/AUX用户线登录系统的用户将被授权用户角色network-admin；通过其它用户线登录系统的用户将被授权用户角色network-operator 不能为从当前用户线登录系统的用户授权安全日志管理员的用户角色

1.8 切换用户角色

1. 功能简介

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

- 为了防止对设备的误操作，通常情况下建议管理员使用较低权限的用户角色登录设备、查看设备运行参数，当需要对设备进行维护时，再临时切换到较高权限的用户角色。
- 当管理员需要暂时离开设备或者将设备暂时交给其它人代为管理时，为了安全起见，可以临时切换到较低权限的用户角色，来限制其他人员的操作。

为了保证操作的安全性，通常用户进行用户角色切换时，均需要输入用户角色切换密码。切换到不同的用户角色时，需要输入相应切换密码。如果服务器没有响应或者没有配置用户角色切换密码，则切换操作失败，若还有备份认证方案，则转而进行备份认证。因此，在进行切换操作前，请先保证配置了正确的用户角色切换密码。

2. 配置用户角色切换时的认证方式

为了保证切换操作的安全性，执行用户角色切换时，需要进行身份认证。设备支持如表 1-13 所示的四种用户角色切换认证方式。

表1-13 用户角色的切换认证方式

认证方式	涵义	说明
local	本地密码认证	设备验证用户输入的用户角色切换密码 使用该方式时，需要在设备上使用**super password**命令设置用户角色切换密码 对于Console/AUX用户，在设备仅采用本地密码切换认证方式且未配置切换密码的情况下，设备不关心用户是否输入切换密码以及输入切换密码的内容，可允许用户成功切换用户角色

认证方式	涵义	说明
scheme	通过HWTACACS或RADIUS进行远程AAA认证	设备将用户角色切换使用的用户名和密码发送给HWTACACS/RADIUS服务器进行远程验证 使用该方式时，需要进行以下相关配置： • 在设备上配置 HWTACACS/RADIUS 方案，并在 ISP 域中引用已创建的 HWTACACS/RADIUS 方案，详细介绍请参见“安全配置指导”中的“AAA” • 在 HWTACACS/RADIUS 服务器上创建相应的用户并配置密码
local scheme	先本地密码认证，后远程AAA认证	先进行本地密码认证，若设备上未设置本地用户角色切换密码，使用Console或VTY用户线登录的用户则转为远程AAA认证，使用AUX用户线登录的用户则可以成功切换用户角色
scheme local	先远程AAA认证，后本地密码认证	先进行远程AAA认证，远程HWTACACS/RADIUS服务器无响应或设备上的AAA远程认证配置无效时，转为本地密码认证

- 当使用 HWTACACS 方案进行用户角色切换认证时，系统使用用户输入的用户角色切换用户名进行角色切换认证，HWTACACS 服务器上也必须存在相应的用户。
  - 当用户要切换到 level-*n* 的用户角色时，要求 HWTACACS 服务器上存在能提供切换到 level-*n* 角色的用户。在 HWTACACS 服务器上，支持切换到用户角色 level-n 的用户也能够支持切换到 level-0 到 level-n 之间任意的用户角色。
  - 当用户要切换到非 level-*n* 的用户角色时，要求 HWTACACS 服务器上存在至少能提供切换到 level-0 角色的用户，且该用户配置了取值为 allowed-roles="*role*"的自定义属性（其中 *role* 为要切换的目的用户角色名称）。
- 当使用 RADIUS 方案进行用户角色切换认证时，系统使用“$enab*n*$”形式的用户名进行用户角色切换认证，其中 *n* 为用户希望切换到的用户角色 level-*n* 中的 *n*，RADIUS 服务器上也必须存在该形式用户名的用户。与 HWTACACS 不同的是，用户进行角色切换时可输入任意用户名，该名称在认证过程中无实际意义。
  - 当用户要切换到 level-*n* 的用户角色时，要求 RADIUS 服务器上存在用户名为“$enab*n*$”的用户。例如，用户希望切换到用户角色 level-3，输入任意用户名，系统忽略用户输入的用户名，使用“$enab3$”形式的用户名进行用户角色切换认证。
  - 当用户要切换到非 level-*n* 的用户角色时，要求 RADIUS 服务器上存在用户名为“$enab0$”的用户，且该用户配置了取值为 allowed-roles="*role*"的自定义属性（其中 *role* 为要切换的目的用户角色名称）。
- 用户进行用户角色切换认证时，系统发送给 RADIUS 服务器的认证请求报文中的用户名中不会携带域名，系统发送给 HWTACACS 服务器的认证请求报文中的用户名是否携带域名由配置决定（**user-name-format**），系统采用的切换认证方案由用户输入的用户名中指定的域名决定，若该用户名中未携带域名，则使用缺省域。
- 当用户从用户角色 a 切换到用户角色 b 后，若输入 **quit** 命令，将退出当前登录的用户线。

表1-14 配置用户角色切换时的认证方式

操作	命令	说明
进入系统视图	**system-view**	-

操作	命令	说明
配置用户角色切换时的认证方式	**super authentication-mode** { **local** | **scheme** } *	缺省情况下，采用**local**认证方式
配置用户角色切换的密码	非FIPS模式下： **super password** [**role** *role-name*] [{ **hash** | **simple** } *string*] FIPS模式下： **super password** [**role** *role-name*]	如果采用**local**认证方式，则该步骤必选 缺省情况下，未设置切换用户角色的密码 若不指定用户角色，则设置的是切换到当前缺省目的用户角色的密码
（可选）配置用户角色切换的缺省目的用户角色	**super default role** *role-name*	缺省情况下，用户角色切换的缺省目的角色为network-admin

3. 切换用户角色

表1-15 切换用户角色

操作	命令	说明
切换用户角色	**super** [*role-name*]	该命令在用户视图下执行 若不指定用户角色，则切换到当前缺省目的用户角色。缺省的目的用户角色由**super default role**命令指定 用户最多可以连续进行三次切换认证，如果三次认证都失败则本轮切换失败 若要执行切换用户角色的操作，必须保证当前用户具有执行本命令的权限

1.9 RBAC显示和维护

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

表1-16 RBAC 显示和维护

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

1.10 RBAC典型配置举例

1.10.1 Telnet用户的本地用户角色授权配置举例

1. 组网需求

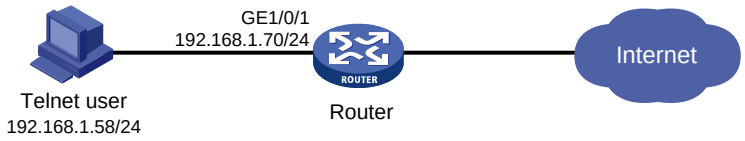
如图 1-1 所示，Telnet 用户主机与 Router 相连，需要实现 Router 对 Telnet 用户进行本地认证并授权用户角色。Telnet 用户的登录用户名为 user1@bbb，认证通过后被授权的用户角色为 role1。

role1 具有如下用户权限：

- 允许用户执行所有特性中读类型的命令；
- 允许用户执行进入接口视图以及接口视图下的相关命令，并具有操作接口 GigabitEthernet1/0/2～GigabitEthernet1/0/4 的权限。

2. 组网图

图1-1 Telnet 用户本地认证/授权配置组网图



3. 配置步骤

配置接口 GigabitEthernet1/0/1 的 IP 地址，Telnet 用户将通过该地址连接 Router。

```
<Router> system-view
[Router] interface gigabitethernet 1/0/1
[Router-GigabitEthernet1/0/1] ip address 192.168.1.70 255.255.255.0
[Router-GigabitEthernet1/0/1] quit
```

开启 Router 的 Telnet 服务器功能。

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

配置 Telnet 用户登录采用 AAA 认证方式。

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

配置 ISP 域 bbb 的 AAA 方法为本地认证和本地授权。

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

创建用户角色 role1。

```
[Router] role name role1
```

配置用户角色规则 1，允许用户执行所有特性中读类型的命令。

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

配置用户角色规则 2，允许用户执行进入接口视图以及接口视图下的相关命令。

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

进入接口策略视图，允许用户具有操作接口 GigabitEthernet1/0/2～GigabitEthernet1/0/4 的权限。

```
[Router-role-role1] interface policy deny
[Router-role-role1-ifpolicy] permit interface gigabitethernet 1/0/2 to gigabitethernet
1/0/4
[Router-role-role1-ifpolicy] quit
[Router-role-role1] quit
```

创建设备管理类本地用户 user1。

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

配置用户的密码是明文的 aabbcc。

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

指定用户的服务类型是 Telnet。

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

指定用户 user1 的授权角色为 role1。

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

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

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

4. 验证配置

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

可通过如下步骤验证用户的权限：

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

进入接口 GigabitEthernet1/0/1 视图。

```
[Router] interface gigabitethernet 1/0/1
Permission denied.
```

配置接口 GigabitEthernet1/0/2 的 IPv4 地址。

```
[Router] interface gigabitethernet 1/0/2
[Router-GigabitEthernet1/0/2] ip address 6.6.6.6 24
[Router-GigabitEthernet1/0/2] quit
```

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

```
[Router] display clock
09:31:56 UTC Sat 01/01/2016
[Router] quit
```

- 不能执行特性中写类型和执行类型的命令。

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

1.10.2 Telnet用户的RADIUS用户角色授权配置举例

1. 组网需求

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

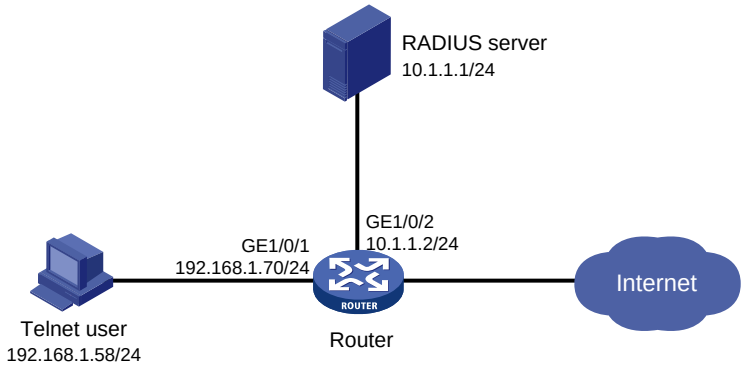
- 由一台 FreeRadius 服务器（IP 地址为 10.1.1.1/24）担当认证/授权/计费 RADIUS 服务器的职责；
- Router 与 RADIUS 服务器交互报文时使用的共享密钥为 expert，认证端口号为 1812；
- Router 向 RADIUS 服务器发送的用户名携带域名；
- Telnet 用户登录 Router 时使用 RADIUS 服务器上配置的用户名 hello@bbb 以及密码进行认证，认证通过后被授权的用户角色为 role2。

role2 具有如下用户权限：

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

2. 组网图

图1-2 Telnet 用户 RADIUS 认证/授权配置组网图



3. 配置步骤

(1) Router 上的配置

配置接口 GigabitEthernet1/0/1 的 IP 地址，Telnet 用户将通过该地址连接 Router。

```
<Router> system-view
[Router] interface gigabitethernet 1/0/1
[Router-GigabitEthernet1/0/1] ip address 192.168.1.70 255.255.255.0
[Router-GigabitEthernet1/0/1] quit
```

配置接口 GigabitEthernet1/0/2 的 IP 地址，Router 将通过该地址与服务器通信。

```
[Router] interface gigabitethernet 1/0/2
[Router-GigabitEthernet1/0/2] ip address 10.1.1.2 255.255.255.0
[Router-GigabitEthernet1/0/2] quit
```

开启 Router 的 Telnet 服务器功能。

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

配置 Telnet 用户登录采用 AAA 认证方式。

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

```
[Router-line-vty0-63] quit
```
创建 RADIUS 方案 rad。
```
[Router] radius scheme rad
```
配置主认证/授权服务器的 IP 地址为 10.1.1.1，认证端口号为 1812。
```
[Router-radius-rad] primary authentication 10.1.1.1 1812
```
配置与认证/授权服务器交互报文时的共享密钥为 expert。
```
[Router-radius-rad] key authentication simple expert
[Router-radius-rad] quit
```
配置 ISP 域 bbb 的 AAA 认证方法为 RADIUS 认证/授权、不计费。由于 RADIUS 服务器的授权信息是随认证应答报文发给 RADIUS 客户端的，所以必须保证认证和授权方法相同。
```
[Router] domain bbb
[Router-isp-bbb] authentication login radius-scheme rad
[Router-isp-bbb] authorization login radius-scheme rad
[Router-isp-bbb] accounting login none
[Router-isp-bbb] quit
```
创建特性组 fgroup1。
```
[Router] role feature-group name fgroup1
```
配置特性组 fgroup1 中包含特性 ARP 和 RADIUS。
```
[Router-featuregrp-fgroup1] feature arp
[Router-featuregrp-fgroup1] feature radius
[Router-featuregrp-fgroup1] quit
```
创建用户角色 role2。
```
[Router] role name role2
```
配置用户角色规则 1，允许用户执行 ISP 视图下的所有命令。
```
[Router-role-role2] rule 1 permit command system-view ; domain *
```
配置用户角色规则 2，允许用户执行特性组 fgroup1 中所有特性的读和写类型的命令。
```
[Router-role-role2] rule 2 permit read write feature-group fgroup1
```
配置用户角色规则 3，允许用户执行创建 VLAN 以及进入 VLAN 视图后的相关命令。
```
[Router-role-role2] rule 3 permit command system-view ; vlan *
```
配置用户角色规则 4，允许用户执行进入接口视图以及接口视图下的相关命令。
```
[Router-role-role2] rule 4 permit command system-view ; interface *
```
进入 VLAN 策略视图，允许用户具有操作 VLAN 1～VLAN 20 的权限。
```
[Router-role-role2] vlan policy deny
[Router-role-role2-vlanpolicy] permit vlan 1 to 20
[Router-role-role2-vlanpolicy] quit
```
进入接口策略视图，允许用户具有操作接口 GigabitEthernet1/0/1～GigabitEthernet1/0/4 的权限。
```
[Router-role-role2] interface policy deny
[Router-role-role2-ifpolicy] permit interface gigabitethernet 1/0/1 to gigabitethernet
1/0/4
[Router-role-role2-ifpolicy] quit
[Router-role-role2] quit
```
(2) RADIUS 服务器的配置

需要在 FreeRadius 服务器的 users 中增加配置文本：
```
Cisco-AVPair = "shell:roles=role2"
```

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

4. 验证配置

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

可通过如下步骤验证用户的权限：

- 可执行 ISP 视图下所有的命令。

```
[Router] domain abc
[Router-isp-abc] authentication login radius-scheme abc
[Router-isp-abc] quit
```

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

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

RADIUS 方案的显示信息此处略。

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

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

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

```
[Router] vlan 10
```

将接口 GigabitEthernet1/0/2 加入到 VLAN 10。

```
[Router-vlan10] port gigabitethernet 1/0/2
```

将接口 GigabitEthernet1/0/5 加入到 VLAN 10。

```
[Router-vlan10] port gigabitethernet 1/0/5
Permission denied.
```

1.10.3 Telnet用户的HWTACACS用户角色切换认证配置

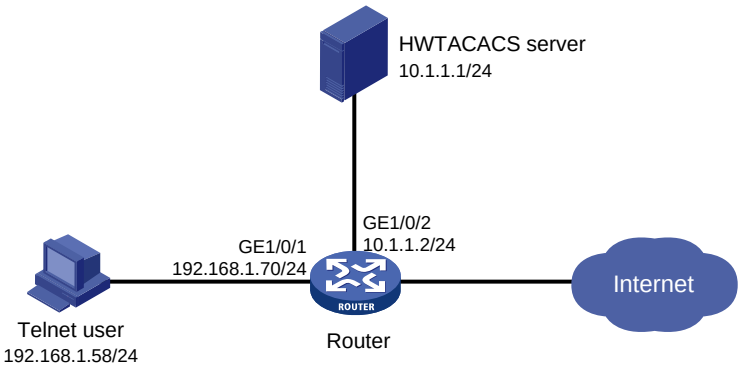
1. 组网需求

如图 1-3 所示，Telnet 用户主机与 Router 直接相连，Router 与一台 HWTACACS 服务器相连，需要配置 Router 实现对登录 Router 的 Telnet 用户进行用户级别切换认证。具体要求如下：

Telnet 用户登录 Router 时进行本地认证，登录后被授予用户角色 level-0，当进行 level-0～level-3 之间的任意用户角色切换或切换到 network-admin 用户角色时，首先使用 HWTACACS 认证，若 AAA 配置无效或者 HWTACACS 服务器没有响应则转为 **local** 认证。

2. 组网图

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



3. 配置思路

在 Router 上的配置思路如下：

(1) 配置 Telnet 用户登录采用 AAA 认证方式（**scheme**），并且使用 AAA 中的本地认证。

- 创建 ISP 域 bbb，配置 Telnet 用户登录时采用的 **login** 认证和授权方法为 **local**，计费方式为不计费。
- 创建本地用户，配置 Telnet 用户登录密码及登录后的用户角色。

(2) Telnet 用户进行用户角色切换时，首先使用 HWTACACS 认证，若 AAA 配置无效或者 HWTACACS 服务器没有响应则转为本地认证。

- 配置用户角色切换认证方式为 **scheme local**。
- 配置 HWTACACS 方案 hwtac，指定 HWTACACS 服务器 IP 地址及与其进行交互的相关参数（HWTACACS 协议报文交互时使用的共享密钥，Router 发送给 HWTACACS 服务器的用户名不带域名）。在 ISP 域 bbb 下配置用户角色切换认证方法为 HWTACACS 方案 hwtac。
- 配置采用本地认证方式时的用户角色切换密码。

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

4. 配置步骤

(1) 配置 Router

配置接口 GigabitEthernet1/0/1 的 IP 地址，Telnet 客户端将通过该地址连接 Router。

```
<Router> system-view
[Router] interface gigabitethernet 1/0/1
[Router-GigabitEthernet1/0/1] ip address 192.168.1.70 255.255.255.0
[Router-GigabitEthernet1/0/1] quit
```

配置接口 GigabitEthernet1/0/2 的 IP 地址，Router 将通过该地址与服务器通信。

```
[Router] interface gigabitethernet 1/0/2
[Router-GigabitEthernet1/0/2] ip address 10.1.1.2 255.255.255.0
[Router-GigabitEthernet1/0/2] quit
```

开启 Router 的 Telnet 服务器功能。

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

配置 Telnet 用户登录采用 AAA 认证方式。

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

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

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

创建 HWTACACS 方案 hwtac。

```
[Router] hwtacacs scheme hwtac
```

配置主认证服务器的 IP 地址为 10.1.1.1，认证端口号为 49。

```
[Router-hwtacacs-hwtac] primary authentication 10.1.1.1 49
```

配置与认证服务器交互报文时的共享密钥为 expert。

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

配置向 HWTACACS 服务器发送的用户名不携带域名。

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

创建 ISP 域 bbb。

```
[Router] domain bbb
```

配置 Telnet 用户登录认证方法为本地认证。

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

配置 Telnet 用户登录授权方法为本地授权。

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

配置 Telnet 用户登录计费方法为不计费。

```
[Router-isp-bbb] accounting login none
```

配置用户角色切换认证方法为 hwtac。

```
[Router-isp-bbb] authentication super hwtacacs-scheme hwtac
[Router-isp-bbb] quit
```

创建并配置设备管理类本地 Telnet 用户 test。

```
[Router] local-user test class manage
[Router-luser-manage-test] service-type telnet
[Router-luser-manage-test] password simple aabbcc
```

指定 Telnet 用户登录系统后被授予的用户角色为 level-0。

```
[Router-luser-manage-test] authorization-attribute user-role level-0
```

为保证 Telnet 用户仅使用授权的用户角色 level-0，删除用户 test 具有的缺省用户角色 network-operator。

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

配置用户角色切换认证方式为本地认证时，切换到用户角色 level-3 时使用的密码为 654321。

```
[Router] super password role level-3 simple 654321
```

配置切换到用户角色 network-admin 时使用的密码为 654321。

```
[Router] super password role network-admin simple 654321
[Router] quit
```

(2) 配置 HWTACACS server

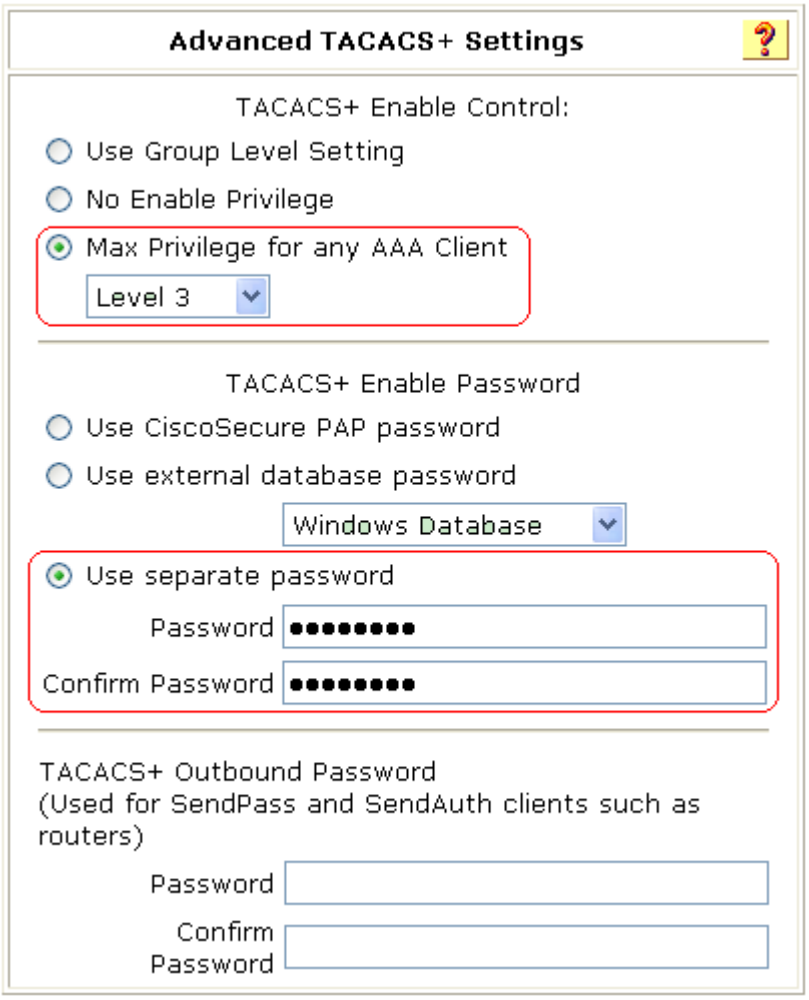
说明

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

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

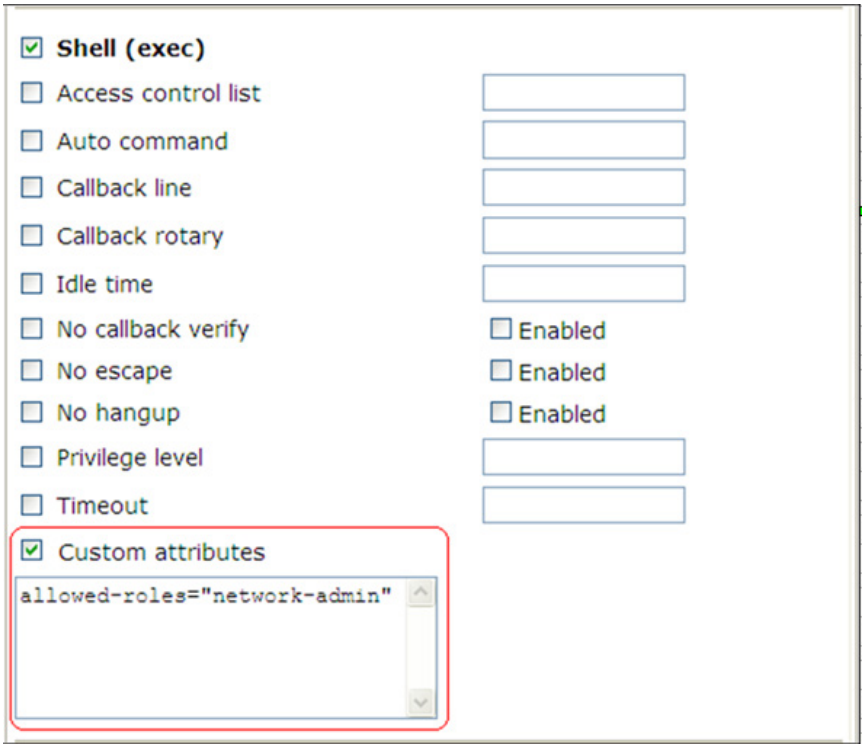
- 设置 Enable Password 为 enabpass；
- 设置 Max Privilege 为 Level 3，表示用户角色在 level-0 到 level-3 之间任意切换时均使用密码 enabpass 进行认证。如果目的切换角色仅仅为 network-admin，则 Max Privilege 可以设置为任意 Level。

图1-4 设置 Telnet 用户的高级属性



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

图1-5 设置 Telnet 用户的 HWTACACS 属性



5. 验证配置

(1) Telnet 用户建立与 Router 的连接

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

```
<Router> telnet 192.168.1.70
Trying 192.168.1.70 ...
Press CTRL+K to abort
Connected to 192.168.1.59 ...
******************************************************************************
* Copyright (c) 2004-2018 New H3C Technologies Co., Ltd. All rights reserved.*
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************

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

```
  tracert      Tracert function

<Router>
```

(2) 切换用户角色

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

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

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

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

切换到用户角色 level-0、level-1、level-2、network-admin 的过程同上。

1.10.4 Telnet 用户的RADIUS用户角色切换认证配置

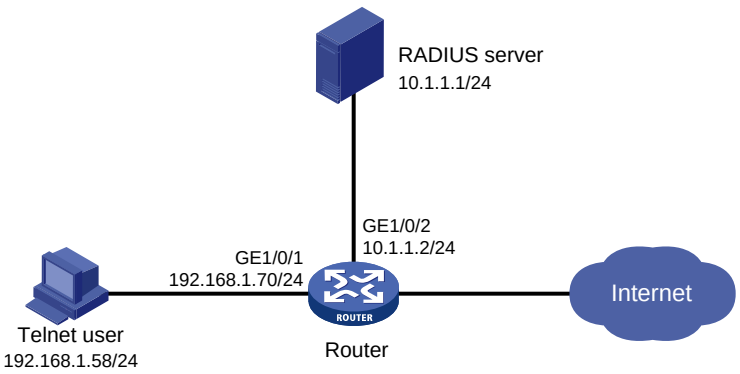
1. 组网需求

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

Telnet 用户登录 Router 时进行本地认证，登录后被授予用户角色 level-0，当切换到用户角色 network-admin 时，首先使用 RADIUS 认证，若 AAA 配置无效或者 RADIUS 服务器没有响应则转为 **local** 认证。

2. 组网图

图1-6 Telnet 用户远端 RADIUS 用户角色切换认证配置组网图



3. 配置思路

在 Router 上的配置思路如下：

(1) 配置 Telnet 用户登录采用 AAA 认证方式（**scheme**），并且使用 AAA 中的本地认证。

- 创建 ISP 域 bbb，配置 Telnet 用户登录时采用的 **login** 认证和授权方法为 **local**，计费方式为不计费。
- 创建本地用户，配置 Telnet 用户登录密码及登录后的用户角色。

(2) Telnet 用户进行用户角色切换时，首先使用 RADIUS 认证，若 AAA 配置无效或者 RADIUS 服务器没有响应则转为本地认证。

- 配置用户角色切换认证方式为 **scheme local**。
- 配置 RADIUS 方案 radius，指定 RADIUS 服务器 IP 地址及与其进行交互的相关参数（RADIUS 协议报文交互时使用的共享密钥，Router 发送给 RADIUS 服务器的用户名不带域名）。在 ISP 域 bbb 下配置用户角色切换认证方法为 RADIUS 方案 radius。
- 配置采用本地认证方式时的用户角色切换密码。

在 RADIUS server 上需要添加用于用户角色切换认证的用户名“$enab0$”和密码。

4. 配置步骤

(1) 配置 Router

配置接口 GigabitEthernet1/0/1 的 IP 地址，Telnet 客户端将通过该地址连接 Router。

```
<Router> system-view
[Router] interface gigabitethernet 1/0/1
[Router-GigabitEthernet1/0/1] ip address 192.168.1.70 255.255.255.0
[Router-GigabitEthernet1/0/1] quit
```

配置接口 GigabitEthernet1/0/2 的 IP 地址，Router 将通过该地址与服务器通信。

```
[Switch] interface gigabitethernet 1/0/2
[Router-GigabitEthernet1/0/2] ip address 10.1.1.2 255.255.255.0
[Router-GigabitEthernet1/0/2] quit
```

开启 Router 的 Telnet 服务器功能。

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

配置 Telnet 用户登录采用 AAA 认证方式。

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

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

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

创建 RADIUS 方案 radius。

```
[Router] radius scheme radius
```

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

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

配置向 RADIUS 服务器发送的用户名不携带域名。

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

创建 ISP 域 bbb。

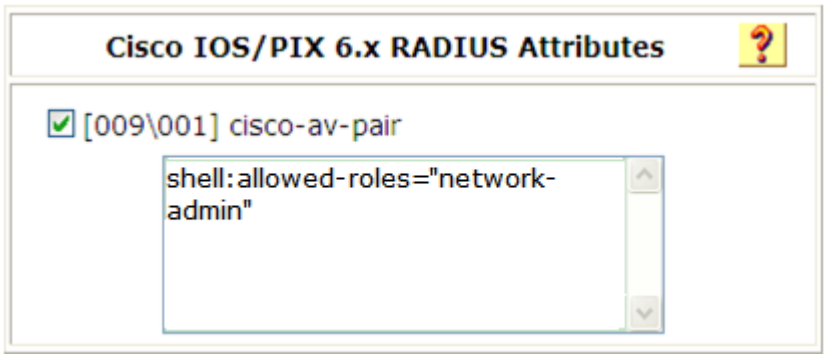
```
[Router] domain bbb
```
配置 Telnet 用户登录认证方法为本地认证。
```
[Router-isp-bbb] authentication login local
```
配置 Telnet 用户登录授权方法为本地授权。
```
[Router-isp-bbb] authorization login local
```
配置 Telnet 用户登录计费方法为不计费本地授权。
```
[Router-isp-bbb] accounting login none
```
配置用户角色切换认证方法为 radius。
```
[Router-isp-bbb] authentication super radius-scheme radius
[Router-isp-bbb] quit
```
创建并配置设备管理类本地 Telnet 用户 test。
```
[Router] local-user test class manage
[Router-luser-manage-test] service-type telnet
[Router-luser-manage-test] password simple aabbcc
```
指定 Telnet 用户登录系统后被授予的用户角色为 level-0。
```
[Router-luser-manage-test] authorization-attribute user-role level-0
```
为保证 Telnet 用户仅使用授权的用户角色 level-0，删除用户 test 具有的缺省用户角色 network-operator。
```
[Router-luser-manage-test] undo authorization-attribute user-role network-operator
[Router-luser-manage-test] quit
```
配置用户角色切换认证方式为本地认证时，切换到用户角色 network-admin 时使用的密码为 abcdef654321。
```
[Router] super password role network-admin simple abcdef654321
[Router] quit
```
(2) 配置 RADIUS server


说明

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

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

图1-7 设置 Telnet 用户的 RADIUS 属性



5. 验证配置

(1) Telnet 用户建立与 Router 的连接

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

```
<Router> telnet 192.168.1.70
Trying 192.168.1.70 ...
Press CTRL+K to abort
Connected to 192.168.1.59 ...
******************************************************************************
* Copyright (c) 2004-2018 New H3C Technologies Co., Ltd. All rights reserved.*
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************

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

<Router>
```

(2) 切换用户角色

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

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

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

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

1.11 常见配置错误举例

1.11.1 被授权的用户角色与本地用户实际拥有的权限不符

1. 故障现象

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

2. 故障分析

可能是该本地用户被授权了其它用户角色，例如该本地用户还具有缺省的用户角色。

3. 处理过程

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

1.11.2 使用远程认证服务器进行身份认证的用户登录设备失败

1. 故障现象

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

2. 故障分析

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

3. 处理过程

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

目 录

1 登录设备方式介绍

设备各款型对于 AUX 口的支持情况有所不同，详细差异信息如下：

型号	特性	描述
MSR810/810-W/810-W-DB/810-LM/810-W-LM/810-10-PoE/810-LM-HK/810-W-LM-HK/810-LMS/810-LUS	AUX口	不支持
MSR2600-6-X1/2600-10-X1		• MSR2600-6-X1：不支持 • MSR2600-10-X1：支持
MSR 2630		支持
MSR3600-28/3600-51		支持
MSR3600-28-SI/3600-51-SI		不支持
MSR3610-X1/3610-X1-DP/3610-X1-DC/3610-X1-DP-DC		不支持
MSR 3610/3620/3620-DP/3640/3660		支持
MSR5620/5660/5680		支持

型号	特性	描述
MSR810-W-WiNet/810-LM-WiNet	AUX口	不支持
MSR830-4LM-WiNet		不支持
MSR830-5BEI-WiNet/830-6EI-WiNet/830-10BEI-WiNet		不支持
MSR830-6BHI-WiNet/830-10BHI-WiNet		不支持
MSR2600-10-X1-WiNet		支持
MSR2630-WiNet		支持
MSR3600-28-WiNet		支持
MSR3610-X1-WiNet		不支持
MSR3610-WiNet/3620-10-WiNet/3620-DP-WiNet/3620-WiNet/3660-WiNet		支持

型号	特性	描述
MSR810-LM-GL	AUX口	不支持
MSR810-W-LM-GL		不支持
MSR830-6EI-GL		不支持
MSR830-10EI-GL		不支持
MSR830-6HI-GL		不支持

型号	特性	描述
MSR830-10HI-GL		不支持
MSR2600-6-X1-GL		不支持
MSR3600-28-SI-GL		不支持

设备支持 CLI（Command Line Interface，命令行接口）、Web 和 SNMP（Simple Network Management Protocol，简单网络管理协议）三种登录方式：

- 通过 CLI 登录设备后，可以直接输入命令行，来配置和管理设备。CLI 方式下又根据使用的登录接口以及登录协议不同，分为：通过 Console 口、AUX 口、Telnet 或 SSH 登录方式。
- 通过 Web 登录设备后，用户可以使用 Web 界面直观地管理和维护网络设备。
- 通过 SNMP 登录设备后，NMS 可以通过 Set 和 Get 等操作来配置和管理设备。关于 SNMP 的详细介绍请参见“网络管理与维护配置指导”中的“SNMP”。

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

表1-1 各种登录设备方式的最小配置描述表

登录方式	缺省情况最小配置描述
配置通过Console口/AUX口本地登录设备	缺省情况下，Console口登录时认证方式为none，存在安全隐患。用户在首次登录后，可以通过修改Console口登录的认证方式以及其它参数来增强设备的安全性 对于AUX口进行本地登录，首先配置password认证方式的密码，或者更改认证方式并完成相关参数的设置（缺省情况下，AUX用户采用password认证方式，但密码为空，回车即可成功登录），然后配置AUX用户的用户角色（缺省情况下，AUX用户的角色为network-operator）
配置通过Telnet登录设备	• 开启设备的 Telnet 功能 • 配置 IP 地址，并确保设备与 Telnet 登录用户间路由可达（缺省情况下，设备未配置 IP 地址） • 配置 password 认证方式的密码，或者更改认证方式并完成相关参数的设置（缺省情况下，VTY 用户采用 password 认证方式） • 配置 VTY 用户的用户角色（缺省情况下，VTY 用户的角色为 network-operator）
配置通过SSH登录设备	• 开启设备 SSH 功能并完成 SSH 属性的配置 • 配置 IP 地址，并确保设备与 SSH 登录用户间路由可达（缺省情况下，设备未配置 IP 地址） • 配置 VTY 用户的认证方式为 scheme（缺省情况下，VTY 用户采用 password 认证方式） • 配置 VTY 用户的用户角色（缺省情况下，VTY 用户的角色为 network-operator）
配置通过Web登录设备	• 配置设备 IP 地址，确保设备与 Web 登录用户间路由可达（缺省情况下，设备未配置 IP 地址） • 配置 Web 用户的用户名与密码（缺省情况下，设备未创建 Web 用户名和密码） • 配置 Web 用户的用户角色（缺省情况下，Web 用户的角色为 network-operator） • 配置 Web 用户的服务类型为 http 或者 https（缺省情况下，未配置 Web 登录用户的服

登录方式	缺省情况最小配置描述
	务类型）
配置通过SNMP登录设备	• 配置 IP 地址，并确保设备与 NMS 登录用户间路由可达（缺省情况下，设备未配置 IP 地址） • 配置 SNMP 基本参数

2 缺省情况下如何通过Console口登录设备

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

通过 Console 口登录设备时，请按照以下步骤进行操作：

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

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

提示

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

图2-1 将设备与 PC 通过配置口电缆进行连接

(3) 给 PC 上电。

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

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

说明

如果 PC 使用的是 Windows Server2003 操作系统，请在 Windows 组件中添加超级终端程序后，再按照本文介绍的方式登录和管理设备；如果 PC 使用的是 Windows Server 2008、Windows Vista、Windows 7 或其它操作系统，请准备第三方的终端控制软件，使用方法请参照软件的使用指导或联机帮助。

(5) 设备上电，终端上显示设备自检信息，自检结束后提示用户键入回车，出现命令行提示符后即可键入命令来配置设备或查看设备运行状态，需要帮助可以随时键入?。

3 配置通过CLI登录设备

3.1 配置通过CLI登录设备简介

说明

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

设备各款型对于 AUX 口的支持情况有所不同，详细差异信息如下：

型号	特性	描述
MSR810/810-W/810-W-DB/810-LM/810-W-LM/810-10-PoE/810-LM-HK/810-W-LM-HK/810-LMS/810-LUS	AUX口	不支持
MSR2600-6-X1/2600-10-X1		• MSR2600-6-X1：不支持 • MSR2600-10-X1：支持
MSR 2630		支持
MSR3600-28/3600-51		支持
MSR3600-28-SI/3600-51-SI		不支持
MSR3610-X1/3610-X1-DP/3610-X1-DC/3610-X1-DP-DC		不支持
MSR 3610/3620/3620-DP/3640/3660		支持
MSR5620/5660/5680		支持

型号	特性	描述
MSR810-W-WiNet/810-LM-WiNet	AUX口	不支持
MSR830-4LM-WiNet		不支持
MSR830-5BEI-WiNet/830-6EI-WiNet/830-10BEI-WiNet		不支持
MSR830-6BHI-WiNet/830-10BHI-WiNet		不支持
MSR2600-10-X1-WiNet		支持
MSR2630-WiNet		支持
MSR3600-28-WiNet		支持
MSR3610-X1-WiNet		不支持
MSR3610-WiNet/3620-10-WiNet/3620-DP-WiNet/3620-WiNet/3660-WiNet		支持

型号	特性	描述
MSR810-LM-GL	AUX口	不支持
MSR810-W-LM-GL		不支持
MSR830-6EI-GL		不支持
MSR830-10EI-GL		不支持
MSR830-6HI-GL		不支持
MSR830-10HI-GL		不支持
MSR2600-6-X1-GL		不支持
MSR3600-28-SI-GL		不支持

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

- 缺省情况下，用户不需要任何认证即可通过 Console 口登录设备，这给设备带来许多安全隐患。
- 缺省情况下，如设备上既有 Console 口又有 AUX 口，当用户通过 AUX 口进行本地设备登录时，用户认证方式为 password，但密码为空（回车即可登录），这给设备带来许多安全隐患。
- 缺省情况下，用户不能通过 Telnet 以及 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。

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

3.1.1 用户线简介

用户线用于管理、限制 CLI 登录用户的访问行为：网络管理员可以给每个用户线配置一系列参数，比如用户登录时是否需要认证、用户登录后的角色等。当用户使用 Console 口、AUX 口、Telnet 及 SSH 登录到设备的时候，系统会给用户分配一个用户线，登录用户将受到该用户线下配置参数的约束。

1. 用户线概述

设备提供了三种类型的用户线：

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

2. 用户与用户线的关系

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

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

如果没有空闲的、相应类型的用户线可分配，则用户不能登录设备。

3. 用户线的编号

用户线的编号有两种方式：绝对编号方式和相对编号方式。

(1) 绝对编号方式

使用绝对编号方式，可以唯一的指定一个用户线。绝对编号从 0 开始自动编号，每次增长 1，先给所有 Console 用户线编号，然后是所有 AUX 用户线，最后是所有 VTY 用户线。使用 **display line**（不带参数）可查看到设备当前支持的用户线以及它们的绝对编号。

(2) 相对编号方式

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

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

3.1.2 认证方式简介

在用户线下配置认证方式，可以要求当用户使用指定用户线登录时是否需要认证，以提高设备的安全性。非 FIPS 模式下，设备支持的认证方式有 none、password 和 scheme 三种；FIPS 模式下，设备仅支持 scheme 认证方式。

- 认证方式为 none：表示下次使用该用户线登录时不需要进行用户名和密码认证，任何人都可以登录到设备上，这种情况可能会带来安全隐患。
- 认证方式为 password：表示下次使用该用户线登录时，需要输入密码。只有密码正确，用户才能登录到设备上。配置认证方式为 password 后，请妥善保存密码。
- 认证方式为 scheme：表示下次使用该用户线登录设备时需要进行用户名和密码认证，用户名或密码错误，均会导致登录失败。配置认证方式为 scheme 后，请妥善保存用户名及密码。

认证方式不同，配置不同，具体配置如表 3-1 所示。

表3-1 不同认证方式下配置任务简介

认证方式	认证所需配置	说明
none	设置登录用户的认证方式为不认证	具体配置请见各登录方式下的相关章节
password	设置登录用户的认证方式为password认证	具体配置请见各登录方式下的相关章节
	设置密码认证的密码	
scheme	设置登录用户的认证方式为scheme认证	具体配置请见各登录方式下的相关章节
	在ISP域视图下为login用户配置认证方法	请参见“安全配置指导”中的“AAA”

3.1.3 用户角色简介

用户角色对登录用户至关重要，角色中定义了允许用户操作哪些系统功能以及资源对象，即用户登录后可以执行哪些命令。关于用户角色的详细描述以及配置请参见“基础配置指导”中的“RBAC”。

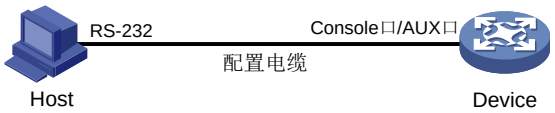
- 对于 none 和 password 认证方式，登录用户的角色由用户线下的用户角色配置决定。
- 对于 scheme 认证方式，且用户通过 SSH 的 publickey 或 password-publickey 方式登录设备时，登录用户将被授予同名的设备管理类本地用户视图下配置的授权用户角色。
- 对于 scheme 认证方式，非 SSH 登录以及用户通过 SSH 的 password 方式登录设备时，登录用户使用 AAA 认证用户的角色配置。尤其对于远程 AAA 认证用户，如果 AAA 服务器没有下发用户角色且缺省用户角色授权功能处于关闭状态时，用户将不能登录设备。

3.2 配置通过Console口/AUX口本地登录设备

通过 Console 口/AUX 口进行本地登录是登录设备的基本方式之一，用户可以使用本地链路登录设备，便于系统维护。如图 3-1 和图 3-2 所示。

图3-1 通过 Console 口登录设备示意图

图3-2 通过 Console 口/AUX 口登录设备示意图



如设备上既有 Console 口又有 AUX 口：

- 当用户通过 Console 口登录设备时，缺省认证方式为 none（不需要用户名和密码），用户角色为 network-admin。用户可以修改认证方式、用户角色以及其它登录参数，来增加设备的安全性及可管理性。
- 当用户通过 AUX 口进行本地设备登录时，缺省认证方式为 password，但密码为空（回车即可登录），用户角色为 network-operator。关于角色 network-operator 权限的详细介绍，请参见“基础配置”中的“RBAC”。

3.2.1 通过Console口/AUX口登录设备配置任务简介

表3-2 通过 Console 口/AUX 口登录设备配置任务简介

配置任务		说明	详细配置
配置通过Console口/AUX	配置通过Console口/AUX口登录设备时无需认证（none）	必选 请根据实际需要选	3.2.2 1.
	配置通过Console口/AUX口登录设备时采用密码认证		3.2.2 2.

配置任务		说明	详细配置
口登录设备时的认证方式	（password）	择其中的一种认证方式 FIPS模式下，仅支持AAA认证（scheme）	
	配置通过Console口/AUX口登录设备时采用AAA认证（scheme）		3.2.2 3.
配置Console口/AUX口登录方式的公共属性		可选	3.2.2 4.

说明

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

3.2.2 配置通过Console口/AUX口登录设备

1. 配置通过Console口/AUX口登录设备时无需认证（none）

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

表3-3 配置用户通过 Console 口/AUX 口登录设备时无需认证

操作	命令	说明
进入系统视图	**system-view**	-
进入Console/AUX用户线视图	**line** { **aux** | **console** } *first-number* [*last-number*]	二者选其一 • 用户线视图下的配置优先于用户线类视图下的配置 • 用户线视图下的配置只对该用户线生效 • 用户线类视图下的配置修改不会立即生效，当用户下次登录后所修改的配置值才会生效 • 用户线视图下的属性配置为缺省值时，将采用用户线类视图下配置的值。如果用户线类视图下的属性配置也为缺省值时，则直接采用该属性的缺省值
进入Console/AUX用户线类视图	**line class** { **aux** | **console** }	
设置登录用户的认证方式为不认证	**authentication-mode none**	非FIPS模式：缺省情况下，用户通过Console口登录，认证方式为**none**；用户通过AUX口登录，认证方式为**password** FIPS模式：缺省情况下，用户登录设备的认证方式为**scheme**
配置从当前用户线登录设备的用户角色	**user-role** *role-name*	缺省情况下，通过Console口登录设备的用户角色为network-admin；通过AUX口登录设备的用户角色为network-operator

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

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

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

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

操作	命令	说明
进入系统视图	**system-view**	-
进入Console/AUX用户线视图	**line** { **aux** | **console** } *first-number* [*last-number*]	二者选其一 • 用户线视图下的配置优先于用户线类视图下的配置 • 用户线视图下的配置只对该用户线生效 • 用户线类视图下的配置修改不会立即生效，当用户下次登录后所修改的配置值才会生效 • 用户线视图下的属性配置为缺省值时，将采用用户线类视图下配置的值。如果用户线类视图下的属性配置也为缺省值时，则直接采用该属性的缺省值
进入Console/AUX用户线类视图	**line class** { **aux** | **console** }	
设置登录用户的认证方式为密码认证	**authentication-mode password**	非FIPS模式：缺省情况下，用户通过Console口登录，认证方式为**none**；用户通过AUX口登录，认证方式为**password** FIPS模式：缺省情况下，用户登录设备的认证方式为**scheme**
设置认证密码	**set authentication password** { **hash** | **simple** } *password*	缺省情况下，未设置认证密码
配置从当前用户线登录设备的用户角色	**user-role** *role-name*	缺省情况下，通过Console口登录设备的用户角色为network-admin；通过AUX口登录设备的用户角色为network-operator

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

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

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

要使配置的 AAA 认证方式生效，还需要在 ISP 域视图下配置 login 认证方法。如果选择本地认证，请配置本地用户及相关属性；如果选择远程认证，请配置 RADIUS、HWTACACS 或 LDAP 方案。相关详细介绍请参见“安全配置指导”中的“AAA”。

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

操作	命令	说明
进入系统视图	**system-view**	-
进入Console/AUX用户线视图	**line** { **aux** | **console** } *first-number* [*last-number*]	二者选其一 • 用户线视图下的配置优先于用户线类视图下的配置 • 用户线视图下的配置只对该用户线生效 • 用户线类视图下的配置修改不会立即生效，当用户下次登录后所修改的配置值才会生效 • 用户线视图下的属性配置为缺省值时，将采用用
进入Console/AUX用户线类视图	**line class** { **aux** | **console** }	

操作	命令	说明
		户线类视图下配置的值。如果用户线类视图下的属性配置也为缺省值时，则直接采用该属性的缺省值
设置登录用户的认证方式为通过AAA认证	**authentication-mode scheme**	非FIPS模式：缺省情况下，用户通过Console口登录，认证方式为**none**；用户通过AUX口登录，认证方式为**password** FIPS模式：缺省情况下，用户登录设备的认证方式为**scheme**

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

4. 配置Console口/AUX口登录方式的公共属性

提示

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

表3-6 配置 Console 口/AUX 口登录方式的公共属性

操作	命令	说明
进入系统视图	**system-view**	-
进入Console/AUX用户线视图	**line** { **aux** | **console** } *first-number* [*last-number*]	二者选其一 • 用户线视图下的配置优先于用户线类视图下的配置 • 用户线视图下的配置只对该用户线生效 • 用户线类视图下的配置修改不会立即生效，当用户下次登录后所修改的配置值才会生效 • 用户线视图下的属性配置为缺省值时，将采用用户线类视图下配置的值。如果用户线类视图下的属性配置也为缺省值时，则直接采用该属性的缺省值
进入Console/AUX用户线类视图	**line class** { **aux** | **console** }	
配置传输速率	**speed** *speed-value*	缺省情况下，Console口/AUX口使用的传输速率为9600bit/s 传输速率为设备与访问终端之间每秒钟传送的比特的个数 用户线类视图下不支持该命令
配置校验方式	**parity** { **even** | **mark** | **none** | **odd**	缺省情况下，Console口/AUX口的校验方式为**none**，

操作	命令	说明
	| space }	即不进行校验 用户线类视图下不支持该命令
配置停止位	**stopbits** { **1** | **1.5** | **2** }	缺省情况下，Console口/AUX口的停止位为1 停止位用来表示单个包的结束。停止位的位数越多，传输效率越低 用户线类视图下不支持该命令
配置数据位	**databits** { **5 | 6 | 7** | **8** }	缺省情况下，Console口/AUX口的数据位为8位 数据位的设置取决于需要传送字符的编码类型。如果传送的是标准的ASCII码，则可以将数据位设置为7，如果传输的是扩展的ASCII码，则需要将数据位设置为8 用户线类视图下不支持该命令
配置启动终端会话的快捷键	**activation-key** *character*	缺省情况下，按<Enter>键启动终端会话
配置中止当前运行任务的快捷键	**escape-key** { *character* | **default** }	缺省情况下，键入<Ctrl+C>中止当前运行的任务
配置对当前用户线进行锁定并重新认证的快捷键	**lock-key** *key-string*	缺省情况下，未配置对当前用户线进行锁定并重新认证的快捷键
配置流量控制方式	**flow-control** { **hardware** | **none** | **software** } **flow-control hardware** *flow-control-type1* [**software** *flow-control-type2*] **flow-control software** *flow-control-type1* [**hardware** *flow-control-type2*]	用户线类视图下不支持该命令
配置终端的显示类型	**terminal type** { **ansi | vt100** }	缺省情况下，终端显示类型为ANSI 当设备的终端类型与客户端（如超级终端或者Telnet客户端等）的终端类型不一致，或者均设置为ANSI，并且当前编辑的命令行的总字符数超过80个字符时，客户端会出现光标错位、终端屏幕不能正常显示的现象。建议两端都设置为VT100类型
设置终端屏幕一屏显示的行数	**screen-length** *screen-length*	缺省情况下，终端屏幕一屏显示的行数为24行 **screen-length** 0表示关闭分屏显示功能
设置历史命令缓冲区大小	**history-command max-size** *value*	缺省情况下，每个用户的历史缓冲区的大小为10，即可存放10条历史命令
设置用户线的超时时间	**idle-timeout** *minutes* [*seconds*]	缺省情况下，所有的用户线的超时时间为10分钟，如果直到超时时间到达，某用户线一直没有用户进行操作，则该用户线将自动断开 **idle-timeout** 0表示永远不会超时
设置终端线路的自动执行的命令	**auto-execute command** *command*	缺省情况下，终端线路未设置自动执行命令 当配置自动执行的命令后，登录到终端线路，所配置的命令会自动执行*command*，然后退出当前连接 对于没有AUX用户线，只有Console用户线的设备，

操作	命令	说明
		Console用户线/Console用户线类视图下不支持该命令 对于有Console用户线，又有AUX用户线的设备，Console用户线/Console用户线类视图下不支持该命令，AUX用户线/AUX用户线类视图下支持该命令
设置在终端线路上启动终端服务	**shell**	缺省情况下，所有用户线的终端服务功能处于开启状态 对于没有AUX用户线，只有Console用户线的设备，Console用户线/Console用户线类视图下不支持该命令 对于有Console用户线，又有AUX用户线的设备，Console用户线视图下不支持**undo shell**命令，AUX用户线视图下支持该命令

3.3 配置通过Telnet登录设备

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

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

说明

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

3.3.1 配置设备作为Telnet服务器

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

1. 配置设备作为Telnet服务器的配置任务简介

表3-7 配置设备作为 Telnet 服务器的配置任务简介

配置任务		说明	详细配置
配置设备作为Telnet服务器时的认证方式	配置Telnet登录设备时无需认证（none）	必选 请根据实际需要选择其中的一种认证方式	3.3.1 2.
	配置Telnet登录设备时采用密码认证（password）		3.3.1 3.
	配置Telnet登录设备时采用AAA认证（scheme）		3.3.1 4.
配置Telnet服务器发送报文的DSCP优先级		可选	3.3.1 5.
配置VTY用户线的公共属性		可选	3.3.1 6.

说明

改变 Telnet 登录的认证方式后，新认证方式对新登录的用户生效。

2. 配置Telnet登录设备时无需认证（none）

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

表3-8 认证方式为 none 的配置

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

3. 配置Telnet登录设备时采用密码认证（password）

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

表3-9 认证方式为 password 的配置

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

操作	命令	说明
线视图		• 用户线视图下的配置优先于用户线类视图下的配置 • 用户线视图下的配置只对该用户线生效 • 用户线类视图下的配置修改不会立即生效，当用户下次登录后所修改的配置值才会生效 • 用户线视图下的属性配置为缺省值时，将采用用户线类视图下配置的值。如果用户线类视图下的属性配置也为缺省值时，则直接采用该属性的缺省值
进入VTY用户线类视图	**line class vty**	
设置登录用户的认证方式为密码认证	**authentication-mode password**	非FIPS模式：缺省情况下，VTY用户线的认证方式为**password** 用户线视图下，对**authentication-mode**和**protocol inbound**进行关联绑定，当两条命令中的任意一条配置了非缺省值，那么另外一条取缺省值
设置密码认证的密码	**set authentication password** { **hash** | **simple** } *password*	缺省情况下，未设置密码认证的密码
（可选）配置从当前用户线登录设备的用户角色	**user-role** *role-name*	缺省情况下，通过Telnet登录设备的用户角色为network-operator

4. 配置Telnet登录设备时采用AAA认证（scheme）

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

要使配置的 AAA 认证方式生效，还需要在 ISP 域视图下配置 login 认证方法。如果选择本地认证，请配置本地用户及相关属性；如果选择远程认证，请配置 RADIUS、HWTACACS 或 LDAP 方案。相关详细介绍请参见“安全配置指导”中的“AAA”。

表3-10 配置用户通过 Telnet 登录设备时采用 AAA 认证

操作	命令	说明
进入系统视图	**system-view**	-
开启设备的Telnet服务	**telnet server enable**	缺省情况下，Telnet服务处于关闭状态
进入一个或多个VTY用户线视图	**line vty** *first-number* [*last-number*]	二者选其一 • 用户线视图下的配置优先于用户线类视图下的配置 • 用户线视图下的配置只对该用户线生效 • 用户线类视图下的配置修改不会立即生效，当用户下次登录后所修改的配置值才会生效 • 用户线视图下的属性配置为缺省值时，将采用用户线类视图下配置的值。如果用户线类视图下的属性配置也为缺省值时，则直接采用该
进入VTY用户线类视图	**line class vty**	

操作	命令	说明
		属性的缺省值
设置登录用户的认证方式为通过AAA认证	**authentication-mode scheme**	非FIPS模式：缺省情况下，VTY用户线的认证方式为**password** 用户线视图下，对**authentication-mode**和**protocol inbound**进行关联绑定，当两条命令中的任意一条配置了非缺省值，那么另外一条取缺省值

5. 配置Telnet服务器的公共属性

表3-11 配置 Telnet 服务器的公共属性

操作	命令	说明
进入系统视图	**system-view**	-
配置Telnet服务器发送报文的DSCP优先级	**telnet server dscp** *dscp-value*	缺省情况下，Telnet服务器发送Telnet报文的DSCP优先级48
配置Telnet服务器发送IPv6报文的DSCP优先级	**telnet server ipv6 dscp** *dscp-value*	缺省情况下，IPv6 Telnet服务器发送IPv6 Telnet报文的DSCP优先级48
配置IPv4网络Telnet协议的端口号	**telnet server port** *port-number*	缺省情况下，IPv4网络Telnet协议的端口号为23
配置IPv6网络Telnet协议的端口号	**telnet server ipv6 port** *port-number*	缺省情况下，IPv6网络Telnet协议的端口号为23
配置Telnet登录同时在线的最大用户连接数	**aaa session-limit telnet** *max-sessions*	缺省情况下，Telnet登录同时在线的最大用户连接数为32 该配置对于通过任何一种认证方式（none、password或者scheme）接入设备的用户都生效 配置本命令后，已经在线的用户连接不会受到影响，只对新的用户连接生效。如果当前在线的用户连接数已经达到最大值，则新的连接请求会被拒绝，登录会失败 关于该命令的详细描述，请参见“安全命令参考”中的“AAA”

6. 配置VTY用户线的公共属性

提示

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

表3-12 配置 VTY 用户线的公共属性

操作	命令	说明
进入系统视图	**system-view**	-
进入一个或多个VTY用户线视图	**line vty** *first-number* [*last-number*]	二者选其一 • 用户线视图下的配置优先于用户线类视图下的配置 • 用户线视图下的配置只对该用户线生效 • 用户线类视图下的配置修改不会立即生效，当用户下次登录后所修改的配置值才会生效 • 用户线视图下的属性配置为缺省值时，将采用用户线类视图下配置的值。如果用户线类视图下的属性配置也为缺省值时，则直接采用该属性的缺省值
进入VTY用户线类视图	**line class vty**	
启动终端服务	**shell**	缺省情况下，所有用户线的终端服务功能处于开启状态
配置VTY用户线支持的协议	**protocol inbound** { **all** | **pad** | **ssh** | **telnet** }	缺省情况下，设备同时支持Telnet和SSH协议 使用该命令配置的协议将在用户下次使用该用户线登录时生效 用户线视图下，对**authentication-mode**和**protocol inbound**进行关联绑定，当两条命令中的任意一条配置了非缺省值，那么另外一条取缺省值
配置中止当前运行任务的快捷键	**escape-key** { *character* | **default** }	缺省情况下，键入<Ctrl+C>中止当前运行的任务
配置对当前用户线进行锁定并重新认证的快捷键	**lock-key** *key-string*	缺省情况下，未配置对当前用户线进行锁定并重新认证的快捷键
配置终端的显示类型	**terminal type** { **ansi | vt100** }	缺省情况下，终端显示类型为ANSI
设置终端屏幕一屏显示的行数	**screen-length** *screen-length*	缺省情况下，终端屏幕一屏显示的行数为24行 **screen-length** 0表示关闭分屏显示功能
设置设备历史命令缓冲区大小	**history-command max-size** *value*	缺省情况下，每个用户的历史缓冲区大小为10，即可存放10条历史命令
设置VTY用户线的超时时间	**idle-timeout** *minutes* [*seconds*]	缺省情况下，所有的用户线的超时时间为10分钟 如果10分钟内某用户线没有用户进行操作，则该

操作	命令	说明
		用户线将自动断开 **idle-timeout** 0表示永远不会超时
设置从用户线登录后自动执行的命令	**auto-execute command** *command*	缺省情况下，未配置自动执行命令 配置自动执行命令后，用户在登录时，系统会自动执行已经配置好的命令，执行完命令后，自动断开用户连接。如果这条命令引发起了一个任务，系统会等这个任务执行完毕后再断开连接。该命令通常用来配置Telnet命令，使用户登录时自动连接到指定的主机

3.3.2 配置设备作为Telnet客户端登录其它设备

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

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

图3-3 通过设备登录到其它设备

表3-13 设备作为 Telnet 客户端登录到 Telnet 服务器的配置

操作	命令	说明
进入系统视图	**system-view**	-
（可选）指定设备作为Telnet客户端时，发送Telnet报文的源IPv4地址或源接口	**telnet client source** { **interface** *interface-type interface-number* | **ip** *ip-address* }	缺省情况下，未指定发送Telnet报文的源IPv4地址和源接口，使用报文路由出接口的主IPv4地址作为Telnet报文的源地址
退回到用户视图	**quit**	-
设备作为Telnet客户端登录到Telnet服务器	**telnet** *remote-host* [*service-port*] [**vpn-instance** *vpn-instance-name*] [**source** { **interface** *interface-type interface-number* | **ip** *ip-address* }] [**dscp** *dscp-value*] [**escape** *character*]	二者选其一 此命令在用户视图下执行
	telnet ipv6 *remote-host* [**-i** *interface-type interface-number*] [*port-number*] [**vpn-instance** *vpn-instance-name*] [**source** { **interface** *interface-type interface-number* | **ipv6** *ipv6-address* }] [**dscp** *dscp-value*] [**escape** *character*]	

3.4 配置通过SSH登录设备

3.4.1 通过SSH登录设备简介

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

- 设备可以作为 SSH 服务器，以便用户能够使用 SSH 协议登录到设备进行远程管理和监控。具体请参见“3.4.2 配置设备作为 SSH 服务器”。
- 设备也可以作为 SSH 客户端，使用 SSH 协议登录到别的设备，对别的设备进行管理和监控。具体请参见“3.4.3 配置设备作为 SSH 客户端登录其它设备”。

3.4.2 配置设备作为SSH服务器

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

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

表3-14 设备作为 SSH 服务器时的配置

操作	命令	说明
进入系统视图	**system-view**	-
生成本地密钥对	非FIPS模式下： **public-key local create { dsa | ecdsa secp256r1 | rsa }** FIPS模式下： **public-key local create { ecdsa secp256r1 | rsa }**	缺省情况下，没有生成密钥对
开启SSH服务器功能	**ssh server enable**	缺省情况下，SSH服务器功能处于关闭状态
（可选）建立SSH用户，并指定SSH用户的认证方式	非FIPS模式下： **ssh user** *username* **service-type stelnet authentication-type { password | { any | password-publickey | publickey } assign publickey** *keyname* **}** FIPS模式下： **ssh user** *username* **service-type stelnet authentication-type { password | password-publickey assign publickey** *keyname* **}**	缺省情况下，不存在任何SSH用户
进入VTY用户线视图	**line vty** *first-number* [*last-number*]	二者选其一 • 用户线视图下的配置优先于用户线类视图下的配置 • 用户线视图下的配置只对该用户线生
进入VTY用户线类视图	**line class vty**	

操作	命令	说明
		效 • 用户线类视图下的配置修改不会立即生效，当用户下次登录后所修改的配置值才会生效 • 用户线视图下的属性配置为缺省值时，将采用用户线类视图下配置的值。如果用户线类视图下的属性配置也为缺省值时，则直接采用该属性的缺省值
配置登录用户线的认证方式为**scheme**方式	**authentication-mode scheme**	非FIPS模式下：缺省情况下，VTY用户线认证为**password**方式 FIPS模式下：缺省情况下，VTY用户线认证为**scheme**方式 用户线视图下，对**authentication-mode**和**protocol inbound**进行关联绑定，当两条命令中的任意一条配置了非缺省值，那么另外一条取缺省值
（可选）配置VTY用户线支持的SSH协议	非FIPS模式下： **protocol inbound { all | pad | ssh | telnet }** FIPS模式下： **protocol inbound ssh**	非FIPS模式下：缺省情况下，设备同时支持Telnet和SSH协议 FIPS模式下：缺省情况下，设备支持SSH协议 使用该命令配置的协议将在用户下次使用该用户线登录时生效 用户线视图下，对**authentication-mode**和**protocol inbound**进行关联绑定，当两条命令中的任意一条配置了非缺省值，那么另外一条取缺省值
退回系统视图	**quit**	-
（可选）配置VTY用户线的公共属性	**-**	详细配置请参见“3.3.1 6. 配置VTY用户线的公共属性”
（可选）配置SSH方式登录设备时，同时在线的最大用户连接数	**aaa session-limit ssh** *max-sessions*	缺省情况下，设备支持的最大用户连接数位32 配置本命令后，已经在线的用户连接不会受到影响，只对新的用户连接生效。如果当前在线的用户连接数已经达到最大值，则新的连接请求会被拒绝，登录会失败 关于该命令的详细描述，请参见“安全命令参考”中的“AAA”

3.4.3 配置设备作为SSH客户端登录其它设备

用户已经成功登录到了设备上，并希望将当前设备作为 SSH 客户端登录到其它设备上进行操作，如图 3-4 所示。

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

图3-4 通过设备登录到其它设备

表3-15 设备作为 SSH 客户端登录到其它设备的配置

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

说明

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

3.5 CLI登录显示和维护

表3-16 CLI 显示和维护

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

操作	命令	说明
锁定当前用户线并对其进行重新认证	**lock reauthentication**	在任意视图下执行 缺省情况下，系统不会自动锁定当前用户线并对其进行重新认证 请使用设备登录密码解除锁定并重新登录设备
向指定的用户线发送消息	**send** { **all** | *num1* | { **aux** | **console** | **tty** | **vty** } *num2* }	在用户视图下执行

4 配置通过Web登录设备

设备各款型对于本节所描述的特性的支持情况有所不同，详细差异信息如下：

型号	特性	描述
MSR810/810-W/810-W-DB/810-LM/810-W-LM/810-10-PoE/810-LM-HK/810-W-LM-HK/810-LMS/810-LUS	通过Web登录设备	MSR810/810-W/810-W-DB/810-LM/810-W-LM/810-10-PoE/810-LM-HK/810-W-LM-HK：支持 MSR810-LMS/810-LUS：不支持
MSR2600-6-X1/2600-10-X1		支持
MSR 2630		支持
MSR3600-28/3600-51		支持
MSR3600-28-SI/3600-51-SI		不支持
MSR3610-X1/3610-X1-DP/3610-X1-DC/3610-X1-DP-DC		支持
MSR 3610/3620/3620-DP/3640/3660		支持
MSR5620/5660/5680		不支持

型号	特性	描述
MSR810-W-WiNet/810-LM-WiNet	通过Web登录设备	支持
MSR830-4LM-WiNet		支持
MSR830-5BEI-WiNet/830-6EI-WiNet/830-10BEI-WiNet		支持
MSR830-6BHI-WiNet/830-10BHI-WiNet		支持
MSR2600-10-X1-WiNet		支持
MSR2630-WiNet		支持
MSR3600-28-WiNet		支持
MSR3610-X1-WiNet		支持
MSR3610-WiNet/3620-10-WiNet/3620-DP-WiNet/3620-WiNet/3660-WiNet		支持

型号	特性	描述
MSR810-LM-GL	通过Web登录设备	支持
MSR810-W-LM-GL		支持
MSR830-6EI-GL		支持
MSR830-10EI-GL		支持

型号	特性	描述
MSR830-6HI-GL		支持
MSR830-10HI-GL		支持
MSR2600-6-X1-GL		支持
MSR3600-28-SI-GL		不支持

4.1 通过Web登录设备简介

说明

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

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

设备支持两种 Web 登录方式：

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

缺省情况下，用户不能通过 Web 登录设备。需要先通过 Console 口登录到设备，开启 Web 功能（开启 HTTP 和 HTTPS 服务），并配置设备 IP 地址、Web 用户和认证密码等参数后，才能使用 Web 登录设备。

4.2 配置限制和指导

如果设备上开启了 Lighttpd Web 服务功能，则需要配置 HTTP/HTTPS 服务的端口号为 80/443 之外的其他端口号。

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

4.3 配置通过HTTP方式登录设备

表4-1 配置通过 HTTP 方式登录设备

操作	命令	说明
（可选）配置用户访问Web的固定校验码	**web captcha** *verification-code*	缺省情况下，用户只能使用Web页面显示的校验码访问Web
进入系统视图	**system-view**	-
开启HTTP服务	**ip http enable**	缺省情况下，HTTP服务处于关闭状态
（可选）配置HTTP服务的端口号	**ip http port** *port-number*	缺省情况下，HTTP服务的端口号为80
（可选）配置HTTP服务在响应OPTIONS请求时返回的方法列表	**http method { delete | get | head | options | post | put } ***	缺省情况下，未配置任何方法
（可选）设置Web登录用户连接的超时时间	**web idle-timeout** *minutes*	缺省情况下，Web闲置超时时间为10分钟
（可选）设置同时在线的最大HTTP用户连接数	**aaa session-limit http** *max-sessions*	缺省情况下，最大用户连接数为32 配置本命令后，已经在线的用户连接不会受到影响，只对新的用户连接生效。如果当前在线的用户连接数已经达到最大值，则新的连接请求会被拒绝，登录会失败 关于该命令的详细描述，请参见“安全命令参考”中的“AAA”
（可选）开启Web操作日志输出功能	**webui log enable**	缺省情况下，Web操作日志输出功能处于关闭状态
创建本地用户用于Web登录，并进入本地用户视图	**local-user** *user-name* [**class manage**]	缺省情况下，无本地用户
（可选）设置本地用户的密码	非FIPS模式下： **password** [{ **hash** | **simple** } *password*] FIPS模式下： **password**	用户的密码将在哈希计算后以密文的方式保存到配置文件中 非FIPS模式下： 不存在本地用户密码，即本地用户认证时无需输入密码，只要用户名有效且其它属性验证通过即可认证成功 FIPS模式下： 不存在本地用户密码，但本地用户认证时不能成功
配置Web用户的角色	**authorization-attribute user-role** *user-role*	缺省情况下，Web用户的角色为network-operator
配置Web用户的服务类型为HTTP	**service-type http**	缺省情况下，未配置用户的服务类型

4.4 配置通过HTTPS方式登录设备

HTTPS 登录方式分为以下两种：

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

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4-2 配置通过 HTTPS 方式登录设备

操作	命令	说明
（可选）配置用户访问Web的固定校验码	**web captcha** *verification-code*	缺省情况下，用户只能使用Web页面显示的校验码访问Web
进入系统视图	**system-view**	-
（可选）配置HTTPS服务与SSL服务器端策略关联	**ip https ssl-server-policy** *policy-name*	缺省情况下，HTTPS服务未与SSL服务器端策略关联，HTTPS使用自签名证书 • HTTP 服务和 HTTPS 服务处于开启状态时，对与 HTTPS 服务关联的 SSL 服务器端策略进行的修改不会生效。如需更改 HTTPS 服务与 SSL 服务器端的关联策略，首先执行 **undo ip http enable** 和 **undo ip https enable** 两条命令，再执行 **ip https ssl-server-policy policy-name** 命令，最后重新开启 HTTP 服务和 HTTPS 服务，新的策略即可生效。 • 如需恢复缺省情况，必须先执行 **undo ip http enable** 和 **undo ip https enable** 两条命令，再执行 **undo ip https ssl-server-policy**，最后重新开启 HTTP 服务和 HTTPS 服务即可。
开启HTTPS服务	**ip https enable**	缺省情况下，HTTPS服务处于关闭状态 开启HTTPS服务，会触发SSL的握手协商过程。在SSL握手协商过程中，如果设备的本地证书已经存在，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
（可选）配置HTTPS服务与证书属性访问控制策略关联	**ip https certificate access-control-policy** *policy-name*	缺省情况下，HTTPS服务未与证书属性访问控制策略关联 • 通过将 HTTPS 服务与已配置的客户端证书属性访问控制策略关联，可以实现对客户端的访问权限进行控制，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，

操作	命令	说明
		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”
（可选）配置HTTPS服务的端口	**ip https port** *port-number*	缺省情况下，HTTPS服务的端口号为443
（可选）配置使用HTTPS登录设备时的认证方式	**web https-authorization mode { auto | manual }**	缺省情况下，用户使用HTTPS登录设备时采用的认证模式为**manual**
（可选）设置Web登录用户连接的超时时间	**web idle-timeout** *minutes*	缺省情况下，Web闲置超时时间为10分钟
（可选）设置同时在线的最大HTTPS用户连接数	**aaa session-limit https** *max-sessions*	缺省情况下，最大用户连接数为32 配置本命令后，已经在线的用户连接不会受到影响，只对新的用户连接生效。如果当前在线的用户连接数已经达到最大值，则新的连接请求会被拒绝，登录会失败 关于该命令的详细描述，请参见“安全命令参考”中的“AAA”
（可选）开启Web操作日志输出功能	**webui log enable**	缺省情况下，Web操作日志输出功能处于关闭状态
创建本地用户用于Web登录，并进入本地用户视图	**local-user** *user-name* [**class manage**]	缺省情况下，无本地用户
（可选）设置本地用户的密码	非FIPS模式下： **password** [{ **hash** | **simple** } *password*] FIPS模式下： **password**	用户的密码将在哈希计算后以密文的方式保存到配置文件中 非FIPS模式下： 不存在本地用户密码，即本地用户认证时无需输入密码，只要用户名有效且其它属性验证通过即可认证成功 FIPS模式下： 不存在本地用户密码，但本地用户认证时不能成功
配置Web登录的用户角色	**authorization-attribute user-role** *user-role*	缺省情况下，Web登录的用户角色为network-operator
配置Web登录用户的服务类型为HTTPS	**service-type https**	缺省情况下，未配置用户的服务类型

说明

- HTTPS 服务和 SSL VPN 服务使用相同的端口号时，二者引用的 SSL 服务器端策略必须相同，否则无法同时开启 HTTPS 服务和 SSL VPN 服务。
- HTTPS 服务和 SSL VPN 服务同时开启，并使用相同的端口号时，若要修改引用的 SSL 服务器端策略，则需要先关闭 HTTPS 服务和 SSL VPN 服务，修改 SSL 服务器端策略后，再开启 HTTPS 服务和 SSL VPN 服务，修改后的 SSL 服务器端策略才能生效。

4.5 通过Web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、HTTP 的状态信息和 HTTPS 的状态信息，通过查看显示信息验证配置的效果；可以在用户视图下执行 **free web users** 命令来强制在线 Web 用户下线。

表4-3 Web 用户显示

操作	命令
显示Web用户的相关信息	**display web users**
显示Web的页面菜单树	**display web menu** [**chinese**]
显示HTTP的状态信息	**display ip http**
显示HTTPS的状态信息	**display ip https**
强制在线Web用户下线	**free web users** { **all** | **user-id** *user-id* | **user-name** *user-name* }

4.6 通过Web登录设备典型配置举例

4.6.1 使用HTTP方式登录设备典型配置举例

1. 组网需求

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

2. 组网图

图4-1 配置 HTTP 方式登录组网图

3. 配置步骤

(1) 配置 Device

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 192.168.100.99，子网掩码为 255.255.255.0。

```
[Sysname] interface vlan-interface 999
[Sysname-Vlan-interface999] ip address 192.168.100.99 255.255.255.0
[Sysname-Vlan-interface999] quit
```

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

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

配置开启 HTTP 服务。

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

(2) 配置 PC

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

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

4.6.2 使用HTTPS方式登录设备典型配置举例

1. 组网需求

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

为了满足上述需求，需要进行如下配置：

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

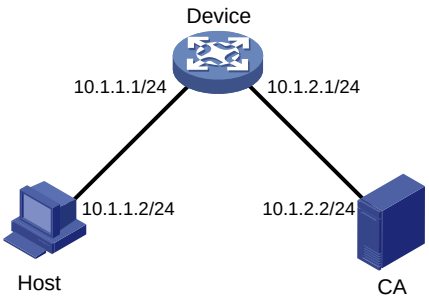
其中，负责为 Device 和 Host 颁发证书的 CA（Certificate Authority，证书颁发机构）名称为 new-ca。

说明

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

2. 组网图

图4-2 HTTPS 配置组网图



3. 配置步骤

(1) 配置 HTTPS 服务器 Device

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

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

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

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

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

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

生成本地的 RSA 密钥对。

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

获取 CA 的证书。

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

为 Device 申请证书。

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

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

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

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

```
[Device] pki certificate attribute-group mygroup1
```

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

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

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

配置 HTTPS 服务与 SSL 服务器端策略 myssl 关联。

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

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

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

开启 HTTPS 服务。

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

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

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

(2) 配置 HTTPS 客户端 Host

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

(3) 验证配置结果

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

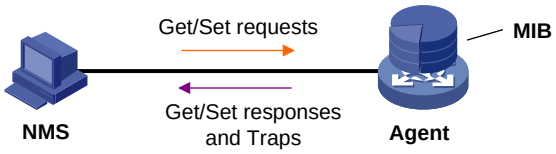
说明

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

5 配置通过SNMP登录设备

使用 SNMP 协议，用户可通过 NMS（Network Management System，网络管理系统）登录到设备上，通过 Set 和 Get 等操作对设备进行管理、配置，如图 5-1 所示。设备支持多种 NMS 软件，如 iMC 等。

图5-1 通过 SNMP 登录设备组网图



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

6 对登录用户的控制

设备各款型对于 AUX 口的支持情况有所不同，详细差异信息如下：

型号	特性	描述
MSR810/810-W/810-W-DB/810-LM/810-W-LM/810-10-PoE/810-LM-HK/810-W-LM-HK/810-LMS/810-LUS	AUX口	不支持
MSR2600-6-X1/2600-10-X1		• MSR2600-6-X1：不支持 • MSR2600-10-X1：支持
MSR 2630		支持
MSR3600-28/3600-51		支持
MSR3600-28-SI/3600-51-SI		不支持
MSR3610-X1/3610-X1-DP/3610-X1-DC/3610-X1-DP-DC		不支持
MSR 3610/3620/3620-DP/3640/3660		支持
MSR5620/5660/5680		支持

型号	特性	描述
MSR810-W-WiNet/810-LM-WiNet	AUX口	不支持
MSR830-4LM-WiNet		不支持
MSR830-5BEI-WiNet/830-6EI-WiNet/830-10BEI-WiNet		不支持
MSR830-6BHI-WiNet/830-10BHI-WiNet		不支持
MSR2600-10-X1-WiNet		支持
MSR2630-WiNet		支持
MSR3600-28-WiNet		支持
MSR3610-X1-WiNet		不支持
MSR3610-WiNet/3620-10-WiNet/3620-DP-WiNet/3620-WiNet/3660-WiNet		支持

型号	特性	描述
MSR810-LM-GL	AUX口	不支持
MSR810-W-LM-GL		不支持
MSR830-6EI-GL		不支持
MSR830-10EI-GL		不支持
MSR830-6HI-GL		不支持

型号	特性	描述
MSR830-10HI-GL		不支持
MSR2600-6-X1-GL		不支持
MSR3600-28-SI-GL		不支持

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

- 当未引用 ACL、或者引用的 ACL 不存在、或者引用的 ACL 为空时，允许所有登录用户访问设备；
- 当引用的 ACL 非空时，则只有 ACL 中 permit 的用户才能访问设备，其它用户不允许访问设备，以免非法用户使用 Telnet/SSH 访问设备。

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

用户登录后，可以通过 AAA 功能来对用户使用的命令行进行授权和计费。

6.1 配置对Telnet/SSH用户的控制

6.1.1 配置准备

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

6.1.2 配置对Telnet/SSH用户的控制

表6-1 配置对 Telnet 用户的控制

操作	命令	说明
进入系统视图	**system-view**	-
使用ACL限制哪些Telnet客户端可以访问设备	**telnet server acl** *acl-number*	请根据需要选择 缺省情况下，未使用ACL限制Telnet客户端
	telnet server ipv6 acl [**ipv6**] *acl-number*	
（可选）开启Telnet客户端匹配ACL deny规则后打印日志信息功能	**telnet server acl-deny-log enable**	缺省情况下，Telnet客户端匹配ACL deny规则后打印日志信息功能处于关闭状态

表6-2 配置对 SSH 用户的控制

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

操作	命令	说明
		“安全命令参考”中的“SSH”
（可选）开启SSH客户端匹配ACL deny规则后打印日志信息功能	**ssh server acl-deny-log enable**	缺省情况下，SSH客户端匹配ACL deny规则后打印日志信息功能处于关闭状态

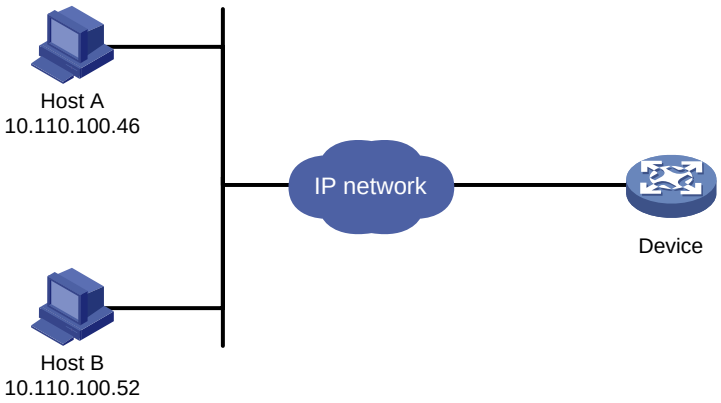
6.1.3 配置举例

1. 组网需求

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

2. 组网图

图6-1 使用 ACL 对 Telnet 用户进行控制



3. 配置步骤

定义 ACL。

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

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

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

6.2 配置对Web用户的控制

通过引用 ACL 可以对访问设备的 Web 用户进行控制。只有 ACL 中 permit 的用户才能使用 Web 访问设备，其它用户不允许访问设备，以免非法用户使用 Web 访问设备。关于 ACL 的定义请参见“ACL 和 QoS 配置指导”中的“ACL”。

6.2.1 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，即配置好 ACL。

6.2.2 通过源IP对Web用户进行控制

在通过源 IP 对 Web 用户进行控制时需要注意，Web 登录时用户输入的用户名和密码属于敏感信息，Web 登录请求是采用 HTTPS 的方式发送到 Web 服务器的。所以，如果 **ip https acl** 命令中的 ACL 规则拒绝客户端通过 HTTPS 服务访问 Web 页面，那么该客户端也无法通过 HTTP 服务访问 Web 页面。

表6-3 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**	-
引用访问控制列表对Web用户进行控制	**ip http acl** [**advanced** | **mac**] { *acl-number* | **name** *acl-name* }	HTTP和HTTPS是两种独立的登录方式，请根据需要二者任选其一
	ip https acl [**advanced** | **mac**] { *acl-number* | **name** *acl-name* }	

6.2.3 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6-4 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* }	该命令在用户视图下执行

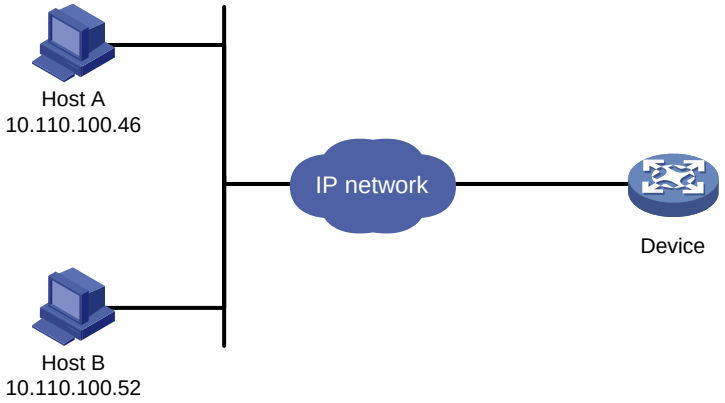
6.2.4 配置举例

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6-2 对 Device 的 HTTP 用户进行 ACL 控制



3. 配置步骤

定义基本访问控制列表。

```
<Sysname> system-view
[Sysname] acl basic 2030 match-order config
[Sysname-acl-ipv4-basic-2030] rule 1 permit source 10.110.100.52 0
```

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

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

6.3 配置对NMS的控制

6.3.1 配置准备

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

6.3.2 配置对NMS的控制

表6-5 SNMPv1/SNMPv2c 版本配置对 NMS 的控制

操作	命令	说明
进入系统视图	**system-view**	-
在配置SNMP团体名的命令中引用ACL	VACM方式： **snmp-agent community** { **read** | **write** } [**simple** | **cipher**] community-name [**mib-view** view-name] [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } | **acl ipv6** { *ipv6-acl-number* | **name** *ipv6-acl-name* }] *	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” 配置SNMP团体名或用户名时二者选其一
	RBAC方式： **snmp-agent community** [**simple** | **cipher**] *community-name* **user-role** *role-name* [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } | **acl ipv6** { *ipv6-acl-number* | **name** *ipv6-acl-name* }] *	
在配置	**snmp-agent group** { **v1** | **v2c** } *group-name* [**read-view**	

操作	命令	说明
SNMPv1/SNMPv2c用户名的命令中引用ACL	*view-name*] [**write-view** *view-name*] [**notify-view** *view-name*] [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } | **acl ipv6** { *ipv6-acl-number* | **name** *ipv6-acl-name* }] *	
	snmp-agent usm-user { **v1** | **v2c** } *user-name group-name* [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } | **acl ipv6** { *ipv6-acl-number* | **name** *ipv6-acl-name* }] *	

表6-6 SNMPv3 版本配置对 NMS 的控制

操作	命令	说明
进入系统视图	**system-view**	-
在配置SNMPv3组名的命令中引用ACL	非FIPS模式下： **snmp-agent group v3** *group-name* [**authentication** | **privacy**] [**read-view** *view-name*] [**write-view** *view-name*] [**notify-view** *view-name*] [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } | **acl ipv6** { *ipv6-acl-number* | **name** *ipv6-acl-name* }] * FIPS模式下： **snmp-agent group v3** *group-name* { **authentication** | **privacy** } [**read-view** *view-name*] [**write-view** *view-name*] [**notify-view** *view-name*] [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } | **acl ipv6** { *ipv6-acl-number* | **name** *ipv6-acl-name* }] *	根据网管用户运行的SNMP版本及配置习惯，可以在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SNMPv3用户名的命令中引用ACL	非FIPS模式下： • VACM 方式： **snmp-agent usm-user v3** *user-name group-name* [**remote** { *ipv4-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*]] [{ **cipher** | **simple** } **authentication-mode** { **md5** | **sha** } *auth-password* [**privacy-mode** { **aes128** | **3des** | **des56** } *priv-password*]] [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } | **acl ipv6** { *ipv6-acl-number* | **name** *ipv6-acl-name* }] * • RBAC 方式： **snmp-agent usm-user v3** *user-name* **user-role** *role-name* [**remote** { *ipv4-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*]] [{ **cipher** | **simple** } **authentication-mode** { **md5** | **sha** } *auth-password* [**privacy-mode** { **aes128** | **3des | des56** } *priv-password*]] [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } | **acl ipv6** { *ipv6-acl-number* | **name** *ipv6-acl-name* }] * FIPS模式下： • VACM 方式： **snmp-agent usm-user v3** *user-name group-name* [**remote** { *ipv4-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*]] { **cipher** | **simple** } **authentication-mode sha** *auth-password* [**privacy-mode aes128** *priv-password*] [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } | **acl ipv6** { *ipv6-acl-number* | **name** *ipv6-acl-name* }] * • RBAC 方式： **snmp-agent usm-user v3** *user-name* **user-role** *role-name* [**remote** { *ipv4-address* | **ipv6** *ipv6-address* } [**vpn-instance**	

操作	命令	说明
	vpn-instance-name]] { **cipher** | **simple** } **authentication-mode sha** *auth-password* [**privacy-mode aes128** *priv-password*] [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } | **acl ipv6** { *ipv6-acl-number* | **name** *ipv6-acl-name* }] *	

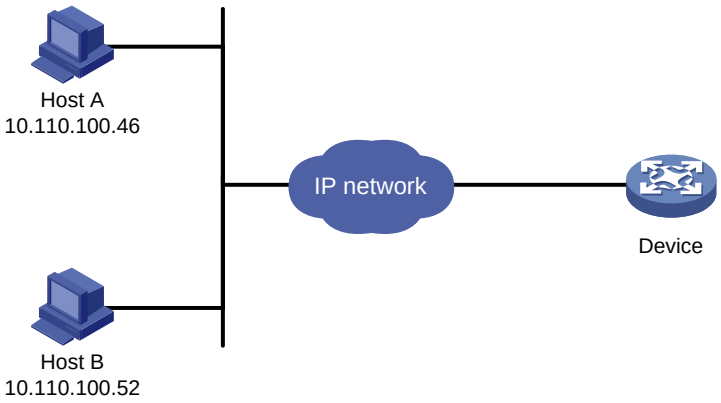
6.3.3 配置举例

1. 组网需求

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

2. 组网图

图6-3 使用 ACL 对 NMS 进行控制



3. 配置步骤

定义基本 ACL。

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

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

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

6.4 配置命令行授权功能

6.4.1 配置步骤

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

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

表6-7 配置命令行授权功能

操作	命令	说明
进入系统视图	**system-view**	-
进入用户线视图	**line** { *first-number1* [*last-number1*] | { **aux** | **console** | **tty** | **vty** } *first-number2* [*last-number2*] }	二者选其一 • 用户线视图下的配置优先于用户线类视图下的配置 • 用户线视图下的配置只对该用户线生效 • 用户线类视图下的配置修改不会立即生效，当用户下次登录后所修改的配置值才会生效 • 用户线视图下的属性配置为缺省值时，将采用用户线类视图下配置的值。如果用户线类视图下的属性配置也为缺省值时，则直接采用该属性的缺省值
进入用户线类视图	**line class** { **aux** | **console** | **tty** | **vty** }	
设置登录用户的认证方式为通过AAA认证	**authentication-mode scheme**	非FIPS模式：缺省情况下，用户通过Console口登录，认证方式为**none**（即不需要进行认证）；用户通过AUX口登录，认证方式为**password**（即需要进行密码认证）；用户通过VTY用户线登录，认证方式为**password** FIPS模式：缺省情况下，用户登录设备的认证方式为**scheme** 用户线视图下，对**authentication-mode**和**protocol inbound**进行关联绑定，当两条命令中的任意一条配置了非缺省值，那么另外一条取缺省值
开启命令行授权功能	**command authorization**	缺省情况下，未开启命令行授权功能，即用户登录后执行命令行不需要授权 如果用户类视图下开启了命令行授权功能，则该类型用户线视图都开启命令行授权功能，并且在该类型用户线视图下将无法关闭命令行授权功能

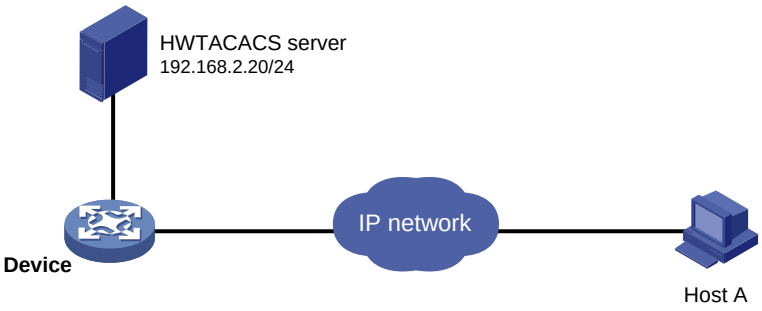
6.4.2 配置举例

1. 组网需求

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

2. 组网图

图6-4 命令行授权配置组网图



3. 配置步骤

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

开启设备的 Telnet 服务器功能，以便用户访问。

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

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

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

开启命令行授权功能，限制用户只能使用授权成功的命令。

```
[Device-line-vty0-63] command authorization
[Device-line-vty0-63] quit
```

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

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

配置缺省域的命令行授权 AAA 方案，使用 HWTACACS 方案。

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

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

```
[Device] local-user monitor
[Device-luser-manage-monitor] password simple 123
[Device-luser-manage-monitor] service-type telnet
```

```
[Device-luser-manage-monitor] authorization-attribute user-role level-1
```

6.5 配置命令行计费功能

6.5.1 配置步骤

当用户线采用 AAA 认证方式并配置命令行计费功能后，系统会将用户执行过的命令记录到 HWTACACS 服务器上，以便集中监视用户对设备的操作。命令行计费功能生效后，如果没有配命令行授权功能，则用户执行的每一条合法命令都会发送到 HWTACACS 服务器上做记录；如果配置了命令行授权功能，则用户执行的并且授权成功的命令都会发送到 HWTACACS 服务器上做记录。

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

表6-8 配置命令行计费功能

操作	命令	说明
进入系统视图	**system-view**	-
进入用户线视图	**line** { *first-number1* [*last-number1*] | { **aux** | **console** | **tty** | **vty** } *first-number2* [*last-number2*] }	二者选其一 • 用户线视图下的配置优先于用户线类视图下的配置 • 用户线视图下的配置只对该用户线生效 • 用户线类视图下的配置修改不会立即生效，当用户下次登录后所修改的配置值才会生效 • 用户线视图下的属性配置为缺省值时，将采用用户线类视图下配置的值。如果用户线类视图下的属性配置也为缺省值时，则直接采用该属性的缺省值
进入用户线类视图	**line class** { **aux** | **console** | **tty** | **vty** }	
设置登录用户的认证方式为通过AAA认证	**authentication-mode scheme**	非FIPS模式：缺省情况下，用户通过Console口登录，认证方式为**none**（即不需要进行认证）；用户通过AUX口登录，认证方式为**password**（即需要进行密码认证）；用户通过VTY用户线登录，认证方式为**password** FIPS模式：缺省情况下，用户登录设备的认证方式为**scheme** 用户线视图下，对**authentication-mode**和**protocol inbound**进行关联绑定，当两条命令中的任意一条配置了非缺省值，那么另外一条取缺省值
开启命令行计费功能	**command accounting**	缺省情况下，未开启命令行计费功能，即计费服务器不会记录用户执行的命令行 如果用户类视图下开启了命令行计费功能，则该类型用户线视图都开启命令行计费功能，并且在该类型用户线视图下将无法关闭命令行计费功能

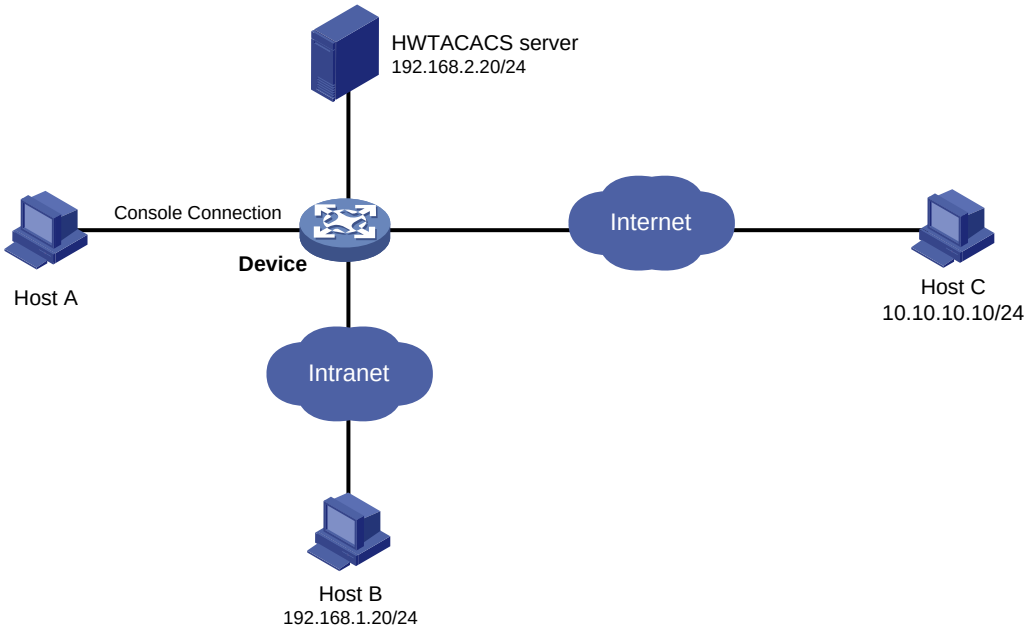
6.5.2 配置举例

1. 组网需求

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

2. 组网图

图6-5 命令行计费配置组网图



3. 配置步骤

开启设备的 Telnet 服务器功能，以便用户访问。

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

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

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

配置缺省域的命令行计费 AAA 方案，使用 HWTACACS 方案。

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

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

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

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

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

目 录

1 FTP

说明

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

设备各款型使用的命令行形式有所不同，详细差异信息如下：

命令行形式	款型
集中式	• MSR810/810-W/810-W-DB/810-LM/810-W-LM/810-10-PoE/810-LM-HK/810-W-LM-HK • MSR810-LMS/810-LUS • MSR2600-6-X1/2600-10-X1/2630 • MSR3600-28/3600-51/3600-28-SI/3600-51-SI • MSR3610-X1/3610-X1-DP/3610-X1-DC/3610-X1-DP-DC • MSR 3610/3620/3620-DP/3640/3660 • MSR810-W-WiNet/810-LM-WiNet/830-4LM-WiNet • MSR830-5BEI-WiNet/830-6EI-WiNet/830-10BEI-WiNet • MSR830-6BHI-WiNet/830-10BHI-WiNet • MSR2600-10-X1-WiNet/2630-WiNet • MSR3600-28-WiNet/3610-X1-WiNet • MSR3610-WiNet/3620-10-WiNet/3620-DP-WiNet/3620-WiNet/3660-WiNet • MSR810-LM-GL/810-W-LM-GL • MSR830-6EI-GL/830-10EI-GL/830-6HI-GL/830-10HI-GL • MSR2600-6-X1-GL/3600-28-SI-GL
分布式	MSR5620/5660/5680

1.1 FTP简介

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

FTP 协议使用 TCP 端口 20 和 21 进行传输。端口 20 用于传输数据，端口 21 用于传输控制消息。FTP 协议基本操作在 RFC959 中进行了描述。

FTP 有两种文件传输模式：

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

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

FTP 有两种工作方式：

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

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

设备可以作为 FTP 服务器，也可以作为 FTP 客户端。

图1-1 FTP 组网应用示意图

提示

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

1.2 配置FTP服务器

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

1.2.1 FTP服务器的基本配置

表1-1 配置 FTP 服务器

操作	命令	说明
进入系统视图	**system-view**	-
启动FTP服务器功能	**ftp server enable**	缺省情况下，FTP服务器功能处于关闭状态
（可选）设置IPv4 FTP客户端对FTP服务器的访问限制	**ftp server acl** { { *advanced-acl-number* | *basic-acl-number* | **mac** *mac-acl-number* } | **ipv6** { *advanced-acl-number* | *basic-acl-number* | **mac** *mac-acl-number* } }	缺省情况下，IPv4 FTP客户端对FTP服务器的访问不受限制
（可选）设置IPv6 FTP客户端对FTP服务器的访问限制	**ftp server acl ipv6** { *advanced-acl-number* | *basic-acl-number* | **mac** *mac-acl-number* }	缺省情况下，IPv6 FTP客户端对FTP服务器的访问不受限制
（可选）开启FTP客户端匹配ACL deny规则后打	**ftp server acl-deny-log enable**	缺省情况下，FTP客户端匹配ACL deny规则后打印日志信息功能处于关闭状态

操作	命令	说明
印日志信息功能		
（可选）配置FTP服务与SSL服务器端策略关联	**ftp server ssl-server-policy** *policy-name*	缺省情况下，未配置SSL服务器端策略与FTP服务关联
（可选）配置FTP服务器的连接空闲时间	**ftp timeout** *minutes*	缺省情况下，连接空闲时间为30分钟 如果在设置的连接空闲时间到期时，FTP服务器和客户端一直没有信息交互，则断开它们之间的连接
（可选）配置FTP服务器发送的FTP报文的DSCP优先级	**ftp server dscp** *dscp-value*	二者选其一 缺省情况下，FTP服务器发送的FTP报文的DSCP优先级为0，FTP服务器发送的IPv6 FTP报文的DSCP优先级为0
（可选）配置FTP服务器发送的IPv6 FTP报文的DSCP优先级	**ftp server ipv6 dscp** *dscp-value*	
（可选）配置使用FTP方式同时登录设备的在线的最大用户连接数	**aaa session-limit ftp** *max-sessions*	缺省情况下，设备支持的最大用户连接数为32 配置本命令后，已经在线的用户连接不会受到影响，只对新的用户连接生效。如果当前在线的用户连接数已经达到最大值，则新的连接请求会被拒绝，登录会失败 关于该命令的详细描述请参见“安全配置指导”中的“AAA”

1.2.2 配置FTP服务器的认证和授权

只有认证通过并授权成功的用户，才能通过 FTP 访问设备上的指定路径。

设备对 FTP 客户端的认证，有以下两种方式：

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

设备对 FTP 客户端的授权，有以下两种方式：

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

关于认证和授权的详细配置请参见“安全配置指导”中的“AAA”。

1.2.3 释放已建立的FTP连接

表1-2 释放已建立的 FTP 连接

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

1.2.4 FTP服务器显示和维护

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

表1-3 FTP 服务器显示和维护

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

1.2.5 FTP服务器典型配置举例（集中式设备-独立运行模式）

1. 组网需求

- Device 作为 FTP 服务器，PC 作为 FTP 客户端。
- 将存储在 PC 上的文件 temp.bin 上传到 FTP 服务器，并使用 FTP 功能备份 Device 的启动配置文件。
- FTP 客户端登录 FTP 服务器的用户名为 abc，密码为 123456。

2. 组网图

图1-2 FTP 服务器典型配置组网图

3. 配置步骤

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

(1) 配置 Device（FTP server）

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

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

启动 Device 的 FTP 服务功能。

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

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

```
<Sysname> dir
```

```
Directory of flash:
     0      drw-           -  Jun 29 2016 18:30:38     logfile
     1      drw-           -  Jun 21 2016 14:51:38     diagfile
     2      drw-           -  Jun 21 2016 14:51:38     seclog
     3      -rw-        2943  Jul 02 2016 08:03:08     startup.cfg
     4      -rw-       63901  Jul 02 2016 08:03:08     startup.mdb
     5      -rw-         716  Jun 21 2016 14:58:02     hostkey
     6      -rw-         572  Jun 21 2016 14:58:02     serverkey
     7      -rw-     6541264  Aug 04 2016 20:40:49     backup.bin

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

(2) 配置 PC（FTP client）

以用户名 abc、密码 123456 登录 FTP 服务器。

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

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

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

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

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

退出 FTP。

```
ftp> bye
```

1.2.6 FTP服务器典型配置举例（分布式设备一独立运行模式）

1. 组网需求

- Device 作为 FTP 服务器，PC 作为 FTP 客户端。
- 将存储在 PC 上的文件 temp.bin 上传到 FTP 服务器，并使用 FTP 功能备份 Device 的启动配置文件。
- FTP 客户端登录 FTP 服务器的用户名为 abc，密码为 123456。

2. 组网图

图1-3 FTP 服务器典型配置组网图

3. 配置步骤

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

(1) 配置 Device（FTP server）

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

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

说明

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

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

启动 Device 的 FTP 服务功能。

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

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

```
<Sysname> dir
Directory of flash:
     0      drw-           -  Jun 29 2016 18:30:38     logfile
     1      drw-           -  Jun 21 2016 14:51:38     diagfile
     2      drw-           -  Jun 21 2016 14:51:38     seclog
     3      -rw-        2943  Jul 02 2016 08:03:08     startup.cfg
     4      -rw-       63901  Jul 02 2016 08:03:08     startup.mdb
     5      -rw-         716  Jun 21 2016 14:58:02     hostkey
     6      -rw-         572  Jun 21 2016 14:58:02     serverkey
     7      -rw-     6541264  Aug 04 2016 20:40:49     backup.bin

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

(2) 配置 PC（FTP client）

以用户名 abc、密码 123456 登录 FTP 服务器。

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

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

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

将传输模式设置为 binary，并上传文件 temp.bin 到主用主控板存储介质的根目录下。

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

退出 FTP。

```
ftp> bye
```

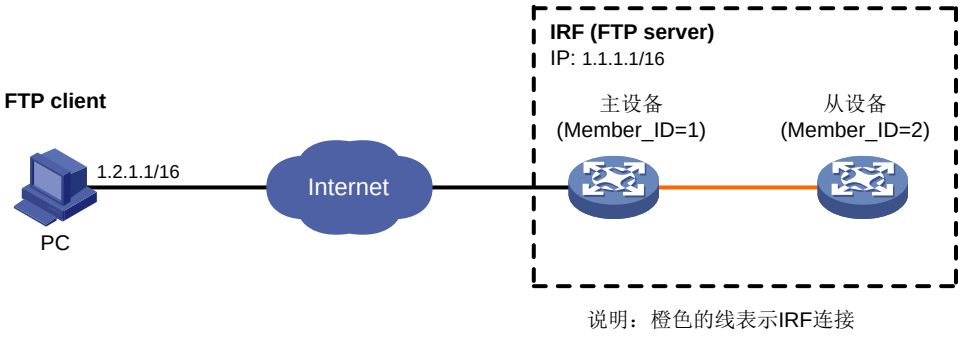
1.2.7 FTP服务器典型配置举例（集中式设备-IRF模式）

1. 组网需求

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

2. 组网图

图1-4 FTP 服务器典型配置组网图



说明：橙色的线表示IRF连接

3. 配置步骤

提示

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

配置前请确保 Device 和 PC 之间路由可达，IP 地址如图 1-4 所示，具体配置步骤略。

(1) IRF（FTP server）上的配置

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

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

说明

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

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

启动 IRF 的 FTP 服务功能。

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

(2) PC（FTP client）的配置

以用户名 abc、密码 123456 登录 FTP 服务器。

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

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

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

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

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

退出 FTP。

```
ftp> bye
```

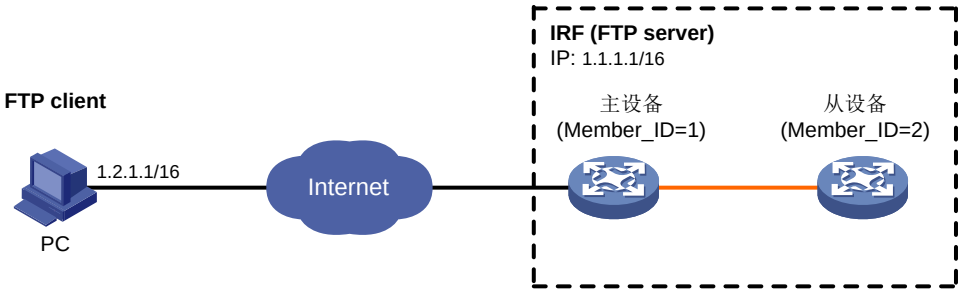
1.2.8 FTP服务器典型配置举例（分布式设备－IRF模式）

1. 组网需求

- 主设备和从设备组成 IRF。主设备的成员编号为 1，主用主控板所在的槽位号为 0，备用主控板所在的槽位号为 1；从设备的成员编号为 2，主用主控板所在的槽位号为 0，备用主控板所在的槽位号为 1。
- IRF 作为 FTP 服务器，PC 作为 FTP 客户端。
- 将存储在 PC 上的文件 temp.bin 上传到 FTP 服务器，并使用 FTP 功能备份 IRF 的配置文件。
- FTP 客户端登录 FTP 服务器的用户名为 abc，密码为 123456。

2. 组网图

图1-5 FTP 服务器典型配置组网图



说明：橙色的线表示IRF连接

3. 配置步骤

提示

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

配置前请确保 IRF 和 PC 之间路由可达，IP 地址如图 1-5 所示，具体配置步骤略。

(1) IRF（FTP server）上的配置

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

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

说明

如果要直接访问全局备用主控板（假设该单板所在设备的成员编号为 2，槽位号为 1）Flash 的根目录，需要将“authorization-attribute work-directory flash:/”配置中的“flash:/”替换成“chassis2#slot1#flash:/”。

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

启动 IRF 的 FTP 服务功能。

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

(2) PC（FTP client）的配置

以用户名 abc、密码 123456 登录 FTP 服务器。

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

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

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

将传输模式设置为 binary，并上传文件 temp.bin 到全局主用主控板存储介质的根目录下。

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

退出 FTP。

```
ftp> bye
```

1.3 配置FTP客户端

1.3.1 建立FTP连接

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

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

表1-4 建立 FTP 连接（IPv4 组网环境）

操作	命令	说明
进入系统视图	**system-view**	-
（可选）在IPv4组网环	**ftp client source** { **interface** *interface-type*	缺省情况下，未配置源地址，使用

操作	命令	说明
境下配置FTP客户端发送的FTP报文的源地址	*interface-number* | **ip** *source-ip-address* }	路由出接口的主IP地址作为设备发送FTP报文的源IP地址
退回用户视图	**quit**	-
在用户视图下直接登录FTP服务器	**ftp** *ftp-server* [*service-port*] [**vpn-instance** *vpn-instance-name*] [**dscp** *dscp-value* | **source** { **interface** { *interface-name* | *interface-type interface-number* } | **ip** *source-ip-address* }] *	二者必选其一 **ftp**命令直接在用户视图下执行；**open**命令在FTP客户端视图下执行
在FTP客户端视图下间接登录FTP服务器	**ftp**	
	open *server-address* [*service-port*]	

说明

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

表1-5 建立 FTP 连接（IPv6 组网环境）

操作	命令	说明
进入系统视图	**system-view**	-
（可选）在IPv6组网环境下配置FTP客户端发送的FTP报文的源地址	**ftp client ipv6 source** { **interface** *interface-type interface-number* | **ipv6** *source-ipv6-address* }	缺省情况下，未配置源地址，设备自动选择IPv6 FTP报文的源IPv6地址，具体选择原则请参见RFC 3484
退回用户视图	**quit**	-
在用户视图下直接登录FTP服务器	**ftp ipv6** *ftp-server* [*service-port*] [**vpn-instance** vpn-instance-name] [**dscp** *dscp-value* | **source** { **interface** *interface-type interface-number* | **ipv6** *source-ipv6-address* }] * [**-i** *interface-type interface-number*]	二者必选其一 **ftp ipv6**命令直接在用户视图下执行；**open**命令在FTP客户端视图下执行
在FTP客户端视图下间接登录FTP服务器	**ftp ipv6**	
	open *server-address* [*service-port*]	

说明

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

1.3.2 操作FTP服务器上的目录

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

表1-6 操作 FTP 服务器上的目录

操作	命令	说明
查看FTP服务器上的目录/文件的详细信息	**dir** [*remotefile* [*localfile*]]	二者选其一
	ls [*remotefile* [*localfile*]]	
切换FTP服务器上的工作路径	**cd** { *directory* | **..** | */* }	-
退出FTP服务器的当前目录，返回FTP服务器的上一级目录	**cdup**	-
显示当前用户正在访问的FTP服务器上的路径	**pwd**	-
在FTP服务器上创建目录	**mkdir** *directory*	-
删除FTP服务器上指定的目录	**rmdir** *directory*	-

1.3.3 操作FTP服务器上的文件

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

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

(2) 删除过时文件，以便有效利用存储空间。

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

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

(5) 进行上传/下载操作。

表1-7 操作 FTP 服务器上的文件

操作	命令	说明
查看FTP服务器上的目录/文件的详细信息	**dir** [*remotefile* [*localfile*]]	二者选其一
	ls [*remotefile* [*localfile*]]	
彻底删除FTP服务器上的指定文件	**delete** *remotefile*	-
设置FTP文件传输的模式为ASCII模式	**ascii**	二者选其一 缺省情况下，文件传输模式为二进制模式
设置FTP文件传输的模式为二进制模式	**binary**	
切换数据的传输方式	**passive**	缺省情况下，数据传输的方式为被动方式
显示或切换FTP客户端本地的工作路径	**lcd** [*directory* | */*]	-
上传本地文件到FTP服务器	**put** *localfile* [*remotefile*]	-
下载FTP服务器上的文件	**get** *remotefile* [*localfile*]	-
在原文件的内容后面添加新文件的内容	**append** *localfile* [*remotefile*]	-

操作	命令	说明
指定重传点	**restart** *marker*	配合**put**、**get**、**append**等命令使用
更新本地文件	**newer** *remotefile*	-
从本地文件的尾部开始获取文件的剩余内容	**reget** *remotefile* [*localfile*]	-
重命名文件	**rename** [*oldfilename* [*newfilename*]]	-

1.3.4 更改登录用户

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

该功能通常用于不同权限用户之间的切换，用户的成功切换不会影响当前的 FTP 连接（即 FTP 控制连接、数据连接以及连接状态都不变）；如果输入的用户名/密码错误，则会断开当前连接，用户必须重新登录才能继续访问 FTP 服务器。

表1-8 更改登录用户

操作	命令	说明
在现有FTP连接上重新发起FTP认证	**user** *username* [*password*]	-

1.3.5 FTP连接的维护与调试

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

表1-9 FTP 连接的维护与调试

操作	命令	说明
显示FTP服务器支持的FTP相关协议命令字	**rhelp**	-
显示FTP服务器支持的FTP相关协议命令字的帮助信息	**rhelp** *protocol-command*	-
显示FTP服务器的状态	**rstatus**	-
显示FTP服务器上指定目录或文件的详细信息	**rstatus** *remotefile*	-
显示当前FTP连接的状态	**status**	-
显示FTP服务器的系统信息	**system**	-
切换FTP功能的协议信息开关	**verbose**	缺省情况下，FTP协议信息开关处于开启状态
打开FTP调试信息开关	**debug**	缺省情况下，FTP客户端调试信息开关处于关闭状态
清除缓存的命令应答	**reset**	-

1.3.6 断开FTP连接

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

表1-10 断开 FTP 连接

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

1.3.7 显示帮助信息

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

表1-11 显示帮助信息

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

1.3.8 FTP客户端显示和维护

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

表1-12 FTP 客户端显示和维护

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

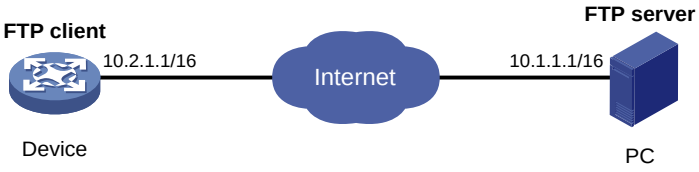
1.3.9 FTP客户端典型配置举例（集中式设备-独立运行模式）

1. 组网需求

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

2. 组网图

图1-6 FTP 客户端典型配置组网图



3. 配置步骤

提示

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

配置前请确保 Device 和 PC 之间路由可达，IP 地址如图 1-6 所示，具体配置步骤略。

以用户名 abc、密码 123456 登录 FTP 服务器。

```
<Sysname> ftp 10.1.1.1
Press CTRL+C to abort.
Connected to 10.1.1.1 (10.1.1.1).
220 WFTPD 2.0 service (by Texas Imperial Software) ready for new user
User (10.1.1.1:(none)): abc
331 Give me your password, please
Password:
230 Logged in successfully
Remote system type is MSDOS.
ftp>
```

将传输模式设置为 binary，以便传输文件。

```
ftp> binary
200 TYPE is now 8-bit binary
```

将文件 temp.bin 从 FTP 服务器下载到 Device。

```
ftp> get temp.bin
local: temp.bin remote: temp.bin
150 Connecting to port 47457
226 File successfully transferred
23951480 bytes received in 95.399 seconds (251.0 kbyte/s)
```

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

```
ftp> ascii
200 TYPE is now ASCII
ftp> put startup.cfg back-startup.cfg
local: startup.cfg remote: back-startup.cfg
150 Connecting to port 47461
226 File successfully transferred
3494 bytes sent in 5.646 seconds (618.00 kbyte/s)
```

```
ftp> bye
221-Goodbye. You uploaded 2 and downloaded 2 kbytes.
221 Logout.
<Sysname>
```

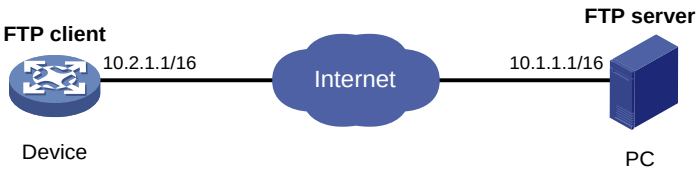
1.3.10 FTP客户端典型配置举例（分布式设备一独立运行模式）

1. 组网需求

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

2. 组网图

图1-7 FTP 客户端典型配置组网图



3. 配置步骤

提示

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

配置前请确保 Device 和 PC 之间路由可达，IP 地址如图 1-7 所示，具体配置步骤略。

以用户名 abc、密码 123456 登录 FTP 服务器。

```
<Sysname> ftp 10.1.1.1
Press CTRL+C to abort.
Connected to 10.1.1.1 (10.1.1.1).
220 WFTPD 2.0 service (by Texas Imperial Software) ready for new user
User (10.1.1.1:(none)): abc
331 Give me your password, please
Password:
230 Logged in successfully
Remote system type is MSDOS.
ftp>
```

将传输模式设置为 binary，以便传输文件。

```
ftp> binary
200 TYPE is now 8-bit binary
```

将文件 temp.bin 从 FTP 服务器下载到 Device。

- 将文件 temp.bin 从 FTP 服务器下载到主用主控板存储介质的根目录下。

```
ftp> get temp.bin
local: temp.bin remote: temp.bin
150 Connecting to port 47457
226 File successfully transferred
23951480 bytes received in 95.399 seconds (251.0 kbyte/s)
```

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

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

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

```
ftp> ascii
200 TYPE is now ASCII
ftp> put startup.cfg back-startup.cfg
local: startup.cfg remote: back-startup.cfg
150 Connecting to port 47461
226 File successfully transferred
3494 bytes sent in 5.646 seconds (618.00 kbyte/s)
ftp> bye
221-Goodbye. You uploaded 2 and downloaded 2 kbytes.
221 Logout.
<Sysname>
```

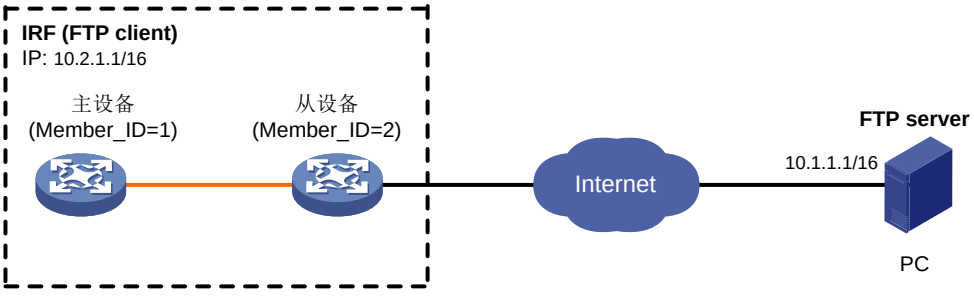
1.3.11 FTP客户端典型配置举例（集中式设备-IRF模式）

1. 组网需求

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

2. 组网图

图1-8 FTP 客户端典型配置组网图



说明：橙色的线表示IRF连接

3. 配置步骤

提示

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

配置前请确保 IRF 和 PC 之间路由可达，IP 地址如图 1-8 所示，具体配置步骤略。

以用户名 abc、密码 123456 登录 FTP 服务器。

```
<Sysname> ftp 10.1.1.1
Press CTRL+C to abort.
Connected to 10.1.1.1 (10.1.1.1).
220 WFTPD 2.0 service (by Texas Imperial Software) ready for new user
User (10.1.1.1:(none)): abc
331 Give me your password, please
Password:
230 Logged in successfully
Remote system type is MSDOS.
ftp>
```

将传输模式设置为 binary，以便传输文件。

```
ftp> binary
200 TYPE is now 8-bit binary
```

将文件 temp.bin 从 FTP 服务器下载到 IRF。

- 将文件 temp.bin 从 FTP 服务器下载到主设备存储介质的根目录下。

```
ftp> get temp.bin
local: temp.bin remote: temp.bin
150 Connecting to port 47457
226 File successfully transferred
23951480 bytes received in 95.399 seconds (251.0 kbyte/s)
```

- 将文件 temp.bin 从 FTP 服务器下载到从设备存储介质的根目录下。

```
ftp> get temp.bin slot2#flash:/temp.bin
```

将 IRF 的配置文件 config.cfg 上传到 FTP 服务器进行备份。

```
ftp> ascii
200 TYPE is now ASCII
ftp> put config.cfg back-config.cfg
local: config.cfg remote: back-config.cfg
150 Connecting to port 47461
226 File successfully transferred
3494 bytes sent in 5.646 seconds (618.00 kbyte/s)
ftp> bye
221-Goodbye. You uploaded 2 and downloaded 2 kbytes.
221 Logout.
<Sysname>
```

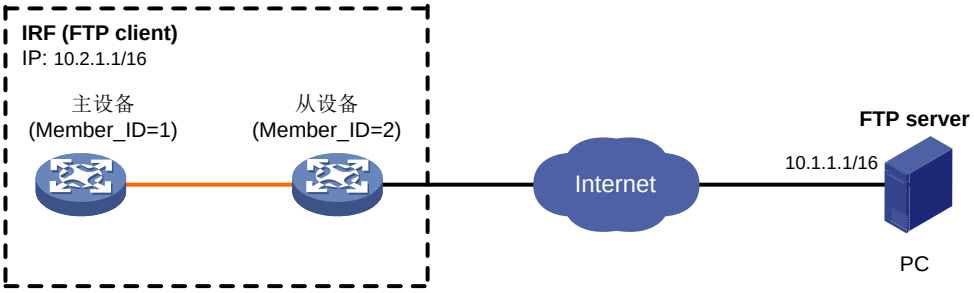
1.3.12 FTP客户端典型配置举例（分布式设备－IRF模式）

1. 组网需求

- 主设备和从设备组成 IRF。主设备的成员编号为 1，主用主控板所在的槽位号为 0，备用主控板所在的槽位号为 1；从设备的成员编号为 2，主用主控板所在的槽位号为 0，备用主控板所在的槽位号为 1。
- IRF 作为 FTP 客户端，PC 作为 FTP 服务器。
- IRF 从 PC 上下载文件 temp.bin，并将配置文件上传到 PC 进行备份。
- PC 上已设置设备登录 FTP 服务器的用户名为 abc，密码为 123456。

2. 组网图

图1-9 FTP 客户端典型配置组网图



说明：橙色的线表示IRF连接

3. 配置步骤

提示

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

配置前请确保 IRF 和 PC 之间路由可达，IP 地址如图 1-9 所示，具体配置步骤略。

以用户名 abc、密码 123456 登录 FTP 服务器。

```
<Sysname> ftp 10.1.1.1
Press CTRL+C to abort.
Connected to 10.1.1.1 (10.1.1.1).
220 WFTPD 2.0 service (by Texas Imperial Software) ready for new user
User (10.1.1.1:(none)): abc
331 Give me your password, please
Password:
230 Logged in successfully
Remote system type is MSDOS.
ftp>
```

将传输模式设置为 binary，以便传输文件。

```
ftp> binary
```

```
200 TYPE is now 8-bit binary
```

将文件 temp.bin 从 FTP 服务器下载到 IRF。

- 将文件 temp.bin 从 FTP 服务器下载到全局主用主控板存储介质的根目录下。

```
ftp> get temp.bin
local: temp.bin remote: temp.bin
150 Connecting to port 47457
226 File successfully transferred
23951480 bytes received in 95.399 seconds (251.0 kbyte/s)
```

- 将文件 temp.bin 从 FTP 服务器下载到全局备用主控板存储介质的根目录下（其中一块全局备用主控板所在设备的成员编号为 1，槽位号为 1；一块全局备用主控板所在设备的成员编号为 2，槽位号为 0；第三块全局备用主控板所在设备的成员编号为 2，槽位号为 1）。

```
ftp> get temp.bin chassis1#slot1#flash:/temp.bin
ftp> get temp.bin chassis2#slot0#flash:/temp.bin
ftp> get temp.bin chassis2#slot1#flash:/temp.bin
```

将 IRF 的配置文件 config.cfg 上传到服务器进行备份。

```
ftp> ascii
200 TYPE is now ASCII
ftp> put config.cfg back-config.cfg
local: config.cfg remote: back-config.cfg
150 Connecting to port 47461
226 File successfully transferred
3494 bytes sent in 5.646 seconds (618.00 kbyte/s)
ftp> bye
221-Goodbye. You uploaded 2 and downloaded 2 kbytes.
221 Logout.
<Sysname>
```

2 TFTP

说明

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

2.1 TFTP简介

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

目前，设备只能作为 TFTP 客户端，不支持作为 TFTP 服务器。

图2-1 TFTP 组网示意图

2.2 配置TFTP客户端

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

表2-1 配置 IPv4 TFTP 客户端

操作	命令	说明
进入系统视图	**system-view**	-
使用ACL限制设备可访问哪些TFTP服务器	**tftp-server acl** *acl-number*	可选 缺省情况下，未使用ACL对设备可访问的TFTP服务器进行限制
配置TFTP客户端的源地址	**tftp client source** { **interface** *interface-type interface-number* | **ip** *source-ip-address* }	缺省情况下，未配置源地址，使用路由出接口的主IP地址作为设备发送TFTP报文的源IP地址
退回用户视图	**quit**	-

操作	命令	说明
在IPv4网络，用TFTP上传/下载文件	**tftp** *tftp-server* { **get** | **put** | **sget** } *source-filename* [*destination-filename*] [**vpn-instance** *vpn-instance-name*] [**dscp** *dscp-value* | **source** { **interface** *interface-type interface-number* | **ip** *source-ip-address* }] *	使用**tftp client source**命令指定了源地址后，又在**tftp**命令中指定了源地址，则采用**tftp**命令中指定的源地址进行通信 该命令在用户视图下执行

表2-2 配置 IPv6 TFTP 客户端

操作	命令	说明
进入系统视图	**system-view**	-
（可选）在IPv6网络，使用ACL限制设备可访问哪些TFTP服务器	**tftp-server ipv6 acl** *ipv6-acl-number*	缺省情况下，未使用ACL对设备可访问的TFTP服务器进行限制
在IPv6网络，配置TFTP客户端的源地址	**tftp client ipv6 source** { **interface** *interface-type interface-number* | **ipv6** *source-ipv6-address* }	缺省情况下，未配置源地址，设备自动选择IPv6 TFTP报文的源IPv6地址，具体选择原则请参见RFC 3484
退回用户视图	**quit**	-
在IPv6网络，用TFTP上传/下载文件	**tftp ipv6** *tftp-server* [**-i** *interface-type interface-number*] { **get** | **put** | **sget** } *source-filename* [*destination-filename*] [**vpn-instance** *vpn-instance-name*] [**dscp** *dscp-value* | **source** { **interface** *interface-type interface-number* | **ipv6** *source-ipv6-address* }] *	使用**tftp client ipv6 source**命令指定了源地址后，又在**tftp ipv6**命令中指定了源地址，则采用**tftp ipv6**命令中指定的源地址进行通信 该命令在用户视图下执行

目 录

1 文件系统管理简介

说明

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

设备各款型使用的命令行形式有所不同，详细差异信息如下：

命令行形式	款型
集中式	• MSR810/810-W/810-W-DB/810-LM/810-W-LM/810-10-PoE/810-LM-HK/810-W-LM-HK • MSR810-LMS/810-LUS • MSR2600-6-X1/2600-10-X1/2630 • MSR3600-28/3600-51/3600-28-SI/3600-51-SI • MSR3610-X1/3610-X1-DP/3610-X1-DC/3610-X1-DP-DC • MSR 3610/3620/3620-DP/3640/3660 • MSR810-W-WiNet/810-LM-WiNet/830-4LM-WiNet • MSR830-5BEI-WiNet/830-6EI-WiNet/830-10BEI-WiNet • MSR830-6BHI-WiNet/830-10BHI-WiNet • MSR2600-10-X1-WiNet/2630-WiNet • MSR3600-28-WiNet/3610-X1-WiNet • MSR3610-WiNet/3620-10-WiNet/3620-DP-WiNet/3620-WiNet/3660-WiNet • MSR810-LM-GL/810-W-LM-GL • MSR830-6EI-GL/830-10EI-GL/830-6HI-GL/830-10HI-GL • MSR2600-6-X1-GL/3600-28-SI-GL
分布式	MSR5620/5660/5680

1.1 文件系统

设备上的一个存储介质即称为一个文件系统。存储介质有多种类型，如 Flash、CF 卡、U 盘和 SD 卡等。

设备各款型对于本节所描述的存储介质的支持情况有所不同，详细差异信息如下：

型号	固定存储介质	可插拔存储介质
MSR810、MSR810-W、MSR810-W-DB、MSR810-LM、MSR810-W-LM、MSR810-10-PoE、MSR810-LM-HK、MSR810-W-LM-HK	Flash	U盘、SD卡
MSR2600-6-X1、MSR2600-10-X1	Flash	U盘

型号	固定存储介质	可插拔存储介质
MSR 2630	Flash	U盘
MSR3600-28、MSR3600-51	CF卡	U盘
MSR3600-28-SI、MSR3600-51-SI	Flash	U盘
MSR3610-X1、MSR3610-X1-DP、MSR3610-X1-DC、MSR3610-X1-DP-DC	Flash	• MSR3610-X1、MSR3610-X1-DP：U 盘、HD 卡、SD 卡 • MSR3610-X1-DC、MSR3610-X1-DP-DC：U 盘、SD 卡
MSR 3610、MSR 3620、MSR 3620-DP、MSR 3640、MSR 3660	• MSR 3610、MSR 3620、MSR 3640、MSR 3660：CF 卡 • MSR 3620-DP：Flash	• MSR 3610、MSR 3620、MSR 3640、MSR 3660：U 盘 • MSR 3620-DP：SD 卡、U 盘
MSR5620/5660/5680	Flash	U盘、CF卡

型号	固定存储介质	可插拔存储介质
MSR810-W-WiNet/810-LM-WiNet	Flash	U盘、SD卡
MSR830-4LM-WiNet	Flash	U盘、SD卡
MSR830-5BEI-WiNet/830-6EI-WiNet/830-10BEI-WiNet	Flash	U盘（仅MSR830-10BEI-WiNet支持）
MSR830-6BHI-WiNet/830-10BHI-WiNet	Flash	U盘、SD卡
MSR2600-10-X1-WiNet	Flash	U盘
MSR2630-WiNet	Flash	U盘
MSR3600-28-WiNet	CF卡	U盘
MSR3610-X1-WiNet	Flash	U盘、HD卡、SD卡
MSR3610-WiNet/3620-10-WiNet/3620-DP-WiNet/3620-WiNet/3660-WiNet	Flash	• MSR3610-WiNet/3620-10-WiNet/3620-DP-WiNet/3620-WiNet：U 盘 • MSR3660-WiNe：SD 卡、U 盘

型号	固定存储介质	可插拔存储介质
MSR810-LM-GL	Flash	U盘、SD卡
MSR810-W-LM-GL	Flash	U盘、SD卡
MSR830-6EI-GL	Flash	-
MSR830-10EI-GL	Flash	U盘
MSR830-6HI-GL	Flash	U盘、SD卡

型号	固定存储介质	可插拔存储介质
MSR830-10HI-GL	Flash	U盘、SD卡
MSR2600-6-X1-GL	Flash	U盘
MSR3600-28-SI-GL	Flash	U盘

1.1.1 文件系统的命名

设备支持的存储介质包括固定存储介质和可插拔存储介质。

1. 存储介质位置

分布式设备 IRF 模式下，存储介质位置的表示方式为：chassis*m*#slot*n*#。其中 *m* 为设备的成员编号，*n* 为成员设备上拥有存储介质的板卡所在槽位号。例如：chassis2#slot1#表示成员设备 2 的 1 号槽位的主控板上的存储介质。不指定 chassis 和 slot 参数时，表示 IRF 中全局主用主控板的存储介质。（适用于分布式设备）

分布式设备独立运行模式下，存储介质位置的表示方式为：slot*n*#。其中 *n* 为设备上拥有存储介质的板卡所在槽位号。例如： slot1#代表 1 号槽位的主控板上的存储介质。不指定 slot 参数时，表示设备主用主控板的存储介质。（适用于分布式设备）

存储介质位置的表示方式为：slot*n*#。其中 *n* 为 IRF 中成员设备的编号。例如：slot2#代表成员设备 2 上的存储介质。不指定 slot 参数时，表示 IRF 中主设备的存储介质。（适用于集中式设备-IRF 模式）

2. 文件系统的名称

设备支持的存储介质包括固定存储介质和可插拔存储介质：

- 固定存储介质指 Flash，其文件系统的名称为“flash:”。
- 可插拔存储介质指 U 盘、CF 卡和 SD 卡，其文件系统的名称由存储介质的位置、存储介质类型、存储介质编号和冒号组成：
  - 存储介质的位置：请参见本文档的“存储介质位置”。
  - 存储介质类型：U 盘的类型名称为“usb”。
  - 存储介质编号：同类型的存储介质以英文小写字母 a 开始进行排序，例如“usba”表示第一个 U 盘。
  - 分区编号：存储介质上的分区以数字 0 开始进行排序（存储介质名称不包括分区编号）。
  - 冒号：作为存储介质名称的结束符，例如第一个 U 盘，其完整名称为“usba0:”。

说明

文件系统名称中的英文字符输入时区分大小写，必须为小写字符。

1.1.2 缺省文件系统

缺省文件系统是指用户登录设备后默认工作在的文件系统。用户在对文件或者文件夹进行操作时，如果不指定文件系统，则表示对设备的缺省文件系统进行操作。例如，在保存当前配置时，如果不输入任何保存位置信息，则下次启动配置文件将保存在缺省文件系统的根目录下。

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

1.1.3 目录

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

1. 根目录

根目录用“/”来表示。在 IRF 中，输入 **cd** *slotn#medium*:/或者 **cd** *chassism#slotn#medium*:/可以进入成员设备的相应文件系统的根目录。

2. 工作目录

工作目录也被称为当前工作目录。

用户登录设备后，缺省的工作目录为设备 Flash 或 CF 卡的根目录。（集中式设备-独立运行模式）

用户登录设备后，缺省的工作目录为主设备 Flash 或 CF 卡的根目录。（集中式设备-IRF 模式）

用户登录设备后，缺省的工作目录为设备主用主控板 CF 卡的根目录。（分布式设备－独立运行模式）

用户登录设备后，缺省的工作目录为设备全局主用主控板 CF 卡的根目录。（分布式设备－IRF 模式）

3. 文件夹的命名

文件夹名称中可以包含数字、字母或特殊字符（除了*|\/?<>":）。给文件夹命名时，首字母请不要使用“.”。因为系统会把名称首字母为“.”的文件夹当成隐藏文件夹。

4. 常用文件夹

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

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

1.1.4 文件

1. 文件的命名

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

2. 常见文件类型

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

- xx.ipe（复合软件包套件，是启动软件包的集合）
- xx.bin（启动软件包）

- xx.cfg（配置文件）
- xx.mdb（二进制格式的配置文件）
- xx.log（用于存放日志的文件）
- 其它后缀的文件

3. 隐藏文件和文件夹

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

1.1.5 指定文件夹和文件

路径是指文件或文件夹所在的位置，包括绝对路径和相对路径。

1. 指定文件夹

我们可以使用相对路径和绝对路径来指定文件夹。例如，当前工作目录为 flash:/，可以通过绝对路径 flash:/test/test1/test2/（末尾的“/”为可选）或相对路径 test/test1/test2/（末尾的“/”为可选）进入 test2 文件夹下。

2. 指定文件

我们可以使用相对路径方式和绝对路径方式来指定文件。例如，当前工作目录为 flash:/test/，可以通过绝对路径方式 flash:/test/test1/test2/samplefile.cfg 或相对路径方式 test1/test2/samplefile.cfg 指定 test2 文件夹下的 samplefile.cfg 文件。

1.2 使用限制和注意事项

- 在执行文件系统操作过程中，禁止对存储介质进行插拔操作。否则，可能会引起文件系统的损坏。（集中式设备-独立运行模式）
- 在执行文件系统操作过程中，禁止对单板或存储介质进行插拔或主备倒换操作。否则，可能会引起文件系统的损坏。（分布式设备－独立运行模式）
- 在执行文件系统操作过程中，禁止对存储介质进行插拔或主设备和从设备的倒换操作。否则，可能会引起文件系统的损坏。（集中式设备-IRF 模式）
- 在执行文件系统操作过程中，禁止对单板或存储介质进行插拔或全局主用主控板和全局备用主控板的主备倒换操作。否则，可能会引起文件系统的损坏。（分布式设备－IRF 模式）
- 当用户占用可插拔存储介质的资源（如用户正在访问某个目录或正在打开文件等）时，存储介质被强制拔出。此时，请先释放占用的存储介质的资源（如切换目录、关闭打开的文件或 **umount** 相应的文件系统等），再插入存储介质。否则，存储介质被插入后可能不能被识别。
- 当需要对 U 盘进行写文件系统操作，请确保没有将 U 盘写保护。如果 U 盘写保护了，这些操作将执行失败。其它文件系统操作不受写保护开关影响。
- 当一个用户对存储介质或文件系统执行 **fixdisk** 或 **format** 操作时，其他用户不能访问该存储介质或文件系统。需要等待这些操作结束后，通过以下方式来访问此存储介质或文件系统：
  a. 通过命令行参数直接指定绝对路径。例如，使用 **dir** flash:/命令来显示 flash:中的文件。
  b. 通过 **cd** 命令切换到该存储介质或文件系统目录下后，再使用相对路径访问。例如，使用 **cd** flash:/进入 flash:，再使用 **dir** 命令显示 flash:中的文件。

1.3 存储介质和文件系统操作

1.3.1 存储介质分区

注意

- 分区操作会清除存储介质中的数据，操作前请务必做好文件备份。
- Flash 不支持分区操作。

存储介质分区是将存储介质分成多个不同的逻辑设备，每个逻辑设备可以单独进行文件操作。

对存储介质分区操作时，如果同时还有其他用户在访问该存储介质，系统会提示分区失败。

对存储介质进行交互式分区时，需保证每个分区至少为 32MB。

对 U 盘进行分区时，请确保没有对 U 盘设置写保护。否则分区失败，需要重新挂载或者插拔 U 盘后，才能正常访问 U 盘。

分区完成后各分区的大小可能与用户指定的大小不一致，但误差小于存储介质总容量的 5%。

表1-1 存储介质分区

操作	命令	说明
对存储介质进行分区 （本命令仅缺省MDC支持）	**fdisk** *medium* [*partition-number*]	可通过配置*partition-number*参数，指定分区数量，此时会将存储介质分成多个大小相等的分区。如果不指定*partition-number*参数，则会进行交互式分区。可根据提示指定分区的数量及每个分区的大小

1.3.2 文件系统的挂载/卸载

注意

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

设备各款型对于本节所描述的特性支持情况有所不同，详细差异信息如下：

型号	特性	描述
MSR810/810-W/810-W-DB/810-LM/810-W-LM/810-10-PoE/810-LM-HK/810-W-LM-HK/810-LMS/810-LUS	文件系统的挂载/卸载	支持
MSR2600-6-X1/2600-10-X1		支持
MSR 2630		支持

型号	特性	描述
MSR3600-28/3600-51		支持
MSR3600-28-SI/3600-51-SI		支持
MSR3610-X1/3610-X1-DP/3610-X1-DC/3610-X1-DP-DC		支持
MSR 3610/3620/3620-DP/3640/3660		支持
MSR5620/5660/5680		支持

型号	特性	描述
MSR810-W-WiNet/810-LM-WiNet	文件系统的挂载/卸载	支持
MSR830-4LM-WiNet		支持
MSR830-5BEI-WiNet/830-6EI-WiNet/830-10BEI-WiNet		支持
MSR830-6BHI-WiNet/830-10BHI-WiNet		支持
MSR2600-10-X1-WiNet		支持
MSR2630-WiNet		支持
MSR3600-28-WiNet		支持
MSR3610-X1-WiNet		支持
MSR3610-WiNet/3620-10-WiNet/3620-DP-WiNet/3620-WiNet/3660-WiNet		支持

型号	特性	描述
MSR810-LM-GL	文件系统的挂载/卸载	支持
MSR810-W-LM-GL		支持
MSR830-6EI-GL		不支持
MSR830-10EI-GL		支持
MSR830-6HI-GL		支持
MSR830-10HI-GL		支持
MSR2600-6-X1-GL		支持
MSR3600-28-SI-GL		支持

支持热插拔的存储介质（如 CF 卡等），可以在用户视图下，使用 **mount** 和 **umount** 命令挂载和卸载其对应的文件系统。

- 缺省情况下，存储介质连接到设备后，其文件系统自动被挂载，可以直接使用。如果系统未能自动识别插入的存储设备，则必须手动进行挂载操作后，才能对该文件系统执行读写操作。

- 卸载存储介质中所有的文件系统后用户才可以安全的拔出存储介质，否则可能引起文件损坏甚至存储介质损坏、不可用。
- 被卸载的文件系统需重新挂载方可使用。

表1-2 文件系统的挂载/卸载

操作	命令	说明
挂载文件系统	**mount** *filesystem*	缺省情况下，存储介质连接到设备后，其文件系统自动被挂载，处于挂载状态，可以直接使用 该命令在用户视图下执行
卸载文件系统	**umount** *filesystem*	缺省情况下，存储介质连接到设备后，其文件系统自动被挂载，处于挂载状态，可以直接使用 该命令在用户视图下执行

1.3.3 格式化文件系统

注意

格式化操作将导致文件系统中的所有文件丢失，并且不可恢复，请谨慎使用。

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

表1-3 格式化文件系统

操作	命令	说明
格式化文件系统	**format** *filesystem*	该命令在用户视图下执行

1.3.4 恢复文件系统的空间

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

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

表1-4 恢复文件系统的空间

操作	命令	说明
恢复文件系统的空间	**fixdisk** *filesystem*	该命令在用户视图下执行

1.4 文件夹操作

1.4.1 显示文件夹信息

表1-5 显示文件夹信息

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

1.4.2 显示当前的工作路径

表1-6 显示当前的工作路径

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

1.4.3 修改当前的工作路径

表1-7 修改当前的工作路径

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

1.4.4 创建文件夹

表1-8 创建文件夹

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

1.4.5 重命名文件夹

表1-9 重命名文件夹

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

1.4.6 打包文件夹和解包

打包是将用户指定的原文件夹拷贝，打包保存成一个新文件（原文件夹仍然存在）。该功能可用于文件夹的备份，也可用于文件夹的整理，使文件夹变得简洁。用户可选择直接打包保存或者打包后压缩保存，如果选择打包后压缩保存，还可节省存储空间。

解包是打包的逆向操作，是将打包文件还原成原文件夹。需要注意的是，当指定参数 **screen** 时，请选择较小的文件/文件夹。否则会出现登录终端长时间显示且无法中断，最终登录终端崩溃的现象。

表1-10 打包文件夹和解包

操作	命令	说明
将多个文件夹打包成一个新文件	**tar create** [**gz**] **archive-file** *dest-file* [**verbose**] **source** *source-directory*&<1-5>	该命令在用户视图下执行
显示指定打包文件夹中包含的文件和文件夹的名称	**tar list archive-file** *file*	该命令在用户视图下执行
解包指定文件	**tar extract archive-file** *file* [**verbose**] [**screen** | **to** *directory*]	该命令在用户视图下执行

1.4.7 删除文件夹

在删除文件夹前，必须先永久删除或者暂时删除文件夹中的所有文件和子文件夹。如果文件只是暂时删除，那么执行 **rmdir** 会将这些文件从回收站中彻底删除。

表1-11 删除文件夹

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

1.4.8 设置操作文件夹时是否提示

用户可以通过命令行来设置执行文件夹操作时是否提示：

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

表1-12 设置操作文件夹时是否提示

操作	命令	说明
进入系统视图	**system-view**	-
设置操作文件夹时是否提示	**file prompt** { **alert** | **quiet** }	缺省情况下，用户对文件夹进行有危险性的操作时，系统会要求用户进行交互确认 此命令同样也适用于设置操作文件是否提示

1.5 文件操作

1.5.1 文件的操作

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

1.5.2 显示文件信息

表1-13 显示文件信息

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

1.5.3 显示文件内容

表1-14 显示文件内容

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

1.5.4 重命名文件

表1-15 重命名文件

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

1.5.5 拷贝文件

表1-16 拷贝文件

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

1.5.6 移动文件

表1-17 移动文件

操作	命令	说明
移动文件	**move** *source-file* { *dest-file* | *dest-directory* }	该命令在用户视图下执行

1.5.7 压缩/解压缩文件

表1-18 压缩/解压缩文件

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

1.5.8 打包/解包文件

打包是将用户指定的原文件拷贝，打包保存成一个新文件（原文件仍然存在）。该功能可用于文件的备份，也可用于文件夹的整理，使文件夹变得简洁。用户可选择直接打包保存或者打包后压缩保存，如果选择打包后压缩保存，还可节省存储空间。

解包是打包的逆向操作，是将打包文件还原成原文件。

表1-19 打包/解包文件

操作	命令	说明
将多个文件打包成一个新文件	**tar create** [**gz**] **archive-file** *dest-file* [**verbose**] **source** *source-file*&<1-5>	该命令在用户视图下执行
显示指定打包文件中包含的文件的名称	**tar list archive-file** *file*	该命令在用户视图下执行
解包指定文件	**tar extract archive-file** *file* [**verbose**] [**screen** | **to** *directory*]	该命令在用户视图下执行

1.5.9 删除/恢复文件

注意

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

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

表1-20 删除/恢复文件

操作	命令	说明
删除文件并将文件放入回收站	**delete** *file*	该命令在用户视图下执行
恢复回收站中的文件	**undelete** *file*	该命令在用户视图下执行
永久删除文件	**delete /unreserved** *file*	该命令在用户视图下执行

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

1.5.10 彻底删除回收站中的文件

对于支持多个存储介质的设备，每个存储介质下都有一个回收站。回收站文件夹名均为“.trash”，要查看回收站下有哪些文件，请进入相应的存储介质，用 **dir /all** .trash，或者 **cd** .trash 进入回收站文件夹后，再用 **dir** 命令查看。如果确定不再需要某个（些）文件，可使用以下步骤将文件从回收站中彻底删除。

表1-21 彻底删除回收站中的文件

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

1.5.11 计算文件摘要

使用摘要算法计算文件的摘要值，通常用于验证文件的正确性和完整性，防止文件内容被篡改。

表1-22 计算文件摘要

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

1.5.12 设置操作文件时是否提示

用户可以通过命令行来设置执行文件操作时是否提示：

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

表1-23 设置操作文件时是否提示

操作	命令	说明
进入系统视图	**system-view**	-
设置操作文件时是否提示	**file prompt** { **alert** | **quiet** }	缺省情况下，用户对文件进行有危险性的操作时，系统会要求用户进行交互确认 此命令同样也适用于设置操作文件夹是否提示

1.6 自动拷贝操作

设备各款型对于本节所描述的特性支持情况有所不同，详细差异信息如下：

型号	特性	描述
MSR810/810-W/810-W-DB/810-LM/810-W-LM/810-10-PoE/810-LM-HK/810-W-LM-HK/810-LMS/810-LUS	自动拷贝操作	MSR810/810-W/810-W-DB/810-LM/810-W-LM/810-10-PoE/810-LM-HK/810-W-LM-HK：支持 MSR810-LMS/810-LUS：不支持
MSR2600-6-X1/2600-10-X1		不支持
MSR 2630		不支持
MSR3600-28/3600-51		不支持
MSR3600-28-SI/3600-51-SI		不支持
MSR3610-X1/3610-X1-DP/3610-X1-DC/3610-X1-DP-DC		不支持
MSR 3610/3620/3620-DP/3640/3660		不支持
MSR5620/5660/5680		不支持

型号	特性	描述
MSR810-W-WiNet/810-LM-WiNet	自动拷贝操作	支持
MSR830-4LM-WiNet		支持
MSR830-5BEI-WiNet/830-6EI-WiNet/830-10BEI-WiNet		支持
MSR830-6BHI-WiNet/830-10BHI-WiNet		支持
MSR2600-10-X1-WiNet		不支持
MSR2630-WiNet		不支持
MSR3600-28-WiNet		不支持
MSR3610-X1-WiNet		不支持
MSR3610-WiNet/3620-10-WiNet/3620-DP-WiNet/3620-WiNet/3660-WiNet		不支持

型号	特性	描述
MSR810-LM-GL	自动拷贝操作	支持
MSR810-W-LM-GL		支持
MSR830-6EI-GL		支持
MSR830-10EI-GL		支持
MSR830-6HI-GL		支持
MSR830-10HI-GL		支持
MSR2600-6-X1-GL		不支持
MSR3600-28-SI-GL		不支持

自动拷贝功能可以将可插拔存储介质中的文件自动拷贝到目的路径。通过该功能可以在无需登录设备的情况下，自动更新设备中的文件，例如更新车载 AP 中的网页、视频等本地资源。

在进行自动拷贝操作前，用户需要通过命令行将自动拷贝的源路径设置为可插拔存储介质中的路径，目的路径设置为设备本地路径。配置完成后，当可插拔存储介质插入设备时，设备会根据用户配置的路径将源路径下所有文件拷贝至目的路径。

在自动拷贝过程中，通过设备的 SYS/ALARM 指示灯判断拷贝进度：

- SYS 灯快速闪烁，表示正在进行自动拷贝
- SYS 灯正常闪烁，表示自动拷贝完成
- ALARM 灯闪烁 10 秒，表示自动拷贝失败。

导致自动拷贝失败的原因如下：

- 目的路径没有设置写权限
- 目的路径的可用空间不足，自动拷贝未能完成
- 可插拔存储介质在自动拷贝过程中被拔出
- 可插拔存储介质中不存在配置的源目录

表1-24 配置自动拷贝功能的源路径和目的路径

操作	命令	说明
进入系统视图	**system-view**	-
配置源路径	**auto-copy source-directory** *source-directory*	缺省情况下，没有指定自动拷贝功能的源路径
配置目的路径	**auto-copy destination-directory** *destination-directory*	缺省情况下，没有指定自动拷贝功能的目的路径

1.7 同步文件/文件夹

设备各款型对于本节所描述的特性支持情况有所不同，详细差异信息如下：

型号	特性	描述
MSR810/810-W/810-W-DB/810-LM/810-W-LM/810-10-PoE/810-LM-HK/810-W-LM-HK/810-LMS/810-LUS	同步文件/文件夹	MSR810/810-W/810-W-DB/810-LM/810-W-LM/810-10-PoE/810-LM-HK/810-W-LM-HK：支持 MSR810-LMS/810-LUS：不支持
MSR2600-6-X1/2600-10-X1		不支持
MSR 2630		不支持
MSR3600-28/3600-51		不支持
MSR3600-28-SI/3600-51-SI		不支持
MSR3610-X1/3610-X1-DP/3610-X1-DC/3610-X1-DP-DC		不支持
MSR 3610/3620/3620-DP/3640/3660		不支持
MSR5620/5660/5680		不支持

型号	特性	描述
MSR810-W-WiNet/810-LM-WiNet	同步文件/文件夹	支持
MSR830-4LM-WiNet		支持
MSR830-5BEI-WiNet/830-6EI-WiNet/830-10BEI-WiNet		支持
MSR830-6BHI-WiNet/830-10BHI-WiNet		支持
MSR2600-10-X1-WiNet		不支持
MSR2630-WiNet		不支持
MSR3600-28-WiNet		不支持
MSR3610-X1-WiNet		不支持
MSR3610-WiNet/3620-10-WiNet/3620-DP-WiNet/3620-WiNet/3660-WiNet		不支持

型号	特性	描述
MSR810-LM-GL	同步文件/文件夹	支持
MSR810-W-LM-GL		支持
MSR830-6EI-GL		支持
MSR830-10EI-GL		支持
MSR830-6HI-GL		支持
MSR830-10HI-GL		支持
MSR2600-6-X1-GL		不支持
MSR3600-28-SI-GL		不支持

使用该功能可以把 IPv4 远程服务器上的文件/文件夹同步到设备上的指定路径，并让这两个路径下的内容保持一致。

表1-25 同步文件/文件夹

操作	命令	说明
进入系统视图	**system-view**	-
（可选）配置同步文件/文件夹过程中使用的源IP地址	**rsync client source** { **interface** *interface-type interface-number* | **ip** *source-ip* }	缺省情况下，未配置出接口和源地址，设备使用出接口的主IPv4地址作为同步文件/文件夹过程中设备发送的报文的源IP地址
同步远程服务器上的文件/文件夹	**rsync** [**-s** *source-ip*] *rsync-server source-path destination-path* [*user-name password*]	-

目 录

1 配置文件管理

说明

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

设备各款型使用的命令行形式有所不同，详细差异信息如下：

命令行形式	款型
集中式	• MSR810/810-W/810-W-DB/810-LM/810-W-LM/810-10-PoE/810-LM-HK/810-W-LM-HK • MSR810-LMS/810-LUS • MSR2600-6-X1/2600-10-X1/2630 • MSR3600-28/3600-51/3600-28-SI/3600-51-SI • MSR3610-X1/3610-X1-DP/3610-X1-DC/3610-X1-DP-DC • MSR 3610/3620/3620-DP/3640/3660 • MSR810-W-WiNet/810-LM-WiNet/830-4LM-WiNet • MSR830-5BEI-WiNet/830-6EI-WiNet/830-10BEI-WiNet • MSR830-6BHI-WiNet/830-10BHI-WiNet • MSR2600-10-X1-WiNet/2630-WiNet • MSR3600-28-WiNet/3610-X1-WiNet • MSR3610-WiNet/3620-10-WiNet/3620-DP-WiNet/3620-WiNet/3660-WiNet • MSR810-LM-GL/810-W-LM-GL • MSR830-6EI-GL/830-10EI-GL/830-6HI-GL/830-10HI-GL • MSR2600-6-X1-GL/3600-28-SI-GL
分布式	MSR5620/5660/5680

1.1 配置文件简介

配置文件是用来保存配置的文件。配置文件主要用于：

- 将当前配置保存到配置文件，以便设备重启后，这些配置能够继续生效。
- 使用配置文件，用户可以非常方便地查阅配置信息。
- 当网络中多台设备需要批量配置时，可以将相同的配置保存到配置文件，再上传/下载到所有设备，在所有设备上执行该配置文件来实现设备的批量配置。

1.1.1 配置的类型

1. 出厂配置

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

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

2. 启动配置

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

可以通过以下方式查看启动配置：

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

3. 当前配置

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

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

1.1.2 配置文件的类型

配置文件是用来保存配置的文件，设备上可以同时存在多个配置文件。设备本次启动使用的配置文件称为启动配置文件；设备下次启动使用的配置文件称为下次启动配置文件。为了安全起见，用户可以配置两个下次启动配置文件，一个为主用，一个为备用。

系统启动时，配置文件的选择遵循以下规则：

(1) 优先使用主用下次启动配置文件。

(2) 如果主用下次启动配置文件不存在或损坏，再使用备用下次启动配置文件。

(3) 如果主用和备用下次启动配置文件都不存在或损坏，则使用出厂配置启动。

1.1.3 配置文件的保存格式

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

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

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

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

如无特殊说明，下文描述的配置文件均指字符串类型的配置文件。

1.1.4 配置文件的内容与格式

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

配置文件的内容与格式规则如下：

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

下面摘录了配置文件的部分内容。

```
#
local-user root class manage
 password hash
$h$6$Twd73mLrN8O2vvD5$Cz1vgdpR4KoTiRQNE9pg33gU14Br2p1VguczLSVyJLO2huV5Syx/LfDIf8ROLtVErJ
/C31oq2rFtmNuyZf4STw==
 service-type ssh telnet terminal
 authorization-attribute user-role network-admin
 authorization-attribute user-role network-operator
#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 1.1.1.1 255.255.255.0
#
```

1.2 显示配置差异

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

表1-1 显示两份配置之间的差异

操作	命令	说明
显示指定配置文件和指定配置文件、当前运行配置、下次启动配置文件之间的	**display diff configfile** *file-name-s* { **configfile** *file-name-d* | **current-configuration** | **startup-configuration** }	这些命令在任意视图下均可执行

操作	命令	说明
差异		**display diff startup-configuration current-configuration**和**display current-configuration diff**命令的功能相同，二者选其一即可 只有文本类型的配置文件，才支持查看差异
显示当前运行配置和指定配置文件、下次启动配置文件之间的差异	**display diff current-configuration** { **configfile** *file-name-d* | **startup-configuration** }	
显示下次启动配置文件和指定配置文件之间的差异	**display diff startup-configuration configfile** *file-name-d*	
显示下次启动配置文件与当前运行配置之间的差异	**display diff startup-configuration current-configuration**	
	display current-configuration diff	

1.3 保存当前配置

1.3.1 开启配置文件加密功能

配置文件加密功能就是设备在执行 **save** 命令将当前配置保存到配置文件的同时，将配置文件加密。加密后的文件能被所有运行 Comware V7 平台软件的设备识别和解析。因此，为了防止非法用户对加密后配置文件的解析，需确保只有合法用户才能获取加密后的配置文件。运行其它平台软件的设备不能识别和解析。

开启配置文件加密功能后，将不能使用 **more** 命令查看配置文件（后缀名为“.cfg”的配置文件）的内容。

表1-2 开启配置文件加密功能

操作	命令	说明
进入系统视图	**system-view**	-
开启配置文件加密功能	**configuration encrypt** { **private-key** | **public-key** }	缺省情况下，配置文件加密功能处于关闭状态

1.3.2 保存当前配置

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

提示

执行 **save** [**backup** | **main**] [**force**]命令时，请不要重启设备或者给设备断电，以免造成下次启动配置文件丢失。

表1-3 保存当前配置（集中式设备-独立运行模式）

操作	命令	说明
将当前配置保存到指定文件，但不会将该文件设置为下次启动配置文件	**save** *file-url*	二者选其一 为了安全起见，在需要将当前配置保存到下次启动配置文件的时候，建议选用**safely**参数 两命令均可在任意视图下执行
将当前配置保存到存储介质的根目录下，并将该文件设置为下次启动配置文件	**save** [**safely**] [**backup** | **main**] [**force**] [**changed**]	

表1-4 保存当前配置（分布式设备－独立运行模式）

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

表1-5 保存当前配置（集中式设备-IRF 模式）

操作	命令	说明
将当前配置保存到指定文件，但不会将该文件设置为下次启动配置文件	**save** *file-url* [**all** | **slot** *slot-number*]	二者选其一 为了安全起见，在需要将当前配置保存到下次启动配置文件的时候，建议选用**safely**参数 两命令均可在任意视图下执行
将当前配置保存到所有成员设备存储介质的根目录下，并将该文件设置为下次启动配置文件	**save** [**safely**] [**backup** | **main**] [**force**] [**changed**]	

表1-6 保存当前配置（分布式设备－IRF 模式）

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


说明

如果设备在本次运行过程中发生成员设备离开 IRF 的情况，在不执行 **save** 的前提下此成员设备重新加入 IRF 后设备的配置不会丢失。若执行 **save** 命令，将导致该成员设备的配置丢失。如需恢复

该成员设备的配置，请在该设备重新加入 **IRF** 并重启设备后，执行 **display current-configuration** 查看原来的当前配置是否恢复，在确保恢复的前提下执行 **save** 命令，该成员设备的配置即可自行恢复。（适用于集中式设备-IRF 模式）

说明

如果设备在本次运行过程中发生过单板被拔出或者成员设备离开 IRF 的情况，在不执行 **save** 的前提下此单板重新插入原槽位或者此成员设备重新加入 IRF 后设备的配置不会丢失。若执行 **save** 命令，将导致该单板或该成员设备的配置丢失。如需恢复该单板或该成员设备的配置，请在重新插入并重启该单板或者该设备重新加入 IRF 并重启设备后，执行 **display current-configuration** 查看原来的当前配置是否恢复，在确保恢复的前提下执行 **save** 命令，该单板或者该成员设备的配置即可自行恢复。（适用于分布式设备）

1.4 配置回滚

1.4.1 配置回滚简介

配置回滚是在不重启设备的情况下，将当前的配置回退到指定配置文件中的配置状态。该配置文件必须是有效的.cfg 文件，它可以使用手工/自动备份功能或者 **save** 命令生成，也可以是别的设备的可兼容配置文件，推荐使用手工/自动备份功能生成。（如何使用手工/自动备份功能生成配置文件请参见“1.4.2 备份当前配置”）

配置回滚主要应用于：

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

说明

为了方便描述，定义如下：

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

1.4.2 备份当前配置

1. 设置备份参数

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

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

表1-7 设置备份参数

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

说明

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

2. 自动/手工备份当前配置

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

当需要对设备进行步骤复杂的配置时，可以在修改配置前手工备份当前配置。以便配置过程中出现失败时，可以使用已备份的配置直接将当前配置回滚至配置改变前的状态。

表1-8 自动备份当前配置

操作	命令	说明
进入系统视图	**system-view**	-
开启自动备份当前配置功能，并设置自动备份的时间间隔	**archive configuration interval** *interval*	缺省情况下，自动备份当前配置功能处于关闭状态

表1-9 手工备份当前配置

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

1.4.3 执行配置回滚

提示

配置回滚期间（即系统在执行 **configuration replace file** 命令时）不能进行单板热拔插和主从设备倒换操作，否则可能会造成配置回滚终止。（分布式设备－独立运行模式/分布式设备－IRF 模式）

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

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

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

- 命令不支持完整 **undo** 命令，即直接在配置命令前添加 **undo** 关键字构成的命令不存在，设备不识别。比如命令 **A [B] C**，对应的 **undo** 命令为 **undo A C**，但是配置 **A B C** 回滚的时候，系统会去自动执行 **undo A B C**，此时系统会认为不支持 **undo A B C** 而造成配置 **A B C** 回滚失败。
- 配置不能取消（如硬件相关的命令）。
- 若不同视图下的各配置命令存在依赖关系，命令可能执行失败。
- 使用的配置文件不是由 **save** 命令、自动备份或手工备份生成的完整文件，或是不同类型设备的配置文件，配置回滚可能不能完全恢复至配置文件中的配置状态。因此，需要用户确保回滚配置文件中配置的正确性和与当前设备的兼容性。
- 配置回滚到指定配置文件时，如果有命令行回滚失败，系统将打印提示信息说明有命令行回滚失败，此时，请执行 **display diff current-configuration configfile** 命令将回滚后的运行配置与目标配置文件中的配置对比，差异部分即为回滚失败的命令行。

表1-10 执行配置回滚

操作	命令	说明
进入系统视图	**system-view**	-
执行配置回滚	**configuration replace file** *filename*	*filename*只能是明文配置文件，不能是被加密的配置文件

1.5 管理下次启动配置文件

1.5.1 设置下次启动配置文件

执行以下操作前，请确保指定文件（*cfgfile*）为设备存储介质根目录下的合法配置文件，否则，操作失败。（集中式设备-独立运行模式）

主用主控板和备用主控板的下次启动配置文件必须是相同的文件，因此，使用本命令前，请确保指定的配置文件已经保存在主用主控板和备用主控板相同类型存储介质的根目录下，否则，操作失败。（分布式设备－独立运行模式）

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

所有成员设备上主控板的下次启动配置文件必须是相同的文件，因此，使用本命令前，请确保指定的配置文件已经保存在 IRF 中所有主控板相同类型存储介质的根目录下，否则，操作失败。（分布式设备－IRF 模式）

使用该命令设置配置文件时：

- 不指定 **main** 和 **back** 参数时，缺省使用 **main**。
- 主用下次启动配置文件和备用下次启动配置文件可以设置为同一文件，但为了更可靠，建议设置为不同的文件，或者将一份配置保存在两个不同名的文件中，一个设置为主用，一个设置为备用。
- 在执行 **undo startup saved-configuration** 命令之后，系统会将主用/备用下次启动配置文件均设置为 NULL，但不会删除该文件。

需要注意的是，

- 执行 **undo startup saved-configuration** 命令并重启 IRF 或 IRF 中的成员设备时，会导致 IRF 分裂，请谨慎使用。（集中式设备-IRF 模式/分布式设备－IRF 模式）
- 执行该命令时需确保当前工作路径是主设备路径，可通过 **pwd** 命令确认当前工作路径。有关 **pwd** 命令的相关介绍请参见“基础配置指导”中的“文件系统管理”。（集中式设备-IRF 模式）
- 执行该命令时需确保当前工作路径是主用主控板路径，可通过 **pwd** 命令确认当前工作路径。有关 **pwd** 命令的相关介绍请参见“基础配置指导”中的“文件系统管理”。（分布式设备－IRF 模式）

表1-11 设置下次启动配置文件

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

说明

执行 **save** [**safely**] [**backup** | **main**] [**force**]命令将当前配置保存到指定配置文件时，系统会自动把该文件设置为设备的主用下次启动配置文件。详细配置请参见“1.3.2 保存当前配置”。

1.5.2 备份/恢复主用下次启动配置文件

说明

设备运行于 FIPS 模式时，不支持备份/恢复主用下次启动配置文件。

备份是指将设备的主用下次启动配置文件备份到指定的 TFTP 服务器；恢复是指将 TFTP 服务器上保存的配置文件下载到设备并设置为主用下次启动配置文件。

1. 配置准备

在执行配置文件的备份操作前，请进行以下操作：

- 保证设备与服务器之间的路由可达，服务器端开启了 TFTP 服务，执行备份操作的客户端设备已获得了相应的读写权限。
- 在任意视图下使用 **display startup** 命令查看一下设备是否已经设置了下次启动配置文件。如果没有下次启动配置文件，或者所设置的配置文件不存在，备份操作将会失败。

2. 备份/恢复主用下次启动配置文件

表1-12 备份/恢复主用下次启动配置文件

操作	命令	说明
将设备的主用下次启动配置文件备份到指定的TFTP服务器	**backup startup-configuration to** { *ipv4-server* | **ipv6** *ipv6-server* } [*dest-filename*] [**vpn-instance** *vpn-instance-name*]	该命令在用户视图下执行
将TFTP服务器上保存的配置文件下载到设备并设置为主用下次启动配置文件	**restore startup-configuration from** { *ipv4-server* | **ipv6** *ipv6-server* } *src-filename* [**vpn-instance** *vpn-instance-name*]	该命令在用户视图下执行 该命令执行成功后，用户可以在任意视图下使用**display startup**命令以及**display saved-configuration**命令验证配置效果

1.5.3 删除下次启动配置文件

注意

- 本特性会将下次启动配置文件从设备上彻底删除，请谨慎使用。（集中式设备-独立运行模式/分布式设备－独立运行模式）
- 本特性会将下次启动配置文件从所有成员设备上彻底删除，请谨慎使用。（集中式设备-IRF 模式/分布式设备－IRF 模式）

出现以下情况时，用户可能需要删除设备中的下次启动配置文件：

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

用户可以只删除主用下次启动配置文件，或者只删除备用下次启动配置文件。如果当前设备的主用下次启动配置文件和备用下次启动配置文件相同，仅执行一次删除操作（假设指定了 **backup** 参数），系统只会将相应的下次启动配置文件设置为 NULL，不会删除该文件，需要再执行一次删除操作（指定 **main** 参数），才能将这个配置文件彻底删除。

下次启动配置文件被删除后，设备重启时，系统将采用出厂配置进行初始化。

表1-13 删除设备中的下次启动配置文件

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

1.6 配置文件管理显示和维护

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

表1-14 配置文件管理显示和维护

操作	命令
显示配置回滚功能的相关信息	**display archive configuration**
显示当前配置	**display current-configuration** [**configuration** [*module-name*] | **controller** | **exclude-provision** | **interface** [*interface-type* [*interface-number*]] | **vpn-instance** [*vpn-instance-name*]]
显示出厂配置	**display default-configuration**
显示下次启动配置文件的内容	**display saved-configuration**
显示用于本次及下次启动的配置文件的名称	**display startup**
显示当前视图下生效的配置	**display this**

目 录

1 软件升级

设备各款型使用的命令行形式有所不同，详细差异信息如下：

命令行形式	款型
集中式	• MSR810/810-W/810-W-DB/810-LM/810-W-LM/810-10-PoE/810-LM-HK/810-W-LM-HK • MSR810-LMS/810-LUS • MSR2600-6-X1/2600-10-X1/2630 • MSR3600-28/3600-51/3600-28-SI/3600-51-SI • MSR3610-X1/3610-X1-DP/3610-X1-DC/3610-X1-DP-DC • MSR 3610/3620/3620-DP/3640/3660 • MSR810-W-WiNet/810-LM-WiNet/830-4LM-WiNet • MSR830-5BEI-WiNet/830-6EI-WiNet/830-10BEI-WiNet • MSR830-6BHI-WiNet/830-10BHI-WiNet • MSR2600-10-X1-WiNet/2630-WiNet • MSR3600-28-WiNet/3610-X1-WiNet • MSR3610-WiNet/3620-10-WiNet/3620-DP-WiNet/3620-WiNet/3660-WiNet • MSR810-LM-GL/810-W-LM-GL • MSR830-6EI-GL/830-10EI-GL/830-6HI-GL/830-10HI-GL • MSR2600-6-X1-GL/3600-28-SI-GL
分布式	MSR5620/5660/5680

1.1 设备软件简介

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

设备上存在主控板和业务板，业务板的 Boot ROM 程序/启动软件包集成在主控板的 Boot ROM 程序/启动软件包中。系统在升级主控板时会自动升级业务板，不需要单独升级业务板。

1.1.1 Boot ROM程序

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

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

1.1.2 启动软件包

1. 启动软件包的分类

启动软件包是用于引导设备启动的程序文件，按其功能可以分为以下几类：

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

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

2. 启动软件包的发布形式

启动软件包有以下两种发布形式：

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

3. 主/备用下次启动软件包以及软件包列表

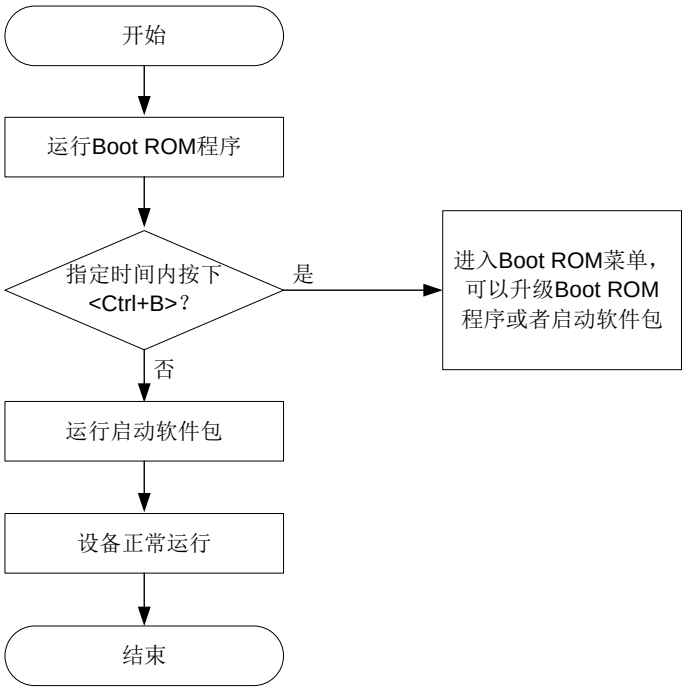
设备下次启动时使用的软件包称为下次启动软件包。用户可通过命令行将本设备存储介质上的某个软件包指定为设备的下次启动软件包，并指定软件包的属性为主用或者备用。被指定为主用属性的软件包称为主用下次启动软件包，被指定为备用属性的软件包称为备用下次启动软件包。

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

1.1.3 设备启动过程

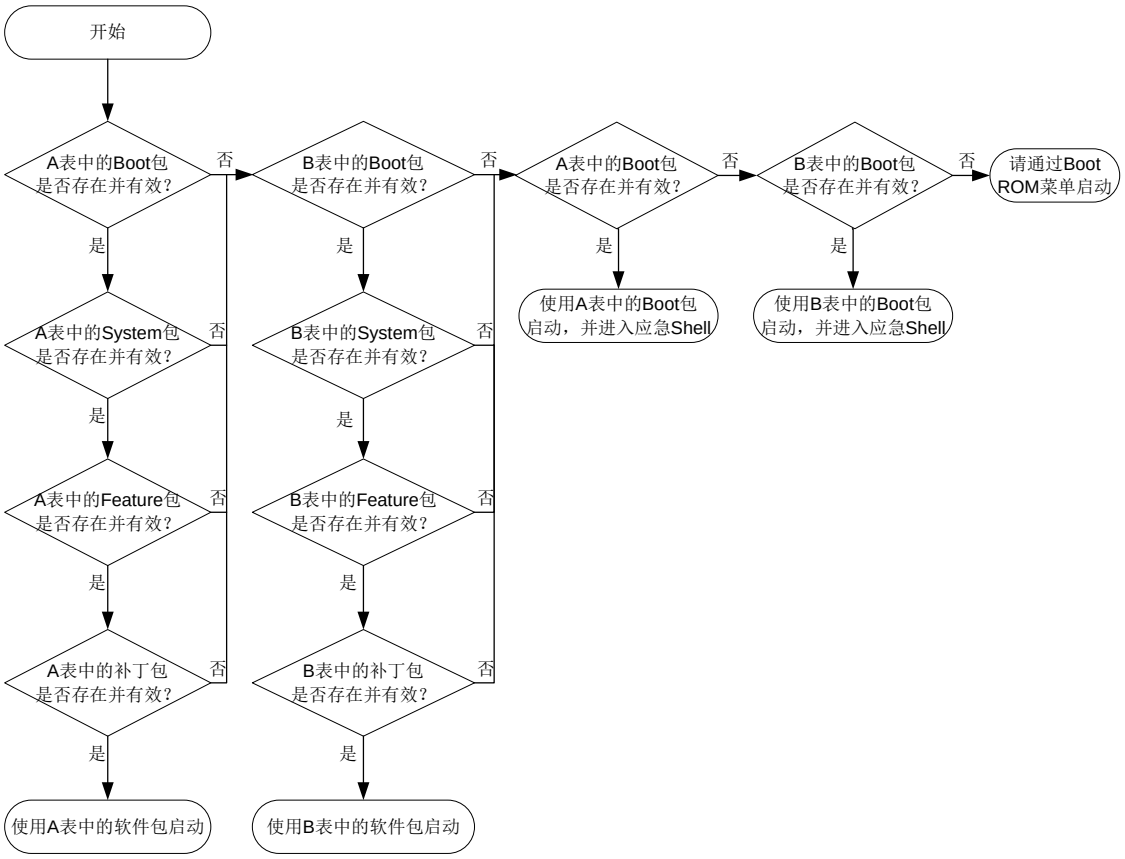
设备上电后，先运行 Boot ROM 文件，初始化硬件并显示设备的硬件参数，然后运行启动软件包，如图 1-1 所示。图中“指定时间”为 5 秒。

图1-1 设备启动过程示意图



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

图1-2 启动软件包运行流程示意图



说明：流程图中“A表”表示主用启动软件包列表，“B表”表示备用启动软件包列表

- 系统会根据启动软件包列表自动判断相应的软件包是否存在，如果存在则继续判断是否有效。如果启动软件包列表中没有 Feature 包/补丁包，则跳过 Feature 包/补丁包的判断流程。
- 当主用和备用启动软件包列表中的 Boot 包均不存在或不可用时，请通过 Boot ROM 菜单进行软件升级。
- 当设备进入应急 Shell 环境时，请使用 Console 口连接到设备，在应急 Shell 环境下，手工重新加载 System 包，才能进入 Comware 系统。具体操作请参见“基础配置指导”中的“应急 Shell”。

1.2 软件升级方式简介

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

表1-1 软件升级方式描述表

升级方式		升级对象	升级说明
通过命令行进行软件升级	通过整机重启方式升级	• Boot ROM 程序 • 启动软件包（该方式不能升级补丁包）	需要重启设备来实现设备软件的升级 使用该方式升级设备软件时会导致当前业务中断
	通过**install**命令升级	启动软件包	通过该方式可以实现对软件包（包括Boot包、System包、Feature包和Patch包）的安装及升级
通过Boot ROM菜单进行软件升级		• Boot ROM 程序 • 启动软件包	可在设备无法正常启动时升级设备软件 当使用该方式升级路由器时，请先连接到路由器的Console接口，断电重启路由器。启动过程中根据提示按<Ctrl+B>进入Boot ROM菜单，通过Boot ROM来重新加载Boot包

1.3 通过整机重启方式升级设备软件

1.3.1 升级步骤

请参照以下步骤来升级设备软件：

(1) 使用 **display version** 命令查看设备当前运行的 Boot ROM 程序以及启动软件的版本。

(2) 获取新软件的版本发布说明书，了解新软件的版本号、软件大小以及和当前 Boot ROM 程序、启动软件的兼容性。

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

(4) 使用 **dir** 命令查看存储介质是否有足够的空间存储新的软件，以免升级失败。如果存储空间不足，可使用 **delete** 命令删除一些暂时不用的文件。关于 **dir** 和 **delete** 命令的详细描述请参见“基础配置命令参考”中的“文件系统管理”。（集中式设备－独立运行模式）

(5) 使用 **dir** 命令分别查看主用主控板和备用主板存储介质是否有足够的空间存储新的软件，以免升级失败。如果存储空间不足，可使用 **delete** 命令删除一些暂时不用的文件。关于 **dir** 和 **delete** 命令的详细描述请参见“基础配置命令参考”中的“文件系统管理”。（分布式设备－独立运行模式）

(6) 使用 **dir** 命令分别查看所有成员设备上存储介质是否有足够的空间存储新的软件，以免升级失败。如果存储空间不足，可使用 **delete** 命令删除一些暂时不用的文件。关于 **dir** 和 **delete** 命令的详细描述请参见“基础配置命令参考”中的“文件系统管理”。（集中式设备－IRF 模式）

(7) 使用 **dir** 命令分别查看全局主用主控板和全局备用主控板上存储介质是否有足够的空间存储新的软件，以免升级失败。如果存储空间不足，可使用 **delete** 命令删除一些暂时不用的文件。关于 **dir** 和 **delete** 命令的详细描述请参见“基础配置命令参考”中的“文件系统管理”。（分布式设备－IRF 模式）

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

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

(10) 指定下次启动软件包并完成升级。

1.3.2 加载Boot ROM程序

设备各款型对于本节所描述的特性支持情况有所不同，详细差异信息如下：

型号	特性	描述
MSR810/810-W/810-W-DB/810-LM/810-W-LM/810-10-PoE/810-LM-HK/810-W-LM-HK/810-LMS/810-LUS	加载Boot ROM程序	不支持
MSR2600-6-X1/2600-10-X1		支持
MSR 2630		支持
MSR3600-28/3600-51		支持
MSR3600-28-SI/3600-51-SI		支持
MSR3610-X1/3610-X1-DP/3610-X1-DC/3610-X1-DP-DC		支持
MSR 3610/3620/3620-DP/3640/3660		支持
MSR5620/5660/5680		支持

型号	特性	描述
MSR810-W-WiNet/810-LM-WiNet	加载Boot ROM程序	不支持
MSR830-4LM-WiNet		不支持
MSR830-5BEI-WiNet/830-6EI-WiNet/830-10BEI-WiNet		不支持
MSR830-6BHI-WiNet/830-10BHI-WiNet		不支持
MSR2600-10-X1-WiNet		支持
MSR2630-WiNet		支持
MSR3600-28-WiNet		支持
MSR3610-X1-WiNet		支持
MSR3610-WiNet/3620-10-WiNet/3620-DP-WiNet/3620-WiNet/3660-WiNet		支持

型号	特性	描述
MSR810-LM-GL	加载Boot ROM程序	不支持
MSR810-W-LM-GL		不支持
MSR830-6EI-GL		不支持
MSR830-10EI-GL		不支持

型号	特性	描述
MSR830-6HI-GL		不支持
MSR830-10HI-GL		不支持
MSR2600-6-X1-GL		支持
MSR3600-28-SI-GL		支持

表1-2 加载 Boot ROM 程序（集中式设备－独立运行模式）

操作	命令	说明
加载新的Boot ROM程序	**bootrom update file** *file-url* **slot** *slot-number-list*	执行该命令，系统会将存储介质中的Boot ROM程序加载到Boot ROM的Normal区 加载后，要使新的Boot ROM程序生效，需要重启设备

表1-3 加载 Boot ROM 程序（分布式设备－独立运行模式/集中式设备－IRF 模式）

操作	命令	说明
加载新的Boot ROM程序	**bootrom update file** *file-url* **slot** *slot-number-list* [**subslot** *subslot-number-list*]	执行该命令，系统会将存储介质中的Boot ROM程序加载到Boot ROM的Normal区 加载后，要使新的Boot ROM程序生效，需要重启设备

表1-4 加载 Boot ROM 程序（分布式设备－IRF 模式）

操作	命令	说明
加载新的Boot ROM程序	**bootrom update file** *file-url* **chassis** *chassis-number* **slot** *slot-number-list* [**subslot** *subslot-number-list*]	执行该命令，系统会将存储介质中的Boot ROM程序加载到Boot ROM的Normal区 加载后，要使新的Boot ROM程序生效，需要重启设备

1.3.3 指定下次启动软件包并完成升级

1. 集中式设备－独立运行模式

当指定下次启动软件包/IPE 文件时，命令中指定的软件包（IPE 文件）必须放在设备存储介质主分区的根目录下且后缀名为.bin（.ipe），文件名中必须包含存储介质的名称，形如 flash:/xx.bin（flash:/xx.ipe）。

表1-5 指定下次启动软件包并完成升级

操作	命令	说明
指定设备下次启动时使用的软件包/IPE文件	**boot-loader file** *ipe-filename* { **backup** | **main** }	二者选其一 命令在用户视图下执行 请不要通过多个用户同时执行该命令，以免配置失败
	boot-loader file boot *boot-package* **system** *system-package* [**feature** *feature-package*&<1-30>] { **backup** | **main** }	
保存当前配置	**save**	保存当前配置，以便当前配置在设备重启后继续生效 保存配置后重启设备，设备将优先使用二进制类型的配置文件，以便提高加载配置的速度 该命令在用户视图下执行
重启设备	**reboot**	设备重启时，会运行新的启动软件包，从而完成升级 该命令在用户视图下执行

2. 分布式设备－独立运行模式

- 当指定下次启动软件包/IPE 文件时，命令中指定的软件包（IPE 文件）必须放在存储介质主分区的根目录下且后缀名为.bin（.ipe），文件名中必须包含存储介质的名称。
- 为备用主控板指定下次启动软件包/IPE 文件时，系统会自动检查存储在指定路径的下次启动软件包/IPE 文件是否已拷贝到备用主控板的存储介质根目录下。如果还未拷贝，则自动从指定路径拷贝一份并设置为备用主控板的主用下次启动软件包/IPE 文件。

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

- 如果主用主控板当前是使用主用启动软件包列表启动的，则将其主用下次启动软件包列表中的软件包拷贝到备用主控板的对应目录下，并设置为备用主控板的主用下次启动软件包。如果这些软件包中有任一软件包不存在或者不可用，则命令执行失败。
- 如果主用主控板当前是使用备用启动软件包列表启动的，则将其备用下次启动软件包列表中的软件包拷贝到备用主控板的对应目录下，并设置为备用主控板的主用下次启动软件包。如果这些软件包中有任一软件包不存在或者不可用，则命令执行失败。

表1-6 指定新的下次启动软件包并完成升级

操作	命令	说明
指定主用主控板下次启动时使用的软件包/IPE文件	**boot-loader file** *ipe-filename* { **all** | **slot** *slot-number* } { **backup** | **main** }	二者选其一 命令在用户视图下执行 请不要通过多个用户同时执行该命令，以免配置失败
	boot-loader file boot *boot-package* **system** *system-package* [**feature** *feature-package*&<1-30>] { **all** | **slot** *slot-number* } { **backup** | **main** }	
指定备用主控板下次启动时使用的软件包/IPE文件	**boot-loader file** *ipe-filename* { **all** | **slot** *slot-number* } { **backup** | **main** }	三者选其一 命令在用户视图下执行 请不要通过多个用户同时执行 **boot-loader file**命令，以免配置
	boot-loader file boot *boot-package* **system** *system-package* [**feature** *feature-package*&<1-30>] { **all** | **slot**	

操作	命令	说明
	slot-number } { **backup** | **main** }	失败
	boot-loader update { **all** | **slot** *slot-number* }	
保存当前配置	**save**	保存当前配置，以便当前配置在设备重启后继续生效 保存配置后重启设备，设备将优先使用二进制类型的配置文件，以便提高加载配置的速度 该命令在用户视图下执行
重启设备	**reboot**	设备重启时，会运行新的启动软件包，从而完成升级 该命令在用户视图下执行

3. 集中式设备－IRF模式

- 当单台设备组成 IRF 时，该设备的角色为主设备，用户只需为主设备指定下次启动软件包。
- 当多台设备组成 IRF 时，用户需要分别为主设备和从设备指定下次启动软件包。

关于 IRF 的详细介绍请参见“IRF 配置指导”中的“IRF”。

- 当指定下次启动软件包/IPE 文件时，命令中指定的软件包（IPE 文件）必须放在存储介质主分区的根目录下且后缀名为.bin（.ipe），文件名中必须包含存储介质的名称。
- 为从设备指定下次启动软件包/IPE 文件时，系统会自动检查存储在指定路径的下次启动软件包/IPE 文件是否已拷贝到从设备的存储介质根目录下。如果还未拷贝，则自动从指定路径拷贝一份并设置为从设备的下次启动软件包/IPE 文件。

通过命令 **boot-loader update slot** *slot-number* 指定从设备的下次启动软件包时，系统会进行如下处理：

- 如果主设备当前是使用主用启动软件包列表启动的，则将其主用下次启动软件包列表中的软件包拷贝到从设备的对应目录下，并设置为从设备的主用下次启动软件包。如果这些软件包中有任一软件包不存在或者不可用，则命令执行失败。
- 如果主设备当前是使用备用启动软件包列表启动的，则将其备用下次启动软件包列表中的软件包拷贝到从设备的对应目录下，并设置为从设备的主用下次启动软件包。如果这些软件包中有任一软件包不存在或者不可用，则命令执行失败。

表1-7 指定新的下次启动软件包并完成升级

操作	命令	说明
指定主设备下次启动时使用的软件包/IPE文件	**boot-loader file** *ipe-filename* { **all** | **slot** *slot-number* } { **backup** | **main** }	二者选其一 命令在用户视图下执行 请不要通过多个用户同时执行该命令，以免配置失败 执行本命令时，请不要重启任何成员设备，以免设备不能正常启动
	boot-loader file boot *boot-package* **system** *system-package* [**feature** *feature-package*&<1-30>] { **all** | **slot** *slot-number* } { **backup** | **main** }	
指定从设备下次启动时使用的软件包/IPE文件	**boot-loader file** *ipe-filename* { **all** | **slot** *slot-number* } { **backup** | **main** }	三者选其一 命令在用户视图下执行
	boot-loader file boot *boot-package* **system**	

操作	命令	说明
	system-package [**feature** *feature-package*&<1-30>] { **all** | **slot** *slot-number* } { **backup** | **main** }	请不要通过多个用户同时执行**boot-loader file**命令，以免配置失败 执行本命令时，请不要重启任何成员设备，以免设备不能正常启动
	boot-loader update { **all** | **slot** *slot-number* }	
保存当前配置	**save**	保存当前配置，以便当前配置在设备重启后继续生效 保存配置后重启设备，设备将优先使用二进制类型的配置文件，以便提高加载配置的速度 该命令在用户视图下执行
重启IRF中所有设备	**reboot**	所有成员设备重启时，会运行新的启动软件包，从而完成整个IRF的升级 该命令在用户视图下执行

4. 分布式设备－IRF模式

- 如果 IRF 中只有一个成员设备，且成员设备上只有一块主控板，则这块主控板是全局主用主控板，用户只需为全局主用主控板指定下次启动软件包。
- 如果 IRF 中有多块主控板，则用户需要分别为全局主用主控板和全局备用主控板指定下次启动软件包。

关于 IRF 的详细介绍请参见“IRF 配置指导”中的“IRF”。

- 当指定下次启动软件包/IPE 文件时，命令中指定的软件包（IPE 文件）必须放在存储介质主分区的根目录下且后缀名为.bin（.ipe），文件名中必须包含存储介质的名称。
- 为全局备用主控板指定下次启动软件包/IPE 文件时，系统会自动检查存储在指定路径的下次启动软件包/IPE 文件是否已拷贝到全局备用主控板的存储介质根目录下。如果还未拷贝，则从指定路径拷贝一份并设置为全局备用主控板的下次启动软件包/IPE 文件。

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

- 如果全局主用主控板当前是使用主用启动软件包列表启动的，则将其主用下次启动软件包列表中的软件包拷贝到全局备用主控板的对应目录下，并设置为全局备用主控板的主用下次启动软件包。如果这些软件包中有任一软件包不存在或者不可用，则命令执行失败。
- 如果全局主用主控板当前是使用备用启动软件包列表启动的，则将其备用下次启动软件包列表中的软件包拷贝到全局备用主控板的对应目录下，并设置为全局备用主控板的主用下次启动软件包。如果这些软件包中有任一软件包不存在或者不可用，则命令执行失败。

表1-8 指定新的下次启动软件包并完成升级

操作	命令	说明
指定全局主用主控板下次启动时使用的软件包/IPE文件	**boot-loader file** *ipe-filename* { **all** | **chassis** *chassis-number* **slot** *slot-number* } { **backup** | **main** }	二者选其一 命令在用户视图下执行 请不要通过多个用户同时执行该命令，以免配置失败 执行本命令时，请不要重启任何单
	boot-loader file boot *boot-package* **system** *system-package* [**feature** *feature-package*&<1-30>] { **all** | **chassis** *chassis-number* **slot** *slot-number* } { **backup** |	

操作	命令	说明
	main }	板，以免单板不能正常启动
指定全局备用主控板下次启动时使用的软件包/IPE文件	**boot-loader file** *ipe-filename* { **all** | **chassis** *chassis-number* **slot** *slot-number* } { **backup** | **main** }	三者选其一 命令在用户视图下执行 请不要通过多个用户同时执行**boot-loader file**命令，以免配置失败 执行本命令时，请不要重启任何单板，以免单板不能正常启动
	boot-loader file boot *boot-package* **system** *system-package* [**feature** *feature-package*&<1-30>] { **all** | **chassis** *chassis-number* **slot** *slot-number* } { **backup** | **main** }	
	boot-loader update { **all** | **chassis** *chassis-number* **slot** *slot-number* }	
保存当前配置	**save**	保存当前配置，以便当前配置在设备重启后继续生效 保存配置后重启设备，设备将优先使用二进制类型的配置文件，以便提高加载配置的速度 该命令在用户视图下执行
重启IRF	**reboot**	所有主控板重启时，会运行新的启动软件包，从而完成整个IRF的升级 该命令在用户视图下执行

1.4 通过install命令升级

1.4.1 通过install命令升级策略

软件在发布的时候，开发会根据当前版本和历史版本是否兼容以及兼容的程度，制定升级策略。通过 **install** 命令升级策略有四种：增量升级、软重启升级、重启升级以及不兼容升级。

进行 **install** 命令方式前，请先将要升级的目标软件包下载到设备存储介质的根目录下，然后通过 **display version comp-matrix file** 命令显示设备将采用的升级策略。升级策略不同对当前业务的影响不同，采用的升级步骤也会有差异。

表1-9 install 命令升级策略描述表

升级策略		描述	对应 **display version comp-matrix file** 命令中的显示信息
兼容升级	增量升级	本策略用于只有用户态进程需要更新时。使用该策略升级时，系统会仅对有差异的用户态进程实施升级，并通过进程的备份和倒换来保证升级过程中业务不中断。该策略对系统影响最小、升级速度最快	Upgrade Way字段显示为： • Service Upgrade：表示服务级增量升级，该策略仅对本业务模块有影响，对系统以及其他业务模块没有影响 • File Upgrade：表示文件级增量升级。该策略仅对系统内的、用户不可见的程序文件进行升级，对系统以及业务模块没有影响
	重启升级（集中式设	本策略用于版本间的差异仍属于兼容范围内，但无法进行增量和软重启时。该方式通过重启	Upgrade Way字段显示为Reboot时，表示采用的是重启升级方式

升级策略		描述	对应 **display version comp-matrix file** 命令中的显示信息
	备—独立运行模式）	本设备加载新软件来完成升级，因此，升级过程会到导致业务中断	
	重启升级（分布式设备－独立运行模式）	本策略用于版本间的差异仍属于兼容范围内，但无法进行增量和软重启时。该方式通过重启单板加载新软件来完成升级 重启升级过程中，除了正在重启的主控板，其它主控板均处于工作状态，从而保证了升级过程中业务不中断	Upgrade Way字段显示为Reboot时，表示该单板升级时会直接重启来加载新软件
	重启升级（集中式设备—IRF模式）	本策略用于版本间的差异仍属于兼容范围内，但无法进行增量和软重启时。采用该方式时，系统会自动重启本成员设备，并在重启过程中加载新软件来完成本设备的软件升级 重启升级过程中，除了正在重启的成员设备，其它成员设备均处于工作状态，从而保证了升级过程中业务不中断	Upgrade Way字段显示为Reboot时，表示采用的是重启升级方式
	重启升级（分布式设备－IRF模式）	该方式通过重启单板加载新软件来完成升级 重启升级过程中，除了正在重启的成员设备/主控板，其它成员设备/主控板均处于工作状态，从而保证了升级过程中业务不中断	Upgrade Way字段显示为Reboot时，表示该单板升级时会直接重启来加载新软件
不兼容升级（集中式设备—独立运行模式）		表示设备当前运行的软件版本和要升级的目标软件版本不兼容时的升级	Incompatible upgrade
不兼容升级（分布式设备－独立运行模式）		表示设备当前运行的软件版本和要升级的目标软件版本不兼容时的升级 不兼容版本因为版本差异较大，所以，在同一个系统中，两个版本不能同时运行。因此，不兼容升级过程中： **1.** 请先将备用主控板升级到新版本，备用主控板升级完成后，系统会将它处于隔离状态，不能转发报文，主用主控板处于工作状态 **2.** 然后执行主备倒换操作，此时，备用主控板变成主用主控板，自动接替原主用主控板工作，原主用主控板重启完成升级	Incompatible upgrade
不兼容升级（集中式设备—IRF模式/分布式设备－IRF模式）		表示设备当前运行的软件版本和要升级的目标软件版本不兼容时的升级 不兼容版本因为版本差异较大，所以，在同一个系统中，两个版本不能同时运行。因此，不兼容升级过程中： **1.** 请先将某个（些）备设备升级到新版本，备设备升级完成后，系统会将它处于隔离状态，不能转发报文，主设备和其它没有升级的备设备处于工作状态 **2.** 然后执行主备倒换操作，此时，备设备变成主设备，自动接替原主设备工作，原主设备和其它没有升级的备设备逐个重启完成升级	Incompatible upgrade

1.4.2 升级指导

在升级过程中，请遵循以下指导：

- 请确保网络拓扑稳定，禁止手工重启单板和插拔单板。
- 请确保系统中除了当前执行升级命令的用户外无其他用户登录。
- 请不要执行 **install** 升级命令之外的配置命令，包括配置修改及信息查询等。
- 禁止对启动软件包进行修改、删除以及重命名等操作。
- 执行 **install activate** 或 **install deactivate** 命令前，请使用 **display system stable state** 命令查看设备是否处于稳定状态。只有 System State 处于 Stable 状态，才能进行该升级。关于 **display system stable state** 命令的详细介绍请参见“基础配置命令参考”中的“设备管理”。
- **install** 命令升级完成后，如需配置设备，请重新登录。

1.4.3 通过IPE文件获得软件包

如果用户要升级的软件包是以 IPE 文件的形式发布的，请在执行其它 **install** 命令前，先按以下步骤将 IPE 包解压缩：

(1) 通过 FTP 或 TFTP 将 IPE 文件下载到设备存储介质的根目录。

(2) 通过 **display install ipe-info** 命令查看该 IPE 文件中包含的软件包。

(3) 解压缩 IPE 文件：将 IPE 文件解压缩，生成软件包。

表1-10 解压缩 IPE 文件

操作	命令	说明
解压缩IPE文件	**install add** *ipe-filename medium-name*:	该命令在用户视图下执行

1.4.4 激活软件包

执行 **install activate** 命令可以安装/升级软件包。如果当前系统没有运行相同类型的软件包，则该过程称为安装软件包；如果当前系统有相同类型的软件包在运行，则该过程称为升级软件包。

在执行激活软件包前，请注意以下事项：

(1) 当需要升级两个或两个以上软件包时，请选择以下任意一种方法来激活软件包：

- 方法一：使用一条命令激活完一个 **slot** 的所有软件包后再激活另一个 **slot** 的所有软件包。
- 方法二：先升级完所有 **slot** 的某种类型的包（比如 Boot 包）之后，再升级所有 **slot** 的另外一种类型的包（比如 System 包）。

(2) 安装新 Feature 包/补丁包时，必须先激活主用主控板；升级已有软件包时，若存在备用主控板，必须先激活备用主控板，再激活主用主控板。否则，安装/升级过程可能出错。（分布式设备－独立运行模式）

(3) 安装新 Feature 包/补丁包时，必须先激活主设备；升级已有软件包时，必须先激活从设备，再激活主设备。否则，安装/升级过程可能出错。（集中式设备—IRF 模式）

(4) 安装以成员设备为单位进行，先激活主设备，再激活从设备；成员设备内安装时，必须激活主用主控板；升级也以成员设备为单位进行，先激活从设备，再激活主设备；成员设备内升级时，必须先激活备用主控板，再激活主用主控板。（分布式设备－IRF 模式）

(5) 安装/升级主用主控板的软件时，系统会根据版本需要自动同时激活业务板的软件，因此，业务板不需要单独执行激活操作。（分布式设备－独立运行模式/分布式设备－IRF 模式）

(6) 对于增量升级和补丁包升级方式，软件包激活只在设备本次运行过程中生效，用户只有通过 **install commit** 命令确认软件包的更改后，才能使此次激活的软件包在系统重启后仍处于激活状态；对于软重启和重启升级方式，该步骤可选，因为用户在执行 **install activate** 命令时，系统已经修改了下次启动软件列表，升级软件包会在系统重启后继续生效。

(7) 设备上可安装的软件包（包括 Boot 包、System 包、Feature 包和补丁包）共为 32 个，其中 Boot 包和 System 包只能安装一个，Feature 包和补丁包总共可安装 30 个。

1. 激活Boot包/System包/Feature包

表1-11 激活 Boot 包/System 包/Feature 包

操作	命令	说明
（可选）显示Boot包/System包/Feature包的升级策略（集中式设备—独立运行模式）	**install activate** { **boot** *filename* | **system** *filename* | **feature** *filename*&<1-30> } * **test**	该命令在用户视图下执行
（可选）显示Boot包/System包/Feature包的升级策略（集中式设备—IRF模式）	**install activate** { **boot** *filename* | **system** *filename* | **feature** *filename*&<1-30> } * **slot** *slot-number* **test**	该命令在用户视图下执行
（可选）显示Boot包/System包/Feature包的升级策略（分布式设备－独立运行模式）	**install activate** { **boot** *filename* | **system** *filename* | **feature** *filename*&<1-30> } * **slot** *slot-number* **test**	该命令在用户视图下执行
（可选）显示Boot包/System包/Feature包的升级策略（分布式设备－IRF模式）	**install activate** { **boot** *filename* | **system** *filename* | **feature** *filename*&<1-30> } * **chassis** *chassis-number* **slot** *slot-number* **test**	该命令在用户视图下执行
激活Boot包/System包/Feature包（集中式设备—独立运行模式）	**install activate** { **boot** *filename* | **system** *filename* | **feature** *filename*&<1-30> } *	该命令在用户视图下执行
激活Boot包/System包/Feature包（集中式设备—IRF模式）	**install activate** { **boot** *filename* | **system** *filename* | **feature** *filename*&<1-30> } * **slot** *slot-number*	该命令在用户视图下执行
激活Boot包/System包/Feature包（分布式设备－独立运行模式）	**install activate** { **boot** *filename* | **system** *filename* | **feature** *filename*&<1-30> } * **slot** *slot-number*	该命令在用户视图下执行
激活Boot包/System包/Feature包（分布式设备－IRF模式）	**install activate** { **boot** *filename* | **system** *filename* | **feature** *filename*&<1-30> } * **chassis** *chassis-number* **slot** *slot-number*	该命令在用户视图下执行
（可选）确认软件包更改	**install commit**	该命令在用户视图下执行

2. 激活补丁包

安装补丁包前，需进行如下操作：

- 如果当前设备上未安装补丁包，那么直接安装补丁包。
- 如果当前设备上已安装补丁包，则需查看版本说明书，对比新旧补丁包之间的功能差异：
  - 若新版本的补丁包中包含旧版本补丁包中的所有功能，且在安装完新版本的补丁后旧版本的补丁还存在，为了清理存储空间，可以手工卸载并删除旧版本的补丁包，不会影响设备的运行。
  - 若新版本的补丁包中不包含或不完全包含旧版本补丁包中的所有功能，请不要对旧版本的补丁包进行卸载或删除操作。

表1-12 激活补丁包

操作	命令	说明
激活补丁包（集中式设备—独立运行模式）	**install activate patch** *filename*	该命令在用户视图下执行
激活补丁包（集中式设备—IRF模式）	**install activate patch** *filename* { **all** | **slot** *slot-number* }	该命令在用户视图下执行
激活补丁包（分布式设备－独立运行模式）	**install activate patch** *filename* { **all** | **slot** *slot-number* }	该命令在用户视图下执行
激活补丁包（分布式设备－IRF模式）	**install activate patch** *filename* { **all** | **chassis** *chassis-number* **slot** *slot-number* }	该命令在用户视图下执行
（可选）确认软件包更改	**install commit**	该命令在用户视图下执行

说明

如果产品针对同一 System 包发布了多个补丁包，直接安装最新版本的补丁包即可，且不需要先卸载旧的补丁包。

1.4.5 卸载Feature包/补丁包

因为 Boot 包和 System 包是设备运行的基础软件，所以 Boot 包和 System 包不支持卸载，只能卸载 Feature 包和补丁包。当 Feature 包/补丁包被卸载后，该软件包将处于未激活状态，系统也将不再具备该软件包提供的功能。但是软件包仍然存在于存储介质上，可以通过 **install remove** 命令将卸载后的软件包从存储介质上彻底删除。

Feature 包/补丁包卸载也只在设备本次运行过程中生效。如果用户希望系统重启后，Feature 包/补丁包卸载依然生效，请用户使用 **install commit** 命令确认软件包的更改。

表1-13 卸载 Feature 包

操作	命令	说明
卸载Feature包（集中式设备—独立运行模式）	**install deactivate feature** *filename*&<1-30>	该命令在用户视图下执行
卸载Feature包（集中式设备—IRF模	**install deactivate feature** *filename*&<1-30> **slot** *slot-number*	该命令在用户视图下执行

操作	命令	说明
式）		
卸载Feature包（分布式设备－独立运行模式）	**install deactivate feature** *filename*&<1-30> **slot** *slot-number*	该命令在用户视图下执行
卸载Feature包（分布式设备－IRF模式）	**install deactivate feature** *filename*&<1-30> **chassis** *chassis-number* **slot** *slot-number*	该命令在用户视图下执行
（可选）确认软件包更改	**install commit**	该命令在用户视图下执行

表1-14 卸载补丁包

操作	命令	说明
卸载补丁包（集中式设备—独立运行模式）	**install deactivate patch** *filename*	该命令在用户视图下执行
卸载补丁包（集中式设备—IRF模式）	**install deactivate patch** *filename* { **all** | **slot** *slot-number* }	该命令在用户视图下执行
卸载补丁包（分布式设备－独立运行模式）	**install deactivate patch** *filename* { **all** | **slot** *slot-number* }	该命令在用户视图下执行
卸载补丁包（分布式设备－IRF模式）	**install deactivate patch** *filename* { **all** | **chassis** *chassis-number* **slot** *slot-number* }	该命令在用户视图下执行
（可选）确认软件包更改	**install commit**	该命令在用户视图下执行

1.4.6 软件包回滚

每次激活或者卸载软件包之后，系统中将运行新的软件特性集（即不同于升级前的软件包集合），系统将这些变化记录为回滚点。通过回滚功能，可将系统回滚到某个历史状态，或者恢复到 **install** 命令升级初始状态。

当升级方式为增量升级时，软件包回滚只在设备本次运行过程中生效，用户只有通过 **install commit** 命令确认软件包的更改后，才能使此次的回滚操作在系统重启后生效。系统最多支持 50 个回滚点，当回滚点超过最大值时，旧的回滚点会被删除，新的回滚点会被保存。

当升级方式为软重启或重启升级时，旧的回滚点会被删除，系统只支持一次回滚，即只支持回滚到系统升级初始状态。

表1-15 软件包回滚

操作	命令	说明
软件包回滚	**install rollback to** { *point-id* | **original** }	执行该命令前，可通过**display install rollback**命令查看回滚点信息 补丁包不支持回滚操作 该命令在用户视图下执行

操作	命令	说明
（可选）确认软件包更改	**install commit**	该命令在用户视图下执行

1.4.7 取消软件包操作

增量升级方式下，当系统正在执行软件包的激活或卸载操作时，用户可以通过 **install abort** 命令或者按 Ctrl+C 取消正在执行中的操作，从而使系统回退到操作前的状态。

表1-16 取消软件包操作

操作	命令	说明
取消正在执行的**install**命令升级操作	**install abort** [*job-id*]	该命令在用户视图下执行

1.4.8 校验Boot包/System包/Feature包

为了保证设备进行 **install** 命令升级之后能够正常运行，需要执行本命令对软件包进行如下检验：

完整性：检验 Boot 包、System 包和 Feature 包的完整性。

一致性：检验系统内各激活的软件包列表的差异，以方便用户知道系统内各软件包版本是否一致。

软件包状态：检查各设备上激活的软件包列表和确认的软件包列表之间的差异，以方便用户知道是否有未确认的软件包。

当发现有不一致的软件包时，用户可使用 **install activate** 命令或 **install deactivate** 命令更新激活的软件包列表，使用 **install commit** 命令更新确认的软件包列表。

表1-17 校验 Boot 包/System 包/Feature 包

操作	命令	说明
Boot包/System包/Feature包校验	**install verify**	该命令在用户视图下执行

1.4.9 删除软件包

软件包升级成功后，可以通过以下步骤删除旧版本的软件包。

需要注意的是，执行删除操作后，软件包会从设备上彻底删除，用户将不能执行与该软件包相关的 **install rollback to** 或者 **install abort** 命令。请确认不需要使用该软件包之后，再执行删除操作。

表1-18 删除软件包

操作	命令	说明
删除软件包（集中式设备—独立运行模式）	**install remove** { *filename* | **inactive** }	该命令在用户视图下执行
删除软件包（集中式设备—IRF模式）	**install remove** [**slot** *slot-number*] { *filename* | **inactive** }	该命令在用户视图下执行
删除软件包（分布式设	**install remove** [**slot** *slot-number*]	该命令在用户视图下执行

操作	命令	说明
备－独立运行模式）	{ *filename* | **inactive** }	
删除软件包（分布式设备－IRF模式）	**install remove** [**chassis** *chassis-number* **slot** *slot-number*] { *filename* | **inactive** }	该命令在用户视图下执行

1.5 开启备用主控板启动软件包自动加载功能

注意

- 加载启动软件包需要一定时间，在加载期间，请不要插拔主控板或者手工重启备用主控板，否则，会导致备用主控板加载启动软件包失败而不能启动。用户可打开日志信息显示开关，并根据日志信息的内容来判断加载过程是否开始以及是否结束。
- 本节所述命令只在分布式设备－独立运行模式下支持。

在独立运行模式下，用户可使用本特性来自动保证备用主控板和主用主控板启动软件包版本的一致性；在 IRF 模式下，用户可使用“开启启动文件的自动加载功能”来自动保证全局备用主控板和全局主用主控板启动软件包版本的一致性。关于“开启启动文件的自动加载功能”的详细介绍请参见“IRF 配置指导”中的“IRF”。

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

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

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

表1-19 开启备用主控板启动软件包自动加载功能

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

1.6 升级CPLD和FPGA等固件

设备上某些固件（包括 CPLD、FPGA、CPU、3G Modem 模块等）运行的不是 Comware 系统，这样的固件需要使用特定的软件单独升级。

固件升级后需要对其所在的板卡进行下电后重新上电才能生效，对板卡下电的方式有：切断外部电源、插拔板卡、使用 **power-supply off** 和 **power-supply on** 命令等方式，请根据板卡的实际支持情况，选择下电方式。

表1-20 升级固件

操作	命令	说明
升级CPLD、FPGA等固件（集中式设备－独立运行模式）	**firmware update slot** *slot-number* { **cpld** *cpld-number* | **cpu** *cpu-number* | **fpga** *fpga-number* | **module** *module-number* } **file** *filename*	本命令在用户视图下执行
升级CPLD、FPGA等固件（分布式设备－独立运行模式/集中式设备－IRF模式）	**firmware update slot** *slot-number* **subslot** *subslot-number* { **cpld** *cpld-number* | **cpu** *cpu-number* | **fpga** *fpga-number* | **module** *module-number* } **file** *filename*	本命令在用户视图下执行
升级CPLD、FPGA等固件（分布式设备－IRF模式）	**firmware update chassis** *chass-number* **slot** *slot-number* **subslot** *subslot-number* { **cpld** *cpld-number* | **cpu** *cpu-number* | **fpga** *fpga-number* | **module** *module-number* } **file** *filename*	本命令在用户视图下执行

1.7 软件升级显示和维护

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

请在用户视图下执行 **reset** 命令。

表1-21 软件升级显示和维护（集中式设备—独立运行模式）

操作	命令
显示本次启动和下次启动所采用的启动软件包的名称	**display boot-loader**
显示设备将采用的升级策略	**display version comp-matrix file** { **boot** *filename* | **system** *filename* | **feature** *filename*&<1-30> } * **display version comp-matrix file ipe** *ipe-filename*
显示当前系统中已激活的软件包的相关信息	**display install active** [**verbose**]
显示存储介质根目录下、没有被激活的所有软件包的相关信息	**display install inactive** [**verbose**]
显示设备下次启动时使用的主用软件包的相关信息	**display install committed** [**verbose**]
显示设备下次启动时使用的备用软件包的相关信息	**display install backup** [**verbose**]
显示系统中正在执行的激活、卸载、回滚三种操作	**display install job**

操作	命令
显示与**install**命令升级相关的日志	**display install log** [*log-id*] [**verbose**]
显示软件包信息	**display install package** { *filename* | **all** } [**verbose**]
显示IPE文件信息	**display install ipe-info** *ipe-filename*
显示回滚点信息	**display install rollback** [*point-id*]
显示一个组件或文件所属的软件包	**display install which** { **component** *name* | **file** *filename* }
清除**install**命令升级日志	**reset install log-history oldest** *log-number*
清除回滚点	**reset install rollback oldest** *point-id*

表1-22 软件升级显示和维护（分布式设备－独立运行模式）

操作	命令
显示本次启动和下次启动所采用的启动软件包的名称	**display boot-loader** [**slot** *slot-number*]
显示设备将采用的升级策略	**display version comp-matrix file** { **boot** *filename* | **system** *filename* | **feature** *filename*&<1-30> } * **display version comp-matrix file ipe** *ipe-filename*
显示当前系统中已激活的软件包的相关信息	**display install active** [**slot** *slot-number*] [**verbose**]
显示存储介质根目录下、没有被激活的所有软件包的相关信息	**display install inactive** [**slot** *slot-number*] [**verbose**]
显示设备下次启动时使用的主用软件包的相关信息	**display install committed** [**slot** *slot-number*] [**verbose**]
显示设备下次启动时使用的备用软件包的相关信息	**display install backup** [**slot** *slot-number*] [**verbose**]
显示系统中正在执行的激活、卸载、回滚三种操作	**display install job**
显示与**install**命令升级相关的日志	**display install log** [*log-id*] [**verbose**]
显示软件包信息	**display install package** { *filename* | **all** } [**verbose**]
显示IPE文件信息	**display install ipe-info** *ipe-filename*
显示回滚点信息	**display install rollback** [*point-id*]
显示一个组件或文件所属的软件包	**display install which** { **component** *name* | **file** *filename* } [**slot** *slot-number*]
清除**install**命令升级日志	**reset install log-history oldest** *log-number*
清除回滚点	**reset install rollback oldest** *point-id*

表1-23 软件升级显示和维护（集中式设备—IRF 模式）

操作	命令
显示本次启动和下次启动所采用的启动软件包的名称	**display boot-loader** [**slot** *slot-number*]
显示设备将采用的升级策略	**display version comp-matrix file** { **boot** *filename* | **system** *filename* | **feature** *filename*&<1-30> } * **display version comp-matrix file ipe** *ipe-filename*
显示当前系统中已激活的软件包的相关信息	**display install active** [**slot** *slot-number*] [**verbose**]
显示存储介质根目录下、没有被激活的所有软件包的相关信息	**display install inactive** [**slot** *slot-number*] [**verbose**]
显示设备下次启动时使用的主用软件包的相关信息	**display install committed** [**slot** *slot-number*] [**verbose**]
显示设备下次启动时使用的备用软件包的相关信息	**display install backup** [**slot** *slot-number*] [**verbose**]
显示系统中正在执行的激活、卸载、回滚三种操作	**display install job**
显示与**install**命令升级相关的日志	**display install log** [*log-id*] [**verbose**]
显示软件包信息	**display install package** { *filename* | **all** } [**verbose**]
显示IPE文件信息	**display install ipe-info** *ipe-filename*
显示回滚点信息	**display install rollback** [*point-id*]
显示一个组件或文件所属的软件包	**display install which** { **component** *name* | **file** *filename* } [**slot** *slot-number*]
清除**install**命令升级日志	**reset install log-history oldest** *log-number*
清除回滚点	**reset install rollback oldest** *point-id*

表1-24 软件升级显示和维护（分布式设备－IRF 模式）

操作	命令
显示本次启动和下次启动所采用的启动软件包的名称	**display boot-loader** [**chassis** *chassis-number* [**slot** *slot-number*]]
显示设备将采用的升级策略	**display version comp-matrix file** { **boot** *filename* | **system** *filename* | **feature** *filename*&<1-30> } * **display version comp-matrix file ipe** *ipe-filename*
显示当前系统中已激活的软件包的相关信息	**display install active** [**chassis** *chassis-number* **slot** *slot-number*] [**verbose**]
显示存储介质根目录下、没有被激活的所有软件包的相关信息	**display install inactive** [**chassis** *chassis-number* **slot** *slot-number*] [**verbose**]
显示设备下次启动时使用的主用软件包的相关信息	**display install committed** [**chassis** *chassis-number* **slot** *slot-number*] [**verbose**]
显示设备下次启动时使用的备用软件包	**display install backup** [**chassis** *chassis-number* **slot** *slot-number*]

操作	命令
的相关信息	[**verbose**]
显示系统中正在执行的激活、卸载、回滚三种操作	**display install job**
显示与**install**命令升级相关的日志	**display install log** [*log-id*] [**verbose**]
显示软件包信息	**display install package** { *filename* | **all** } [**verbose**]
显示IPE文件信息	**display install ipe-info** *ipe-filename*
显示回滚点信息	**display install rollback** [*point-id*]
显示一个组件或文件所属的软件包	**display install which** { **component** *name* | **file** *filename* } [**chassis** *chassis-number* **slot** *slot-number*]
清除**install**命令升级日志	**reset install log-history oldest** *log-id*
清除回滚点	**reset install rollback oldest** *point-id*

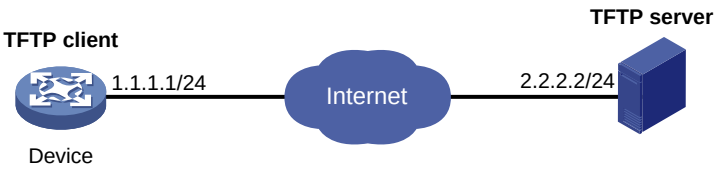
1.8 通过重启方式升级启动软件包配置举例（集中式设备－独立运行模式）

1. 配置需求

使用最新软件版本文件 startup-a2105.ipe，对设备启动软件包进行升级，使设备使用新的启动软件包运行。

2. 组网图

图1-3 通过重启方式升级启动软件包配置举例组网图



3. 配置步骤

说明

为了保险起见，在配置主用下次启动软件包/IPE 文件时，建议将主用下次启动软件包/IPE 文件进行备份，再将备份文件设置为备用下次启动软件包/IPE 文件。如果 Flash 上存储空间有限，可以不备份。

配置 IP 地址以及路由，确保 Device 和 TFTP server 之间路由可达。配置步骤略。

查看设备当前使用的启动软件包的版本。

```
<Sysname> display version
```

复制设备当前使用的启动软件包。

```
<Sysname> copy boot.bin boot_backup.bin
```

```
<Sysname> copy system.bin system_backup.bin
```

指定设备下次启动时使用的备用软件包为 boot_backup.bin/system_backup.bin。

```
<Sysname> boot-loader file boot flash:/boot_backup.bin system flash:/system_backup.bin
backup
```

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

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

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

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

查看主用、备用下次启动 IPE 文件是否配置成功。

```
<Sysname> display boot-loader
```

重启设备，以便运行新的启动软件包完成升级。

```
<Sysname> reboot
```

4. 验证配置

设备重启后，查看设备使用的启动软件包的版本。

```
<Sysname> display version
```

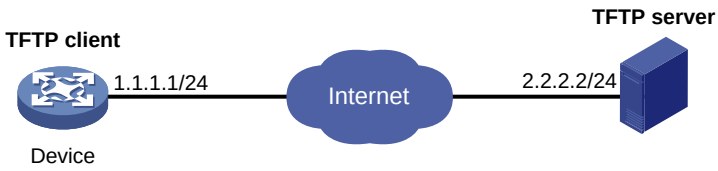
1.9 通过重启方式升级启动软件包配置举例（分布式设备—独立运行模式）

1. 配置需求

- Device 上有两块主控板：主用主控板所在槽位号为 0，备用主控板所在槽位号为 1。
- 现要求对设备启动软件包进行升级，使设备使用新的启动软件包运行。

2. 组网图

图1-4 通过重启方式升级启动软件包配置举例组网图



3. 配置步骤

说明

为了保险起见，在配置主用下次启动软件包/IPE 文件时，建议将主用下次启动软件包/IPE 文件进行备份，再将备份文件设置为备用下次启动软件包/IPE 文件。如果 Flash 上存储空间有限，可以不备份。

配置 IP 地址以及路由，确保 Device 和 TFTP server 之间路由可达。配置步骤略。

查看设备当前使用的启动软件包的版本。

```
<Sysname> display version
```

复制设备当前使用的启动软件包。

```
<Sysname> copy boot.bin boot_backup.bin
<Sysname> copy system.bin system_backup.bin
```

指定所有主控板下次启动时使用的备用软件包为 boot_backup.bin/system_backup.bin。

```
<Sysname> boot-loader file boot flash:/boot_backup.bin system flash:/system_backup.bin slot 0 backup
<Sysname> boot-loader file boot flash:/boot_backup.bin system flash:/system_backup.bin slot 1 backup
```

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

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

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

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

查看主用、备用下次启动 IPE 文件是否配置成功。

```
<Sysname> display boot-loader
```

重启设备，以便运行新的启动软件包完成升级。

```
<Sysname> reboot
```

4. 验证配置

设备重启后，查看设备使用的启动软件包的版本。

```
<Sysname> display version
```

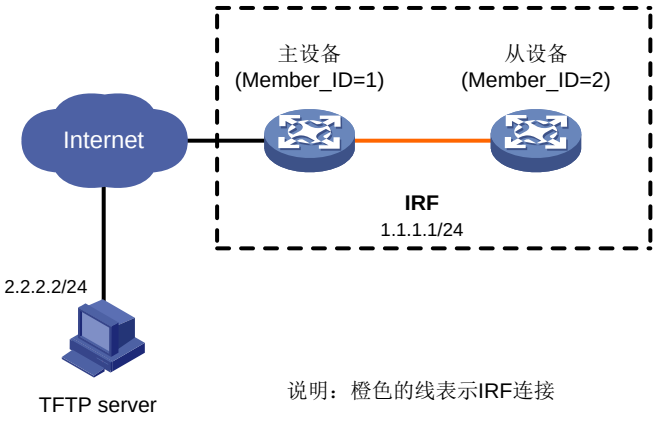
1.10 通过重启方式升级启动软件包配置举例（集中式设备－IRF模式）

1. 配置需求

- IRF 由两个成员设备组成：主设备的成员编号为 1，从设备的成员编号为 2。
- 现要求对设备启动软件包进行升级，使设备使用新的启动软件包运行。

2. 组网图

图1-5 通过重启方式升级启动软件包配置举例组网图



3. 配置步骤

说明

为了保险起见，在配置主用下次启动软件包/IPE 文件时，建议将主用下次启动软件包/IPE 文件进行备份，再将备份文件设置为备用下次启动软件包/IPE 文件。如果 Flash 上存储空间有限，可以不备份。

配置 IP 地址以及路由，确保 IRF 和 TFTP server 之间路由可达。配置步骤略。

查看设备当前使用的启动软件包的版本。

```
<Sysname> display version
```

复制设备当前使用的启动软件包。

```
<Sysname> copy boot.bin boot_backup.bin
<Sysname> copy system.bin system_backup.bin
```

指定主设备和从设备下次启动时使用的备用软件包为 boot_backup.bin/system_backup.bin。

```
<Sysname> boot-loader file boot flash:/boot_backup.bin system flash:/system_backup.bin slot 1 backup
<Sysname> boot-loader file boot flash:/boot_backup.bin system flash:/system_backup.bin slot 2 backup
```

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

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

指定主设备和从设备下次启动时使用 startup-a2105.ipe 作为主用 IPE 文件。

```
<Sysname> boot-loader file flash:/startup-a2105.ipe slot 1 main
<Sysname> boot-loader file flash:/startup-a2105.ipe slot 2 main
```

查看主用、备用下次启动 IPE 文件是否配置成功。

```
<Sysname> display boot-loader
```

重启所有成员设备，以便运行新的启动软件包完成升级。

```
<Sysname> reboot
```

4. 验证配置

设备重启后，查看 IRF 使用的启动软件包的版本。

```
<Sysname> display version
```

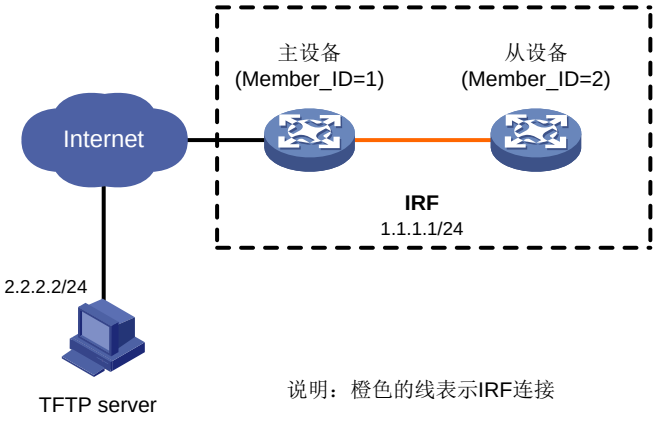
1.11 通过重启方式升级启动软件包配置举例（分布式设备－IRF模式）

1. 配置需求

- IRF 由两个成员设备组成：主设备的成员编号为 1，从设备的成员编号为 2。
- 主设备上有两块主控板：主用主控板所在槽位号为 0，备用主控板所在槽位号为 1。
- 从设备上有两块主控板：主用主控板所在槽位号为 0，备用主控板所在槽位号为 1。
- 现要求对 IRF 启动软件包进行升级，使所有成员设备使用新的启动软件包运行。

2. 组网图

图1-6 通过重启方式升级启动软件包配置举例组网图



3. 配置步骤

说明

为了保险起见，在配置主用下次启动软件包/IPE 文件时，建议将主用下次启动软件包/IPE 文件进行备份，再将备份文件设置为备用下次启动软件包/IPE 文件。如果 Flash 上存储空间有限，可以不备份。

配置 IP 地址以及路由，确保 Device 和 TFTP server 之间路由可达。配置步骤略。

查看 IRF 当前使用的启动软件包的版本。

```
<Sysname> display version
```

复制设备当前使用的启动软件包。

```
<Sysname> copy boot.bin boot_backup.bin
<Sysname> copy system.bin system_backup.bin
```

指定所有主控板下次启动时使用的备用软件包为 boot_backup.bin/system_backup.bin。

```
<Sysname> boot-loader file boot flash:/boot_backup.bin system flash:/system_backup.bin
chassis 1 slot 0 backup
<Sysname> boot-loader file boot flash:/boot_backup.bin system flash:/system_backup.bin
chassis 1 slot 1 backup
<Sysname> boot-loader file boot flash:/boot_backup.bin system flash:/system_backup.bin
chassis 2 slot 0 backup
<Sysname> boot-loader file boot flash:/boot_backup.bin system flash:/system_backup.bin
chassis 2 slot 1 backup
```

将待升级的 IPE 文件 startup-a2105.ipe 从 TFTP server 下载到全局主用主控板 Flash 的根目录下。

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

指定所有主控板下次启动时使用 startup-a2105.ipe 作为主用 IPE 文件。

```
<Sysname> boot-loader file flash:/startup-a2105.ipe chassis 1 slot 0 main
<Sysname> boot-loader file flash:/startup-a2105.ipe chassis 1 slot 1 main
<Sysname> boot-loader file flash:/startup-a2105.ipe chassis 2 slot 0 main
<Sysname> boot-loader file flash:/startup-a2105.ipe chassis 2 slot 1 main
```

查看主用、备用下次启动 IPE 文件是否配置成功。

```
<Sysname> display boot-loader
```

重启所有成员设备，以便运行新的启动软件包完成升级。

```
<Sysname> reboot
```

4. 验证配置

设备重启后，查看 IRF 使用的启动软件包的版本。

```
<Sysname> display version
```

1.12 通过install命令升级配置举例（集中式设备—独立运行模式）

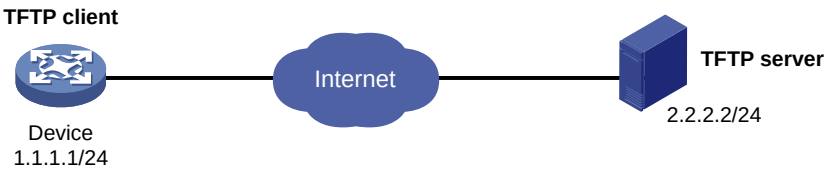
1.12.1 HTTP软件包升级配置举例

1. 配置需求

将 HTTP 特性从 R0201 版本升级到兼容版本 R0202。

2. 组网图

图1-7 HTTP 软件包升级组网图



3. 配置步骤

从 TFTP server 下载包含新版本 HTTP 软件包的 IPE 文件。

```
<Sysname> tftp 2.2.2.2 get http-r0202.ipe
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   256  100  256     0     0    764      0 --:--:-- --:--:-- --:--:--   810
Writing file...Done.
```

解压缩 IPE 文件。

```
<Sysname> install add flash:/http-r0202.ipe flash:
Verifying the file flash:/http-r0202.ipe on the device...Done.
Decompressing file http-r0202.bin to flash:/http-r0202.bin.....................Done.
```

查看升级前激活的软件包。

```
<Sysname> display install active
Active packages on the device:
  flash:/boot-r0201.bin
  flash:/system-r0201.bin
  flash:/http-r0201.bin
```

显示 HTTP 软件包的升级效果。

```
<Sysname> install activate feature flash:/http-r0202.bin test
Verifying the file flash:/http-r0202.bin on the device...Done.
Identifying the upgrade methods...Done.
Upgrade summary according to following table:
```

```
flash:/http-r0202.bin
  Running Version             New Version
  Alpha 0201                  Alpha 0202

Upgrade Way: Service Upgrade

Influenced service according to following table on the device:
  flash:/http-r0202.bin
         HTTP      CFA
```

以上显示信息表明，http-r0202.bin 的升级方式是增量升级，升级过程中 HTTP 和 CFA 模块会重启。

激活新版本的 HTTP 软件包，从而对 HTTP 特性进行升级。

```
<Sysname> install activate feature flash:/http-r0202.bin
Verifying the file flash:/http-r0202.bin on the device...Done.
Identifying the upgrade methods...Done.
Upgrade summary according to following table:

flash:/http-r0202.bin
  Running Version             New Version
  Alpha 0201                  Alpha 0202

Upgrade Way: Service Upgrade
Upgrading software images to compatible versions. Continue? [Y/N]: y
This operation might take several minutes, please wait.....................Done.
```

查看升级后激活的软件包。

```
<Sysname> display install active
Active packages on the device:
  flash:/boot-r0201.bin
  flash:/system-r0201.bin
  flash:/http-r0202.bin
```

确认软件包更改。

```
<Sysname> install commit
This operation will take several minutes, please wait.........................Done.
```

1.12.2 将HTTP软件包回滚到升级前的版本

1. 配置需求

将 HTTP 软件包从 R0202 版本回滚到 R0201 版本。

2. 配置步骤

查看回滚前激活的软件包。

```
<Sysname> display install active
Active packages on the device:
  flash:/boot-r0201.bin
  flash:/system-r0201.bin
  flash:/http-r0202.bin
```

查看回滚点信息。

```
<Sysname> display install rollback
  Install rollback information 1 on the device:
    Updating from flash:/http-r0201.bin
             to flash:/http-r0202.bin.
```

将 HTTP 软件包回滚到 R0201 版本。

```
<Sysname> install rollback to original
```

查看回滚后激活的软件包。

```
<Sysname> display install active
Active packages on the device:
  flash:/boot-r0201.bin
  flash:/system-r0201.bin
  flash:/http-r0201.bin
```

确认软件包更改。

```
<Sysname> install commit
This operation will take several minutes, please wait.........................Done.
```

1.13 通过install命令升级配置举例（分布式设备—独立运行模式）

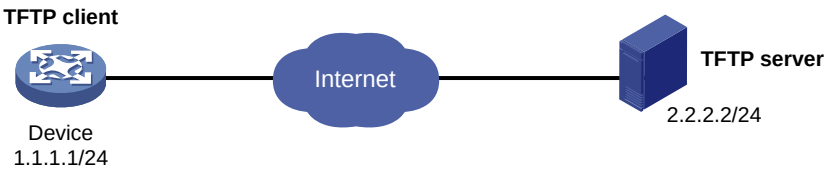
1.13.1 HTTP软件包升级配置举例

1. 配置需求

- Device 上配备了两块主控板：主用主控板所在的槽位号为 0，备用主控板所在的槽位号为 1。
- 将 HTTP 特性从 R0201 版本升级到兼容版本 R0202。

2. 组网图

图1-8 HTTP 软件包升级组网图



3. 配置步骤

从 TFTP server 下载包含新版本 HTTP 软件包的 IPE 文件。

```
<Sysname> tftp 2.2.2.2 get http-r0202.ipe
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   256  100  256     0     0    764      0 --:--:-- --:--:-- --:--:--   810
Writing file...Done.
```

解压缩 IPE 文件。

```
<Sysname> install add flash:/http-r0202.ipe flash:/
Verifying the file flash:/http-r0202.ipe on slot 0...Done.
Decompressing file http-r0202.bin to flash:/http-r0202.bin.....................Done.
```

查看升级前激活的软件包。

```
<Sysname> display install active
Active packages on slot 0:
  flash:/boot-r0201.bin
  flash:/system-r0201.bin
  flash:/http-r0201.bin
Active packages on slot 1:
  flash:/boot-r0201.bin
  flash:/system-r0201.bin
  flash:/http-r0201.bin
```

显示 HTTP 软件包的升级效果。

```
<Sysname> install activate feature flash:/http-r0202.bin slot 1 test
Copying file flash:/http-r0202.bin to slot1#flash:/http-r0202.bin......Done.
Verifying the file flash:/http-r0202.bin on slot 1...Done.
Identifying the upgrade methods...Done.
Upgrade summary according to following table:

flash:/http-r0202.bin
  Running Version             New Version
  Alpha 0201                  Alpha 0202

  Slot                        Upgrade Way
  1                           Service Upgrade

Influenced service according to following table on slot 1:
  flash:/http-r0202.bin
         HTTP      CFA
<Sysname> install activate feature flash:/http-r0202.bin slot 0 test
Verifying the file flash:/http-r0202.bin on slot 0...Done.
Identifying the upgrade methods...Done.
Upgrade summary according to following table:

flash:/http-r0202.bin
  Running Version             New Version
  Alpha 0201                  Alpha 0202

  Slot                        Upgrade Way
  0                           Service Upgrade
  1                           Service Upgrade

Influenced service according to following table on slot 0:
  flash:/http-r0202.bin
         HTTP      CFA
```

以上显示信息表明，http-r0202.bin 的升级方式是增量升级，升级过程中 HTTP 和 CFA 模块会重启。

激活新版本的 HTTP 软件包，从而对 HTTP 特性进行升级。

```
<Sysname> install activate feature flash:/http-r0202.bin slot 1
flash:/http-r0202.bin already exists on slot 1.
Overwrite it?[Y/N]:y
Copying file flash:/http-r0202.bin to slot1#flash:/http-r0202.bin......Done.
```

```
Verifying the file flash:/http-r0202.bin on slot 1...Done.
Identifying the upgrade methods...Done.
Upgrade summary according to following table:

flash:/http-r0202.bin
  Running Version             New Version
  Alpha 0201                  Alpha 0202

  Slot                        Upgrade Way
  1                           Service Upgrade
Upgrading software images to compatible versions. Continue? [Y/N]: y
This operation might take several minutes, please wait.....................Done.
<Sysname> install activate feature flash:/http-r0202.bin slot 0
Verifying the file flash:/http-r0202.bin on slot 0...Done.
Identifying the upgrade methods...Done.
Upgrade summary according to following table:

flash:/http-r0202.bin
  Running Version             New Version
  Alpha 0201                  Alpha 0202

  Slot                        Upgrade Way
  0                           Service Upgrade
  1                           Service Upgrade
Upgrading software images to compatible versions. Continue? [Y/N]: y
This operation might take several minutes, please wait.....................Done.
# 查看升级后激活的软件包。
<Sysname> display install active
Active packages on slot 0:
  flash:/boot-r0201.bin
  flash:/system-r0201.bin
  flash:/http-r0202.bin
Active packages on slot 1:
  flash:/boot-r0201.bin
  flash:/system-r0201.bin
  flash:/http-r0202.bin
# 确认软件包更改。
<Sysname> install commit
This operation will take several minutes, please wait.........................Done.
```

1.13.2 将HTTP软件包回滚到升级前的版本

1. 配置需求

- Device 上配备了两块主控板：主用主控板所在的槽位号为 0，备用主控板所在的槽位号为 1。
- HTTP 软件包从 R0202 版本回滚到 R0201 版本。

2. 配置步骤

查看回滚前激活的软件包。

```
<Sysname> display install active
Active packages on slot 0:
  flash:/boot-r0201.bin
  flash:/system-r0201.bin
  flash:/http-r0202.bin
Active packages on slot 1:
  flash:/boot-r0201.bin
  flash:/system-r0201.bin
  flash:/http-r0202.bin
```

查看回滚点信息。

```
<Sysname> display install rollback
  Install rollback information 1 on slot 0:
    Updating from flash:/http-r0201.bin
             to flash:/http-r0202.bin.
  Install rollback information 2 on slot 1:
    Updating from flash:/http-r0201.bin
             to flash:/http-r0202.bin.
```

将 HTTP 软件包回滚到 R0201 版本。

```
<Sysname> install rollback to original
```

查看回滚后激活的软件包。

```
<Sysname> display install active
Active packages on slot 0:
  flash:/boot-r0201.bin
  flash:/system-r0201.bin
  flash:/http-r0201.bin
Active packages on slot 1:
  flash:/boot-r0201.bin
  flash:/system-r0201.bin
  flash:/http-r0201.bin
```

确认软件包更改。

```
<Sysname> install commit
This operation will take several minutes, please wait.........................Done.
```

1.14 通过install命令升级配置举例（集中式设备—IRF模式）

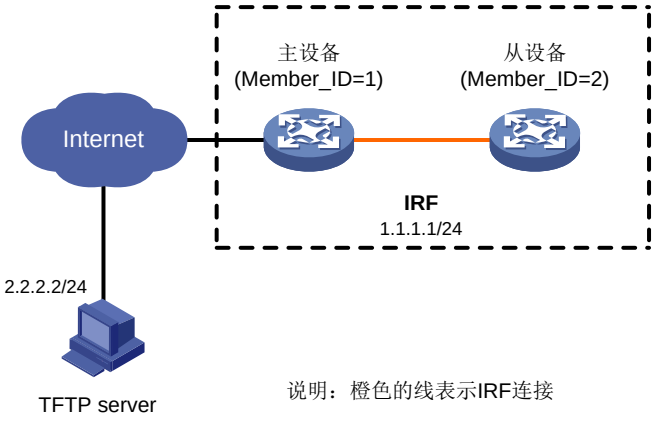
1.14.1 HTTP软件包升级配置举例

1. 配置需求

- IRF 由两个成员设备组成：主设备的成员编号为 1，从设备的成员编号为 2。
- 将 HTTP 特性从 R0201 版本升级到兼容版本 R0202。

2. 组网图

图1-9 HTTP 软件包升级组网图



3. 配置步骤

从 TFTP server 下载包含新版本 HTTP 软件包的 IPE 文件。

```
<Sysname> tftp 2.2.2.2 get http-r0202.ipe
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   256  100  256     0     0    764      0 --:--:-- --:--:-- --:--:--   810
Writing file...Done.
```

解压缩 IPE 文件。

```
<Sysname> install add flash:/http-r0202.ipe flash:
Verifying the file flash:/http-r0202.ipe on slot 1...Done.
Decompressing file http-r0202.bin to flash:/http-r0202.bin.....................Done.
```

查看升级前激活的软件包。

```
<Sysname> display install active
Active packages on slot 1:
  flash:/boot-r0201.bin
  flash:/system-r0201.bin
  flash:/http-r0201.bin
Active packages on slot 2:
  flash:/boot-r0201.bin
  flash:/system-r0201.bin
  flash:/http-r0201.bin
```

显示 HTTP 软件包的升级效果。

```
<Sysname> install activate feature flash:/http-r0202.bin slot 2 test
Copying file flash:/http-r0202.bin to slot2#flash:/http-r0202.bin......Done.
Verifying the file flash:/http-r0202.bin on slot 2...Done.
Identifying the upgrade methods...Done.
Upgrade summary according to following table:

flash:/http-r0202.bin
  Running Version             New Version
  Alpha 0201                  Alpha 0202
```

```
  Slot                          Upgrade Way
  2                             Service Upgrade

Influenced service according to following table on slot 2:
  flash:/http-r0202.bin
         HTTP      CFA
<Sysname> install activate feature flash:/http-r0202.bin slot 1 test
Verifying the file flash:/http-r0202.bin on slot 1...Done.
Identifying the upgrade methods...Done.
Upgrade summary according to following table:

flash:/http-r0202.bin
  Running Version             New Version
  Alpha 0201                  Alpha 0202

  Slot                          Upgrade Way
  1                             Service Upgrade

Influenced service according to following table on slot 1:
  flash:/http-r0202.bin
         HTTP      CFA
```

以上显示信息表明，http-r0202.bin 的升级方式是增量升级，升级过程中 HTTP 和 CFA 模块会重启。

激活新版本的 HTTP 软件包，从而对 HTTP 特性进行升级。

```
<Sysname> install activate feature flash:/http-r0202.bin slot 2
Verifying the file flash:/http-r0202.bin on slot 1...Done.
flash:/http-r0202.bin already exists on slot 2.
Overwrite it?[Y/N]:y
Copying file flash:/http-r0202.bin to slot2#flash:/http-r0202.bin......Done.
Verifying the file flash:/http-r0202.bin on slot 2...Done.
Identifying the upgrade methods...Done.
Upgrade summary according to following table:

flash:/http-r0202.bin
  Running Version             New Version
  Alpha 0201                  Alpha 0202

  Slot                          Upgrade Way
  2                             Service Upgrade
Upgrading software images to compatible versions. Continue? [Y/N]: y
This operation might take several minutes, please wait.....................Done.
<Sysname> install activate feature flash:/http-r0202.bin slot 1
Verifying the file flash:/http-r0202.bin on slot 1...Done.
Identifying the upgrade methods...Done.
Upgrade summary according to following table:

flash:/http-r0202.bin
  Running Version             New Version
```

```
  Alpha 0201                  Alpha 0202

  Slot                        Upgrade Way
  1                           Service Upgrade
Upgrading software images to compatible versions. Continue? [Y/N]: y
This operation might take several minutes, please wait.....................Done.
```

查看升级后激活的软件包。

```
<Sysname> display install active
Active packages on slot 1:
  flash:/boot-r0201.bin
  flash:/system-r0201.bin
  flash:/http-r0202.bin
Active packages on slot 2:
  flash:/boot-r0201.bin
  flash:/system-r0201.bin
  flash:/http-r0202.bin
```

确认软件包更改。

```
<Sysname> install commit
```

1.14.2 将HTTP软件包回滚到升级前的版本

1. 配置需求

- IRF 由两个成员设备组成：主设备的成员编号为 1，从设备的成员编号为 2。
- HTTP 软件包从 R0202 版本回滚到 R0201 版本。

2. 配置步骤

查看回滚前激活的软件包。

```
<Sysname> display install active
Active packages on slot 1:
  flash:/boot-r0201.bin
  flash:/system-r0201.bin
  flash:/http-r0202.bin
Active packages on slot2:
  flash:/boot-r0201.bin
  flash:/system-r0201.bin
  flash:/http-r0202.bin
```

查看回滚点信息。

```
<Sysname> display install rollback
  Install rollback information 1 on slot 1:
    Updating from flash:/http-r0201.bin
             to flash:/http-r0202.bin.
  Install rollback information 2 on slot 2:
    Updating from flash:/http-r0201.bin
             to flash:/http-r0202.bin.
```

将 HTTP 软件包回滚到 R0201 版本。

```
<Sysname> install rollback to original
```

查看回滚后激活的软件包。

```
<Sysname> display install active
Active packages on slot 1:
  flash:/boot-r0201.bin
  flash:/system-r0201.bin
  flash:/http-r0201.bin
Active packages on slot 2:
  flash:/boot-r0201.bin
  flash:/system-r0201.bin
  flash:/http-r0201.bin
```

确认软件包更改。

```
<Sysname> install commit
This operation will take several minutes, please wait.........................Done.
```

1.15 通过install命令升级配置举例（分布式设备－IRF模式）

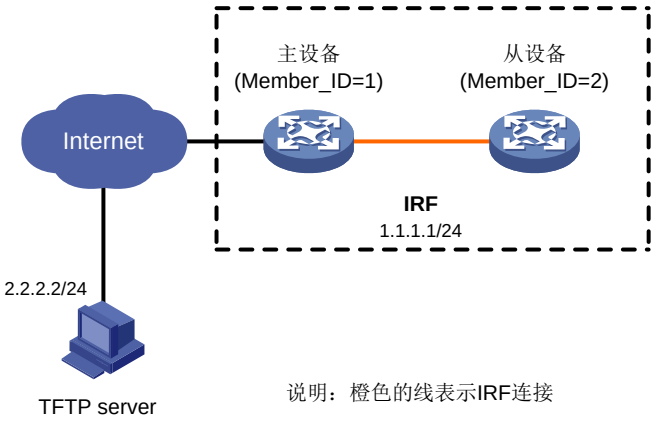
1.15.1 HTTP软件包升级配置举例

1. 配置需求

- IRF 由主设备和从设备组成。主设备的成员编号为 1，主用主控板所在的槽位号为 0，备用主控板所在的槽位号为 1；从设备的成员编号为 2，主用主控板所在的槽位号为 0，备用主控板所在的槽位号为 1。
- HTTP 软件包从 R0201 版本升级到兼容版本 R0202。

2. 组网图

图1-10 软件包升级组网图



3. 配置步骤

从 TFTP Server 下载包含新版本 HTTP 软件包的 IPE 文件。

```
<Sysname> tftp 2.2.2.2 get http-r0202.ipe
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   256  100  256     0     0    764      0 --:--:-- --:--:-- --:--:--   810
Writing file...Done.
```

解压缩软件包。

```
<Sysname> install add flash:/http-r0202.ipe flash:
Verifying the file flash:/http-r0202.ipe on slot 1...Done.
Decompressing file http-r0202.bin to flash:/http-r0202.bin.....................Done.
```

查看升级前激活的软件包。

```
<Sysname> display install active
Active packages on chassis 1 slot 0:
  flash:/boot-r0201.bin
  flash:/system-r0201.bin
  flash:/http-r0201.bin
Active packages on chassis 1 slot 1:
  flash:/boot-r0201.bin
  flash:/system-r0201.bin
  flash:/http-r0201.bin
Active packages on chassis 2 slot 0:
  flash:/boot-r0201.bin
  flash:/system-r0201.bin
  flash:/http-r0201.bin
Active packages on chassis 2 slot 1:
  flash:/boot-r0201.bin
  flash:/system-r0201.bin
  flash:/http-r0201.bin
```

显示 HTTP 软件包的升级效果。

```
<Sysname> install activate feature flash:/http-r0202.bin chassis 2 slot 1 test
Copying file flash:/http-r0202.bin to chassis2#slot1#flash:/http-r0202.bin......Done.
Verifying the file flash:/http-r0202.bin on chassis 2 slot 1...Done.
Identifying the upgrade methods...Done.
Upgrade summary according to following table:

flash:/http-r0202.bin
  Running Version             New Version
  Alpha 0201                  Alpha 0202

  Chassis   Slot              Upgrade Way
  2         0                 Service Upgrade
  2         1                 Service Upgrade

Influenced service according to following table on chassis 2 slot 0:
  flash:/http-r0202.bin
         HTTP      CFA
Influenced service according to following table on chassis 2 slot 1:
  flash:/http-r0202.bin
         HTTP      CFA

<Sysname> install activate feature flash:/http-r0202.bin chassis 2 slot 0 test
Copying file flash:/http-r0202.bin to chassis2#slot0#flash:/http-r0202.bin......Done.
Verifying the file flash:/http-r0202.bin on chassis 2 slot 0...Done.
Identifying the upgrade methods...Done.
Upgrade summary according to following table:
```

```
flash:/http-r0202.bin
  Running Version             New Version
  Alpha 0201                  Alpha 0202

  Chassis   Slot              Upgrade Way
  2         0                 Service Upgrade

Influenced service according to following table on chassis 2 slot 0:
  flash:/http-r0202.bin
         HTTP      CFA
<Sysname> install activate feature flash:/http-r0202.bin chassis 1 slot 1 test
Copying file flash:/http-r0202.bin to chassis1#slot1#flash:/http-r0202.bin......Done.
Verifying the file flash:/http-r0202.bin on chassis 1 slot 1...Done.
Identifying the upgrade methods...Done.
Upgrade summary according to following table:

flash:/http-r0202.bin
  Running Version             New Version
  Alpha 0201                  Alpha 0202

  Chassis   Slot              Upgrade Way
  1         0                 Service Upgrade
  1         1                 Service Upgrade
Influenced service according to following table on chassis 1 slot 0:
  flash:/http-r0202.bin
         HTTP      CFA
Influenced service according to following table on chassis 1 slot 1:
  flash:/http-r0202.bin
         HTTP      CFA
<Sysname> install activate feature flash:/http-r0202.bin chassis 1 slot 0 test
Verifying the file flash:/http-r0202.bin on chassis 1 slot 0...Done.
Identifying the upgrade methods...Done.
Upgrade summary according to following table:

flash:/http-r0202.bin
  Running Version             New Version
  Alpha 0201                  Alpha 0202

  Chassis   Slot              Upgrade Way
  1         0                 Service Upgrade

Influenced service according to following table on chassis 1 slot 0:
  flash:/http-r0202.bin
         HTTP      CFA
```

以上显示信息表明，http-r0202.bin 的升级方式是增量升级，升级过程中 HTTP 和 CFA 模块会重启。

激活新版本的 HTTP 软件包，从而对 HTTP 特性进行升级。

```
<Sysname> install activate feature flash:/http-r0202.bin chassis 2 slot 1
```

```
Verifying the file flash:/http-r0202.bin on chassis 2 slot 1...Done.
flash:/http-r0202.bin already exists on chassis 2 slot 1.
Overwrite it?[Y/N]:y
Copying file flash:/http-r0202.bin to chassis2#slot1#flash:/http-r0202.bin......Done.
Verifying the file flash:/http-r0202.bin on chassis 2 slot 1...Done.
Identifying the upgrade methods...Done.
Upgrade summary according to following table:

flash:/http-r0202.bin
  Running Version             New Version
  Alpha 0201                  Alpha 0202

  Chassis   Slot              Upgrade Way
  2         0                 Service Upgrade
  2         1                 Service Upgrade
Upgrading software images to compatible versions. Continue? [Y/N]: y
This operation might take several minutes, please wait.....................Done.
<Sysname> install activate feature flash:/http-r0202.bin chassis 2 slot 0
flash:/http-r0202.bin already exists on chassis 2 slot 0.
Overwrite it?[Y/N]:y
Copying file flash:/http-r0202.bin to chassis2#slot0#flash:/http-r0202.bin......Done.
Verifying the file flash:/http-r0202.bin on chassis 2 slot 0...Done.
Identifying the upgrade methods...Done.
Upgrade summary according to following table:

flash:/http-r0202.bin
  Running Version             New Version
  Alpha 0201                  Alpha 0202

  Chassis   Slot              Upgrade Way
  2         0                 Service Upgrade
Upgrading software images to compatible versions. Continue? [Y/N]: y
This operation might take several minutes, please wait.....................Done.
<Sysname> install activate feature flash:/http-r0202.bin chassis 1 slot 1
flash:/http-r0202.bin already exists on chassis 1 slot 1.
Overwrite it?[Y/N]:y
Copying file flash:/http-r0202.bin to chassis1#slot1#flash:/http-r0202.bin......Done.
Verifying the file flash:/http-r0202.bin on chassis 1 slot 1...Done.
Identifying the upgrade methods...Done.
Upgrade summary according to following table:

flash:/http-r0202.bin
  Running Version             New Version
  Alpha 0201                  Alpha 0202

  Chassis   Slot              Upgrade Way
  1         0                 Service Upgrade
  1         1                 Service Upgrade
```

```
Upgrading software images to compatible versions. Continue? [Y/N]: y
This operation might take several minutes, please wait.....................Done.
<Sysname> install activate feature flash:/http-r0202.bin chassis 1 slot 0
Verifying the file flash:/http-r0202.bin on chassis 1 slot 0...Done.
Identifying the upgrade methods...Done.
Upgrade summary according to following table:

flash:/http-r0202.bin
  Running Version             New Version
  Alpha 0201                  Alpha 0202

  Chassis   Slot              Upgrade Way
  1         0                 Service Upgrade
Upgrading software images to compatible versions. Continue? [Y/N]: y
This operation might take several minutes, please wait.....................Done.
```

查看已激活的软件包。

```
<Sysname> display install active
Active packages on chassis 1 slot 0:
  flash:/boot-r0201.bin
  flash:/system-r0201.bin
  flash:/http-r0202.bin
Active packages on chassis 1 slot 1:
  flash:/boot-r0201.bin
  flash:/system-r0201.bin
  flash:/http-r0202.bin
Active packages on chassis 2 slot 0:
  flash:/boot-r0201.bin
  flash:/system-r0201.bin
  flash:/http-r0202.bin
Active packages on chassis 2 slot 1:
  flash:/boot-r0201.bin
  flash:/system-r0201.bin
  flash:/http-r0202.bin
```

确认软件包更改。

```
<Sysname> install commit
This operation will take several minutes, please wait.........................Done.
```

1.15.2 HTTP软件包回滚到升级前的版本

1. 配置需求

- IRF 由主设备和从设备组成。主设备的成员编号为 1，主用主控板所在的槽位号为 0，备用主控板所在的槽位号为 1；从设备的成员编号为 2，主用主控板所在的槽位号为 0，备用主控板所在的槽位号为 1。
- HTTP 软件包从 R0202 版本回滚到 R0201 版本。

2. 配置步骤

查看已激活的软件包。

```
<Sysname> display install active
Active packages on chassis 1 slot 0:
  flash:/boot-r0201.bin
  flash:/system-r0201.bin
  flash:/http-r0202.bin
Active packages on chassis 1 slot 1:
  flash:/boot-r0201.bin
  flash:/system-r0201.bin
  flash:/http-r0202.bin
Active packages on chassis 2 slot 0:
  flash:/boot-r0201.bin
  flash:/system-r0201.bin
  flash:/http-r0202.bin
Active packages on chassis 2 slot 1:
  flash:/boot-r0201.bin
  flash:/system-r0201.bin
  flash:/http-r0202.bin
```

查看回滚点信息。

```
<Sysname> display install rollback
  Install rollback information 1 on chassis 1 slot 0:
    Updating from flash:/http-r0201.bin
             to flash:/http-r0202.bin.
  Install rollback information 2 on chassis 1 slot 1:
    Updating from flash:/http-r0201.bin
             to flash:/http-r0202.bin.
  Install rollback information 3 on chassis 2 slot 0:
    Updating from flash:/http-r0201.bin
             to flash:/http-r0202.bin.
  Install rollback information 4 on chassis 2 slot 1:
    Updating from flash:/http-r0201.bin
             to flash:/http-r0202.bin.
```

将 HTTP 软件包回滚到 R0201 版本。

```
<Sysname> install rollback to original
```

查看已激活的软件包。

```
<Sysname> display install active
Active packages on chassis 1 slot 0:
  flash:/boot-r0201.bin
  flash:/system-r0201.bin
  flash:/http-r0201.bin
Active packages on chassis 1 slot 1:
  flash:/boot-r0201.bin
  flash:/system-r0201.bin
  flash:/http-r0201.bin
Active packages on chassis 2 slot 0:
  flash:/boot-r0201.bin
  flash:/system-r0201.bin
  flash:/http-r0201.bin
Active packages on chassis 2 slot 1:
```

```
  flash:/boot-r0201.bin
  flash:/system-r0201.bin
  flash:/http-r0201.bin
```

确认软件包更改。

```
<Sysname> install commit
This operation will take several minutes, please wait.........................Done.
```

目 录

1 应急Shell

设备各款型使用的命令行形式有所不同，详细差异信息如下：

命令行形式	款型
集中式	• MSR810/810-W/810-W-DB/810-LM/810-W-LM/810-10-PoE/810-LM-HK/810-W-LM-HK • MSR810-LMS/810-LUS • MSR2600-6-X1/2600-10-X1/2630 • MSR3600-28/3600-51/3600-28-SI/3600-51-SI • MSR3610-X1/3610-X1-DP/3610-X1-DC/3610-X1-DP-DC • MSR 3610/3620/3620-DP/3640/3660 • MSR810-W-WiNet/810-LM-WiNet/830-4LM-WiNet • MSR830-5BEI-WiNet/830-6EI-WiNet/830-10BEI-WiNet • MSR830-6BHI-WiNet/830-10BHI-WiNet • MSR2600-10-X1-WiNet/2630-WiNet • MSR3600-28-WiNet/3610-X1-WiNet • MSR3610-WiNet/3620-10-WiNet/3620-DP-WiNet/3620-WiNet/3660-WiNet • MSR810-LM-GL/810-W-LM-GL • MSR830-6EI-GL/830-10EI-GL/830-6HI-GL/830-10HI-GL • MSR2600-6-X1-GL/3600-28-SI-GL
分布式	MSR5620/5660/5680

设备各款型对于本手册所描述的特性的支持情况有所不同，详细差异信息如下：

型号	特性	描述
MSR810/810-W/810-W-DB/810-LM/810-W-LM/810-10-PoE/810-LM-HK/810-W-LM-HK/810-LMS/810-LUS	应急Shell	仅MSR810-10-PoE/810-LMS/810-LUS不支持
MSR2600-6-X1/2600-10-X1		支持
MSR 2630		支持
MSR3600-28/3600-51		支持
MSR3600-28-SI/3600-51-SI		不支持
MSR3610-X1/3610-X1-DP/3610-X1-DC/3610-X1-DP-DC		不支持
MSR 3610/3620/3620-DP/3640/3660		仅MSR 3620-DP支持
MSR5620/5660/5680		支持

型号	特性	描述
MSR810-W-WiNet/810-LM-WiNet	应急Shell	支持

型号	特性	描述
MSR830-4LM-WiNet		不支持
MSR830-5BEI-WiNet/830-6EI-WiNet/830-10BEI-WiNet		不支持
MSR830-6BHI-WiNet/830-10BHI-WiNet		不支持
MSR2600-10-X1-WiNet		支持
MSR2630-WiNet		支持
MSR3600-28-WiNet		支持
MSR3610-X1-WiNet		不支持
MSR3610-WiNet/3620-10-WiNet/3620-DP-WiNet/3620-WiNet/3660-WiNet		仅MSR3620-DP-WiNet不支持

型号	特性	描述
MSR810-LM-GL	应急shell	支持
MSR810-W-LM-GL		支持
MSR830-6EI-GL		不支持
MSR830-10EI-GL		不支持
MSR830-6HI-GL		不支持
MSR830-10HI-GL		不支持
MSR2600-6-X1-GL		支持
MSR3600-28-SI-GL		不支持

1.1 应急Shell简介

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

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

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

1.2 配置限制和指导

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

本文描述的操作均是在故障成员设备上执行，且只能对本设备进行操作。比如，某成员设备上 System 包不存在或者异常，进入应急 Shell 环境了，请使用该成员设备的 Console 口登录，执行本文中描述的操作给该成员设备加载 System 包。（集中式设备-IRF 模式）

1.3 文件系统操作

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

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

表1-1 文件系统操作命令

操作	命令	说明
显示目录或文件信息	**dir** [**/all**] [*file-url*]	该命令在用户视图下执行
在指定路径下创建目录	**mkdir** *directory*	如果创建的文件夹与指定路径下的其它文件或目录重名，则创建操作失败 在使用该命令创建目录之前，指定的路径必须已经存在。比如：创建文件夹flash:/test/mytest时，test文件夹必须已经存在，否则mytest文件夹创建失败 该命令在用户视图下执行
显示当前工作路径	**pwd**	该命令在用户视图下执行
复制文件	**copy** *fileurl-source fileurl-dest*	该命令在用户视图下执行
移动文件	**move** *fileurl-source fileurl-dest*	目标目录必须空间足够，否则移动操作失败 该命令在用户视图下执行
显示指定文件的内容	**more** *file-url*	该命令在用户视图下执行
彻底删除指定文件	**delete** *file-url*	该命令在用户视图下执行
删除已有目录	**rmdir** *directory*	被删除的目录必须为空目录，即删除目录前，必须先删除该目录下的所有文件及子目录 该命令在用户视图下执行
格式化存储介质	**format** *device*	该命令在用户视图下执行

1.4 获取System包

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

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

1.4.1 配置管理以太网接口

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

表1-2 配置管理以太网接口（IPv4 网络）

操作	命令	说明
进入系统视图	**system-view**	-
进入管理以太网接口视图	**interface m-eth0**	-
配置接口的IPv4地址	**ip address** *ip-address* { *mask-length* | *mask* }	缺省情况下，未配置管理以太网接口的IPv4地址
打开管理以太网接口	**undo shutdown**	缺省情况下，管理以太网接口处于打开状态
从当前视图退回到上一级视图	**quit**	-

表1-3 配置管理以太网接口（IPv6 网络）

操作	命令	说明
进入系统视图	**system-view**	-
进入管理以太网接口视图	**interface m-eth0**	-
配置接口的IPv6地址	**ipv6 address** *ipv6-address prefix-length*	缺省情况下，未配置管理以太网接口的IPv6地址
打开管理以太网接口	**undo shutdown**	缺省情况下，管理以太网接口处于打开状态
从当前视图退回到上一级视图	**quit**	-

1.4.2 Ping功能

网络参数配置完成后，可使用 **ping** 命令测试网络是否可达。

表1-4 检查指定目的端是否可达（IPv4 网络）

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

表1-5 检查指定目的端是否可达（IPv6 网络）

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

1.4.3 访问远程服务器

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

表1-6 访问远程服务器（IPv4 网络）

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

表1-7 访问远程服务器（IPv6 网络）

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

1.5 加载System包

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

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

表1-8 加载 System 包

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

1.6 重启

表1-9 重启

操作	命令	说明
重启设备（集中式设备-独立运行模式） 重启当前登录的主控板（分布式设备－独立运行模式/分布式设备－IRF模式） 重启当前登录的成员设备（集中式设备-IRF模式）	**reboot**	该命令在用户视图下执行

1.7 应急Shell显示和维护

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

表1-10 应急 Shell 显示和维护

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

1.8 应急Shell配置举例

1. 配置需求

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

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

2. 配置组网

图1-1 应急 Shell 配置举例组网图

3. 配置步骤

查看存储介质上存在哪些文件以及存储介质上的使用情况。

```
<boot> dir
Directory of flash:
   0    drw-      5954  Apr 26 2016 21:06:29   logfile
   1    -rw-      1842  Apr 27 2016 04:37:17   boot.bin
   2    -rw-      1518  Apr 26 2016 12:05:38   startup.cfg
   3    -rw-      2045  May 04 2016 15:50:01   backcfg.cfg

524288 KB total (513248 KB free)
```

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

查看系统版本信息。

```
<boot> display version
H3C Comware Software, Version 7.1.064, Alpha 0408P05
Copyright (c) 2004-2017 New H3C Technologies Co., Ltd. All rights reserved.
H3C MSR3610 uptime is 0 weeks, 0 days, 3 hours, 50 minutes
Last reboot reason : Power on
Boot image: flash:/msr36x1-cmw710-boot-a0408p05.bin
Boot image version: 7.1.064P19, Alpha 0408P05
  Compiled Jun 20 2016 16:00:00
System image: flash:/msr36x1-cmw710-system-a0408p05.bin
System image version: 7.1.064, Alpha 0408P05
  Compiled Jun 20 2016 16:00:00
Feature image(s) list:
  flash:/msr36x1-cmw710-security-a0408p05.bin, version: 7.1.064
    Compiled Jun 20 2016 16:00:00
  flash:/msr36x1-cmw710-voice-a0408p05.bin, version: 7.1.064
    Compiled Jun 20 2016 16:00:00
  flash:/msr36x1-cmw710-data-a0408p05.bin, version: 7.1.064
```

```
    Compiled Jun 20 2016 16:00:00

Slot 1: H3C MSR3610-X1-DP uptime is 0 weeks, 0 days, 3 hours, 50 minutes
Last reboot reason : Power on
CPU ID: 0x11
2G bytes DDR3 SDRAM Memory
8M bytes Flash Memory
PCB               Version:  2.0
CPLD              Version:129.0
Basic    BootWare Version:  1.01
Extended BootWare Version:  1.01
```

给管理以太网接口配置 IP 地址和网关。

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

测试和 TFTP 服务器之间是否可达。

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

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

从 TFTP 服务器上下载文件 system.bin。

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

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

```
<boot> display install package cfa0:/system.bin
  cfa0:/system.bin
  [Package]
  Vendor: H3C
  Product: MSR36
  Service name: boot
  Platform version: 7.1.064P19
  Product version: Alpha 0408P05
  Supported board: MSR36-10,MSR36-20,MSR3620-DP,MSR36-40,MSR36-60
```

加载 System 包，引导设备进入 Comware 系统。

```
<boot> install load flash:/system.bin
flash:/system.bin
  [Package]
  Vendor: H3C
  Product: MSR36
  Service name: system
```

```
  Platform version: 7.1.064
  Product version: Alpha 0408P05
  Supported board: MSR36-10,MSR36-20,MSR3620-DP,MSR36-40,MSR36-60
```

按 ENTER 键可进入 Comware 系统，系统会提示如下信息：

```
<System>
<System>%May 23 18:29:59:777 2016 MSR36 SHELL/5/SHELL_LOGIN: TTY logged in from
 aux0.
```

目 录

1 自动配置

1.1 自动配置简介

自动配置功能是指设备在启动时自动获取并执行配置文件。网络管理员只需将配置文件保存在指定的存储介质上，设备启动时可以自动从存储介质上获取并执行配置文件，实现自动配置，从而简化了网络配置，大大降低了网络管理员的工作量，便于实现对设备的集中管理。

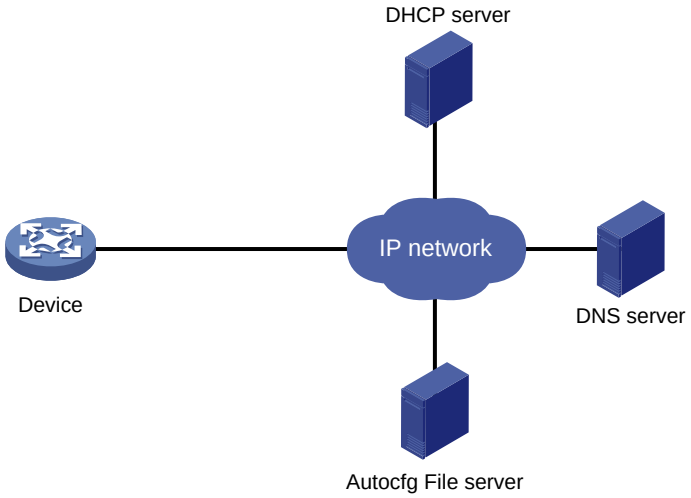
根据配置文件存储介质的不同，自动配置可以通过如下方式实现：

- 服务器自动配置：管理员将配置文件保存在文件服务器上，设备在启动时可以自动从文件服务器上获取并执行配置文件，实现自动配置功能。当网络规模较大，设备位置相对分散时，网络管理员在每一台设备上进行自动配置的工作量很大，这时管理员可以考虑使用服务器自动配置。
- U 盘自动配置：管理员将配置文件保存在 U 盘上，设备在启动时可以自动从 U 盘上获取并执行配置文件，实现自动配置功能。当网络规模较小、设备位置相对集中、缺少多余设备作为文件服务器或者仅有少量设备的配置需要更新的情况下，管理员可以考虑使用 U 盘自动配置。
- 短信自动配置：管理员将配置文件保存在 iMC 服务器上。设备启动后，接收到短信发出端（手机或短信网关）发送的短信，之后通过 3G/4G 网络连接到 iMC 服务器，并根据 iMC 服务器上配置的设备和配置文件对应关系获取相应的配置文件，实现短信自动配置功能。当设备位置相对分散且支持 3G/4G 网络的情况下，管理员可以考虑使用短信自动配置。

设备上优先使用 U 盘自动配置。短信自动配置成本相对较高，可靠性相对较差（受 3G/4G 信号影响较大），如果可以选择其他类型的自动配置方式，不建议使用短信自动配置。

1.2 服务器自动配置

图1-1 服务器自动配置典型组网图



服务器自动配置的典型组网环境如图 1-1 所示。设备需要在 DHCP 服务器、文件服务器（TFTP 服务器或 HTTP 服务器）和 DNS 服务器的配合下，实现服务器自动配置功能。

服务器自动配置的步骤如下：

1.2.1 配置文件服务器

设备可以通过 HTTP 服务器或 TFTP 服务器获取配置文件，管理员需要根据选用的方式在文件服务器上配置相应的 HTTP 服务或 TFTP 服务。

1.2.2 准备文件

设备从文件服务器上获取的文件类型可以是配置文件或者配置脚本两种形式。如果 DHCP 服务器未下发配置文件名，管理员还可以在 TFTP 服务器上创建主机名文件提供主机名和设备 IP 地址的对应关系，以保证执行自动配置的设备获取到配置文件。

1. 主机名文件

主机名文件的文件名为“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，需要上传到 TFTP 服务器。管理员需按照以下格式手工定义主机 IP 地址与主机名称的映射关系：

ip host *host-name ip-address*

例如，主机名文件中可以包括以下内容：

```
ip host host1 101.101.101.101
ip host host2 101.101.101.102
ip host client1 101.101.101.103
ip host client2 101.101.101.104
```

需要注意的是，主机名文件中保存的主机名称是管理员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。增加新的对应关系时必须换行填写。

2. 配置文件

配置文件可以实现下发配置的功能。

如果管理员选择在 TFTP 服务器上获取配置文件，根据配置文件的适用范围，TFTP 服务器上应准备以下几种类型的配置文件：

- 特定配置文件：特定配置文件只对应局域网内的某一台设备，配置特定配置文件可解决网络中设备的配置文件各不相同的需求。特定配置文件的命名规范为“配置文件名.cfg”（为了方便辨识文件名，尽量不要使用包含空格的配置文件名）。为了使设备能够获取到特定配置文件，管理员可以直接配置 DHCP 服务器下发配置文件名，也可以通过架设 DNS 服务器或者在 TFTP 服务器上保存主机名文件的方式来为设备提供主机名和设备 IP 地址的对应关系。
- 部分或全部共用配置文件：部分或全部共用配置文件对应局域网内部分或全部可以共用配置文件的设备，部分或全部共用配置文件可解决网络中部分或全部设备获取相同配置的需求。部分或全部共用配置文件可以使用任意名称来命名，但是文件扩展名必须保证是 cfg。
- 缺省配置文件（device.cfg）：缺省配置文件对应局域网内未获取到以上几种配置文件的设备，TFTP 服务器还能为未匹配以上几种配置文件的设备下发缺省配置文件，该文件包含一般设备启动的公用配置信息。

在服务器自动配置过程中，设备将先检查 TFTP 服务器上是否存在匹配的配置文件，若不存在，则选择缺省配置文件。利用此特点，管理员可以将以上三种方式结合使用，使局域网中的设备都可以获取到合适的配置文件。

如果管理员选择在 HTTP 服务器上获取配置文件，HTTP 服务器上只需要特定配置文件、部分或全部共用配置文件。HTTP 服务器不支持使用主机名文件提供主机名和 IP 地址的对应关系，也不支持配置缺省配置文件（device.cfg）。

3. 配置脚本

配置脚本可以实现自动更新版本、下发配置等功能。目前设备支持的配置脚本包括 Python 脚本和 Tcl 脚本。Python 脚本使用的文件后缀固定为 py，TCL 脚本使用的文件后缀固定为 tcl。

当管理员使用配置脚本下发配置时：

- 在文件服务器上只支持配置特定配置脚本和部分或全部共用配置脚本两种形式。
- 在文件服务器上不支持使用主机名文件提供主机名和 IP 地址的对应关系，也不支持缺省配置脚本。

关于 Python 脚本的详细介绍，请参见“基础配置指导”中的“Python”。关于 Tcl 脚本的详细介绍，请参见“基础配置指导”中的“Tcl”。

1.2.3 配置DHCP服务器

1. 简介

DHCP 服务器为执行服务器自动配置的设备分配 IP 地址，并向设备通告获取自动配置文件或配置脚本的途径。

DHCP 服务器可以根据管理员需要的配置文件类型，进行相应的配置（下发配置脚本和下发配置文件实现一致，下面以下发配置文件为例）：

- 如果管理员为每台设备分配特定配置文件，则需要在 DHCP 服务器上配置静态绑定关系，为每台设备分配特定的 IP 地址和配置文件名。由于一个地址池下只能配置一条配置文件名的命令，所以 DHCP 服务器上每一个地址池视图只能配置一个静态绑定关系。
- 如果管理员为局域网内的部分设备分配相同的配置文件，可以在 DHCP 服务器上为使用部分共用配置文件的设备配置静态绑定关系，并指定文件服务器和部分共用配置文件名。这时，这部分静态绑定关系需要在同一个 DHCP 地址池中配置。也可以使用动态分配 IP 地址的方式，管理员需要划分合适的动态地址段，为这部分设备分配 IP 地址，并指定文件服务器和部分共用配置文件名。
- 如果管理员为局域网内的所有设备分配相同的配置文件，则需要在 DHCP 服务器上配置动态分配 IP 地址的方式。为设备动态分配 IP 地址的同时，分配全部共用配置文件名。如果采用这种方式，全部共用配置文件中只能包含这些设备共有的配置，每个设备特有的配置还需要其他方式完成（如管理员使用 Telnet 登录到设备上手工配置）。

以上三种分配方式可以同时在一台 DHCP 服务器上配置。

2. 配置步骤

DHCP 服务器可以指导 DHCP 客户端从哪台文件服务器上获取配置文件或配置脚本。

如果管理员使用 HTTP 服务器下发配置文件或配置脚本，则 DHCP 服务器的地址池配置如下。

表1-1 使用 HTTP 服务器时的 DHCP 服务器的地址池配置

操作	命令	说明
进入系统视图	**system-view**	-

操作	命令	说明
开启DHCP服务	**dhcp enable**	缺省情况下，DHCP服务处于关闭状态
创建DHCP地址池，并进入DHCP地址池视图	**dhcp server ip-pool** *pool-name*	缺省情况下，设备上不存在DHCP地址池
配置DHCP地址池动态分配的主网段	**network** *network-address* [*mask-length* | **mask** *mask*]	二者选其一 缺省情况下，未配置动态分配的主网段和静态地址绑定 多次执行**static-bind ip-address**命令，可以配置多个静态地址绑定 同一地址只能绑定给一个客户端。不允许通过重复执行**static-bind ip-address**命令的方式修改IP地址与客户端的绑定关系。只有删除了某个地址的绑定关系，才能将该地址与其他客户端绑定
配置静态地址绑定	**static-bind ip-address** *ip-address* [*mask-length* | **mask** *mask*] { **client-identifier** *client-identifier* | **hardware-address** *hardware-address* [**ethernet** | **token-ring**] }	
配置DHCP客户端使用的远程启动配置文件的HTTP形式URL	**bootfile-name** *url*	缺省情况下，未配置DHCP客户端使用的远程启动配置文件的HTTP形式URL

如果管理员使用 TFTP 服务器下发配置文件和配置脚本，则 DHCP 服务器地址池配置如下。

表1-2 使用 TFTP 服务器时的 DHCP 服务器的地址池配置

操作	命令	说明
进入系统视图	**system-view**	-
开启DHCP服务	**dhcp enable**	缺省情况下，DHCP服务处于关闭状态
创建DHCP地址池，并进入DHCP地址池视图	**dhcp server ip-pool** *pool-name*	缺省情况下，设备上不存在DHCP地址池
配置DHCP地址池动态分配的主网段	**network** *network-address* [*mask-length* | **mask** *mask*]	二者选其一 缺省情况下，未配置动态分配的主网段和静态地址绑定 多次执行**static-bind ip-address**命令，可以配置多个静态地址绑定 同一地址只能绑定给一个客户端。不允许通过重复执行**static-bind ip-address**命令的方式修改IP地址与客户端的绑定关系。只有删除了某个地址的绑定关系，才能将该地址与其他客户端绑定
配置静态地址绑定	**static-bind ip-address** *ip-address* [*mask-length* | **mask** *mask*] { **client-identifier** *client-identifier* | **hardware-address** *hardware-address* [**ethernet** | **token-ring**] }	
配置DHCP客户端使用的TFTP服务器地址	**tftp-server ip-address** *ip-address*	二者至少选其一 缺省情况下，未配置DHCP客户端使用的TFTP服务器地址和TFTP服务器名 在DHCP服务器上可以使用主机名或IP地址的形式来指定TFTP服务器。如果使用主机名的方式指定，则需要在网络中架设DNS服务器
配置DHCP客户端使用的TFTP服务器名	**tftp-server domain-name** *domain-name*	
配置DHCP客户端使用的启动配置文件名	**bootfile-name** *bootfile-name*	缺省情况下，未配置DHCP客户端使用的启动配置文件名

1.2.4 配置DNS服务器

在使用服务器自动配置功能时，在如下两种情况时，管理员需要配置 DNS 服务器：

- 当 TFTP 服务器上不存在主机名文件时，执行服务器自动配置的设备可以通过 DNS 服务器将自己的 IP 地址解析为主机名，以便从 TFTP 服务器获取到配置文件；
- 如果设备从 DHCP 应答报文中获取到 TFTP 服务器的域名，设备还可以通过 DNS 服务器将 TFTP 服务器的域名解析为 TFTP 服务器的 IP 地址。

1.2.5 配置网关

如果 DHCP 服务器、文件服务器和 DNS 服务器与执行服务器自动配置的设备不在同一网段，则需要部署网关设备，使得各个服务器和设备之间路由可达，并在网关上配置 DHCP 中继功能。

设备以广播方式向配置文件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，如果执行服务器自动配置的设备与配置文件服务器不在同一个网段，则需要在网关设备上配置 UDP Helper 功能，将广播报文转换成单播报文，转发给指定的配置文件服务器。有关 UDP Helper 功能的详细介绍，请参见“三层技术-IP 业务配置指导”中的“UDP-helper”。

1.2.6 选择接口获取配置文件

设备在进行自动配置时，系统按照如下规则选取符合条件的接口：

(1) 若有处于链路状态 UP 的管理以太网接口，则优先选取管理以太网接口；

(2) 若没有处于链路状态 UP 的管理以太网接口，有处于链路状态 UP 的二层以太网接口，则选取默认 VLAN 对应的 VLAN 虚接口；

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

(4) 若没有处于链路状态 UP 的三层以太网接口，则在 30 秒后开始下次服务器自动配置接口选择过程。

建议管理员将设备的管理以太网接口连入网络中，这样可以加快服务器自动配置的速度。如果设备当前不存在配置文件，设备即可自动执行服务器自动配置流程。

1.2.7 完成自动配置过程

设备进入服务器自动配置时：

- 如果获取并执行配置文件成功，则整个服务器自动配置过程结束。
- 如果获取不到自动配置文件，则本次自动配置尝试失败，设备将继续尝试自动配置。用户可以等待尝试次数达到上限，设备自动结束自动配置，或根据提示信息，使用<Ctrl+C>或<Ctrl+D>快捷键手工终止自动配置。自动配置失败并结束后，设备将以空配置启动。

需要注意的是：设备通过服务器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。建议在配置文件执行完成后，管理员在设备上执行 **save** 命令保存配置。否则，设备重启后还需重新执行服务器自动配置过程。**save** 命令的详细介绍请参见“基础配置命令参考”中的“配置文件管理”。

1.3 U盘自动配置

1.3.1 U盘自动配置简介

U 盘自动配置是指设备启动后自动检测 U 盘里的配置文件，并使用 U 盘的配置文件配置设备。

配置文件有.mdb 和.cfg 两种格式，.mdb 格式的配置文件会在系统启动后，进入自动配置流程之前完成加载。

设备启动时会根据是否存在下次启动配置文件进行如下动作：

- 不存在下次启动配置文件或空配置启动，则拷贝 U 盘的配置文件设置为下次启动配置文件，继续启动。
- 有下次启动配置文件启动的情况下，设备会根据下次启动配置文件是否存在对应的.mdb 文件，采取不同的处理流程：
  - 不存在.mdb 文件，则拷贝 U 盘的.cfg 配置文件设置为下次启动配置文件，继续启动。
  - 存在.mdb 文件，则拷贝 U 盘上的.cfg 配置文件设置为下次启动配置文件，判断当前存储介质上是否有和 U 盘上配置文件同名的.mdb 文件，如果有，则删除该.mdb 文件。如果没有，则重启设备，以便使 U 盘上的配置文件生效。

有关.mdb 和.cfg 文件的详细介绍请参见“基础配置指导”中的“配置文件管理”。

设备支持某些具有预读配置的功能，此时设备会在拷贝 U 盘的配置文件设置为下次启动配置文件之后重启设备。

1.3.2 注意事项

进行 U 盘自动配置，管理员需要注意以下事项：

- 设备只支持单主控板的 U 盘自动配置，在多主控板的情况下，可以在启动后再插入备用主控板，然后，配置文件会从主用主控板同步到备用主控板。
- 设备从 U 盘获取到配置文件后，将比较该配置文件与设备上的当前主配置文件内容是否相同：
  - 如果文件内容相同，设备将直接使用当前主用配置文件，不使用 U 盘上的配置文件。
  - 如果文件内容不相同，则设备将 U 盘中的配置文件复制到本地，并设置为下次启动的配置文件。设备本地存储中有重名配置文件时，根据本地配置文件的属性采用如下处理方式：
    - 如果本地重名配置文件为当前主用配置文件，则设备将该文件以“*原名*_bak.cfg”为名称另存。
    - 如果本地重名配置文件不是当前主用配置文件，则设备直接使用 U 盘中的配置文件覆盖本地重名文件。

1.3.3 操作步骤

为了实现设备可以通过 U 盘获取到配置文件，管理员需要执行以下步骤：

(1) 由于设备缺省情况下开启了 U 盘自动配置功能，设备启动后会自动从 U 盘获取配置文件，并执行该配置文件。如果设备未开启 U 盘自动配置功能，则需要执行 **autodeploy udisk enable** 命令开启该功能，再重启设备。

表1-3 开启 U 盘自动配置功能

操作	命令	说明
进入系统视图	**system-view**	-
开启U盘自动配置功能	**autodeploy udisk enable**	缺省情况下，U盘自动配置功能处于开启状态

说明

管理员执行 **undo autodeploy udisk enable** 命令并执行 **save** 命令保存，设备重新启动后会预先去配置文件查看是否有该配置，若有，则不进行 U 盘自动配置。

(2) 管理员需要创建配置文件名为“设备序列号.cfg”或“autodeploy.cfg”的配置文件，并保存在 U 盘（该 U 盘只能有一个分区）的根目录中。若 U 盘中同时存在“设备序列号.cfg”和“autodeploy.cfg”文件时，设备优先使用配置文件“设备序列号.cfg”。管理员可以使用命令 **display device manuinfo** 查询设备的序列号，该命令的详细介绍请参见“基础配置命令参考”中的“设备管理”。

(3) 管理员将保存有配置文件的 U 盘插入设备的 USB1 接口，即 usba0:，然后上电启动设备。

(4) 设备启动完成后，可以执行 **display current-configuration** 命令查看 U 盘中的配置是否已正确加载，该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”。如果配置文件下发失败，设备会把失败的日志写到 U 盘根目录下，日志文件名为“配置文件全名.log”。管理员可以根据日志信息进行问题定位和处理。

(5) U 盘自动配置完成后需拔出 U 盘，否则设备重启时，配置会被 U 盘中保存的配置文件覆盖。

说明

- 若设备执行 U 盘配置文件中的某条命令失败时，设备会忽略 U 盘配置文件中的所有配置，使用设备之前保存的配置文件；如果设备之前未保存配置文件，则设备空配置启动。
- U 盘自动配置成功时，系统（SYS）指示灯绿色快速闪烁 5 秒；U 盘自动配置失败时，系统（SYS）指示灯黄色快速闪烁 10 秒。

1.4 短信自动配置

1.4.1 注意事项

进行短信自动配置，管理员需要注意以下事项：

- 管理员需保证 iMC 服务器和短信网关设备之间路由可达。
- 管理员需要在需要获取配置文件的设备上配置 LoopBack 口的地址；否则，短信自动配置功能无法成功执行。
- 设备上电开启前，需要安装插有 SIM 卡的 3G/4G Modem 模块。

- 当 3G/4G 网络信号受到干扰或者信号强度较低时，短信发送端（手机或短信网关）与需要获取配置文件的设备之间的短信收发可能存在延迟。使用短信网关的方式，如果等待一段时间（管理员可以在 iMC 服务器设置等待时间）之后还没有收到设备的应答短信，短信网关可以重新发送部署短信。
- 管理员需要保证 SIM 卡未欠费且工作正常，并正确插入 3G/4G Modem 模块。如果是 USB 形式的 3G Modem 模块，可以使用主机来验证是否可以连接到 3G/4G 网络。

1.4.2 操作步骤

为了实现设备可以通过短信获取到配置文件，管理员需要执行以下步骤：

(1) 由于设备缺省情况下开启了短信自动配置功能，设备启动后收到短信发送端（手机或短信网关）的部署短信，自动从 iMC 服务器上获取配置文件，并执行该配置文件。如果设备未开启短信自动配置功能，则需要执行 **autodeploy sms enable** 命令开启该功能。

表1-4 开启短信自动配置功能

操作	命令	说明
进入系统视图	**system-view**	-
开启短信自动配置功能	**autodeploy sms enable**	缺省情况下，短信自动配置功能处于开启状态

(2) 当管理员配置 iMC 服务器并使用短信网关发送部署短信时，需要进行以下的配置：（以下文字描述的内容均需要管理员在 iMC 服务器的 Web 页面进行配置）

a. 添加设备管理：配置设备参数，包括设备名称、设备 SIM 卡号和 SIM 卡运营商信息等。设置设备 LoopBack 口地址作为管理地址；

b. 配置短信网关功能：配置通过短信网关通知设备启动短信自动配置功能。选择对应的短信网关设备，设置短信有效重发次数和短信发送超时时间。完成上述配置后，短信网关会在发送部署短信后开始计时，到达超时时间后，如果还未收到设备的应答短信，则短信网关会重发部署短信；到达重发次数后，短信网关不再发送部署短信，短信自动配置过程终止；

c. 配置短信发送功能：配置 iMC 服务器生成部署短信内容，发送到之前选择的短信网关设备，开启短信网关的短信发送功能；

d. 创建和部署自动配置文件：先创建自动配置文件，然后配置文件和需要获取配置文件的设备之间的对应关系，最后开启 iMC 服务器下发配置文件功能。

(3) 当管理员选择手机发送部署短信的方式时，管理员可以直接通过手机编辑部署短信通知需要获取配置文件的设备启动短信自动配置功能，并指定 iMC 服务器的地址等信息。使用手机发送部署短信的方式可以替代步骤（2）中的 b、c 两步。设备收到部署短信后即可通过 HTTP 方式登录 iMC 服务器并获取相应的配置文件。手工设置部署短信的模板内容为：

```
dpl:
pu:card
ps:card
dn:*99#
an:3gnet
ac:http://60.191.123.87:9090
au:admin
```

as:admin

表1-5 部署短信的模板字段及含义

字段	含义
dpl	部署短信标识，表示本条短信是部署短信，短信不以此开头的不是部署短信，不进行自动部署
pu	PPP认证的用户名，同时配置CHAP和PAP认证
cu	PPP认证的用户名，仅能配置为CHAP认证
1u	PPP认证的用户名，仅能配置为PAP认证
ps	PPP认证的密码
dn	PPP拨号串，由运营商提供： • 中国移动和中国联通：*99# • 中国电信：#777
an	3G/4G接入点名称，由运营商提供
ac	配置自动配置iMC服务器ACS（Auto-Configuration Server）的URL
au	iMC服务器登录用户名
as	iMC服务器登录密码


说明

- 配置部署短信时，dpl\dn\ac\au\as 为必填项。
- 如果设备的 PPP 拨号连接需要认证时（一般都需要进行认证），则应根据认证模式选择 pu、cu 和 1u 中的一种，并且在同一条短信中配置 ps（认证密码）来完成认证工作。
- 当运营商为中国移动、中国联通或中国电信时，an 字段可不填；当运营商为其他提供商时，an 字段必填，填充内容请咨询对应提供商。

(4) 设备启动完成后，可以执行 **display current-configuration** 命令查看 iMC 服务器下发的配置文件中的的配置是否已正确加载，该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”。


说明

- 管理员需要在 iMC 服务器上手工设置配置文件和设备之间的对应关系。这就需要管理员了解需要进行短信自动配置的设备的详细信息。否则，无法成功执行短信自动配置流程。
- 短信自动配置成功和失败，都会通过 3G/4G 网络发送报文通知 iMC 服务器，管理员可以通过 iMC 服务器查询到短信自动配置的执行结果。

1.5 自动配置典型配置举例

1.5.1 服务器自动配置举例（TFTP方式）

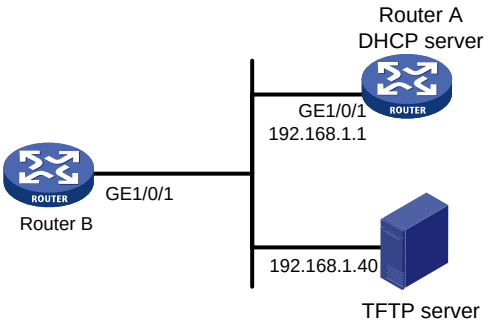
1. 组网需求

如图 1-2 所示，Router B 启动后自动从 TFTP 服务器获取配置文件，并执行该文件，以实现：

- 网络管理员能够通过 Telnet 方式登录、控制设备。
- 登录设备时需要进行认证，以提供一定的安全保证。

2. 组网图

图1-2 服务器自动配置组网图（TFTP 方式）



3. 配置步骤

(1) 配置 DHCP 服务器

开启 DHCP 服务，创建名称为 1 的 DHCP 地址池，配置地址池动态分配 IP 地址的网段为 192.168.1.0/24。

```
<RouterA> system-view
[RouterA] dhcp enable
[RouterA] dhcp server ip-pool 1
[RouterA-dhcp-pool-1] network 192.168.1.0 24
[RouterA-dhcp-pool-1] tftp-server ip-address 192.168.1.40
[RouterA-dhcp-pool-1] bootfile-name device.cfg
```

(2) 配置 TFTP 服务器，保证 Router B 可以从 TFTP 服务器成功下载配置文件 device.cfg。

在 TFTP 服务器创建配置文件 device.cfg，文件内容如下：

```
#
telnet server enable
#
local-user user
password simple abcabc
service-type telnet
authorization-attribute user-role network-operator
quit
#
user-interface vty 0 4
authentication-mode scheme
user-role network-admin
```

```
quit
#
interface gigabitethernet 1/0/1
port link-mode route
ip address dhcp-alloc
return
```

启动 TFTP 管理软件，开启 TFTP 服务（配置过程略）。

4. 验证配置

(1) Router B 在没有配置文件的情况下启动。启动成功后，在 Router A 上查看地址池中的地址绑定信息。

```
<RouterA> display dhcp server ip-in-use
IP address       Client identifier/    Lease expiration      Type
                 Hardware address
192.168.1.2      0030-3030-632e-3239-  May 12 17:41:15 2016  Auto(C)
                 3035-2e36-3736-622d-
                 4574-6830-2f30-2f32
```

(2) 在 Router A 上执行如下命令：

```
<RouterA> telnet 192.168.1.2
```

(3) 输入用户名 user、密码 abcabc 后，用户可以登录 Router B。

1.5.2 服务器自动配置举例（HTTP Tcl方式）

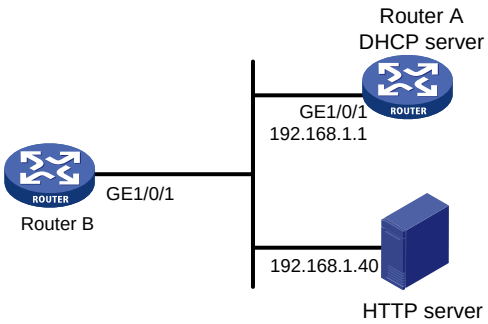
1. 组网需求

如图 1-3 所示，Router B 启动后自动从 HTTP 服务器获取 Tcl 脚本启动配置文件，并执行该文件，以实现：

- 网络管理员能够通过 Telnet 方式登录、控制设备。
- 登录设备时需要进行认证，以提供一定的安全保证。

2. 组网图

图1-3 服务器自动配置组网图（HTTP Tcl 方式）



3. 配置步骤

(1) 配置 DHCP 服务器

开启 DHCP 服务，创建名称为 1 的 DHCP 地址池，配置地址池动态分配 IP 地址的网段为 192.168.1.0/24。

```
<RouterA> system-view
[RouterA] dhcp enable
[RouterA] dhcp server ip-pool 1
[RouterA-dhcp-pool-1] network 192.168.1.0 24
```

配置 DHCP 客户端远程启动配置文件为 HTTP 形式的 URL。

```
[RouterA-dhcp-pool-1] bootfile-name http://192.168.1.40/device.tcl
```

(2) 配置 HTTP 服务器，保证 Router B 可以从 HTTP 服务器成功下载配置文件 device.tcl。

在 HTTP 服务器创建配置文件 device.tcl，文件内容如下：

```
system-view
telnet server enable
local-user user
password simple abcabc
service-type telnet
quit
user-interface vty 0 4
authentication-mode scheme
user-role network-admin
quit

interface gigabitethernet 1/0/1
port link-mode route
ip address dhcp-alloc
return
```

启动 HTTP 管理软件，开启 HTTP 服务（配置过程略）。

4. 验证配置

(1) Router B 在没有配置文件的情况下启动。启动成功后，在 Router A 上查看地址池中的地址绑定信息。

```
<RouterA> display dhcp server ip-in-use
IP address       Client identifier/    Lease expiration      Type
                 Hardware address
192.168.1.2      0030-3030-632e-3239-  May 12 17:41:15 2016  Auto(C)
                 3035-2e36-3736-622d-
                 4574-6830-2f30-2f32
```

(2) 在 Router A 上执行如下命令：

```
<RouterA> telnet 192.168.1.2
```

(3) 输入用户名 user、密码 abcabc 后，用户可以登录 Router B。

1.5.3 服务器自动配置举例（HTTP Python方式）

说明

本配置举例的支持情况请参见基础配置指导中的“Python”。

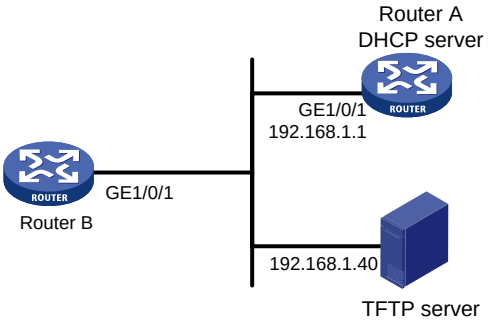
1. 组网需求

如图 1-4 所示，Router B 启动后自动从 HTTP 服务器获取 Python 脚本启动配置文件，并执行该文件，以实现：

- 网络管理员能够通过 Telnet 方式登录、控制设备。
- 登录设备时需要进行认证，以提供一定的安全保证。

2. 组网图

图1-4 服务器自动配置组网图（HTTP Python 方式）



3. 配置步骤

(1) 配置 DHCP 服务器

开启 DHCP 服务，创建名称为 1 的 DHCP 地址池，配置地址池动态分配 IP 地址的网段为 192.168.1.0/24。

```
<RouterA> system-view
[RouterA] dhcp enable
[RouterA] dhcp server ip-pool 1
[RouterA-dhcp-pool-1] network 192.168.1.0 24
```

配置 DHCP 客户端远程启动配置文件为 HTTP 形式的 URL。

```
[RouterA-dhcp-pool-1] bootfile-name http://192.168.1.40/device.py
```

(2) 配置 HTTP 服务器，保证 Router B 可以从 HTTP 服务器成功下载配置文件 device.py。

在 HTTP 服务器创建配置文件 device.py，文件内容如下：

```
#!usr/bin/python

import comware
comware.CLI('system-view ;telnet server enable ;local-user user ;password simple
abcabc ;service-type telnet ;quit ;user-interface vty 0 4 ;authentication-mode
scheme ;user-role network-admin ;quit ;interface gigabitethernet 1/0/1 ;port link-mode
route ;ip address dhcp-alloc ;return ')
```

启动 HTTP 管理软件，开启 HTTP 服务（配置过程略）。

4. 验证配置

(1) Router B 在没有配置文件的情况下启动。启动成功后，在 Router A 上查看地址池中的地址绑定信息。

```
<RouterA> display dhcp server ip-in-use
IP address       Client identifier/    Lease expiration      Type
                 Hardware address
```

```
192.168.1.2      0030-3030-632e-3239-  May 12 17:41:15 2016  Auto(C)
                 3035-2e36-3736-622d-
                 4574-6830-2f30-2f32
```

(2) 在 Router A 上执行如下命令：

```
<RouterA> telnet 192.168.1.2
```

(3) 输入用户名 user、密码 abcabc 后，用户可以登录 Router B。

1.5.4 服务器自动配置实现IRF零配置举例

说明

本举例仅针对支持 IRF 的款型。

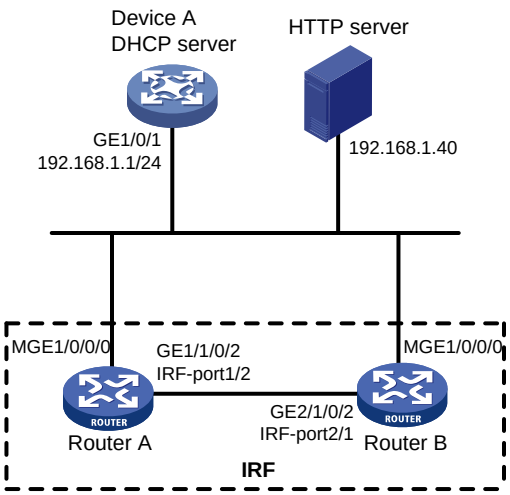
1. 组网需求

如图 1-5 所示，Router A 和 Router B 通过管理以太网口分别与 HTTP 服务器和 Device A 相连。Device A 上开启 DHCP 服务。为网络中的设备动态分配 192.168.1.0/24 网段的 IP 地址。

现要求通过自动配置实现 Router A 和 Router B 根据脚本自动执行 IRF 配置的相关命令。然后再连接 Router A 和 Router B 之间的线缆，完成 IRF 的建立。

2. 组网图

图1-5 服务器自动配置实现 IRF 零配置组网图



3. 配置步骤

(1) 配置设备接口地址，保证设备间路由可达。

配置 HTTP 服务器。启动 HTTP 管理软件，开启 HTTP 服务（配置过程略）。针对 IRF 零配置，HTTP 服务器上需要配置 Python 脚本文件、配置文件、sn.txt 和软件启动包等文件。以下是关于各文件的介绍：

- Python 脚本文件：Python 脚本是设备进行 IRF 零配置操作的主要文件，需要管理员自行准备并保存在 HTTP 服务器上。Python 脚本需要完成的操作：
  - 设备判断 flash 是否存在足够的存储空间（可选）；

- 设备从 HTTP 服务器下载配置文件；
- 设备从 HTTP 服务器下载启动软件包（可选）；
- 设备从 HTTP 服务器下载 sn.txt 文件；
- 配置设备下次启动时使用的启动软件包（可选）；
- 解析 sn.txt 文件并修改设备的 IRF 成员编号；
- 配置设备下次启动时使用的配置文件；
- 设备重新启动。

- 配置文件：配置文件包含了所有设备进行 IRF 的相关命令，管理员可以在已经成功创建 IRF 的设备上，将配置文件导出并修改然后保存在 HTTP 服务器上，供需要创建类似拓扑 IRF 的设备下载使用。
- sn.txt 文件：每个设备都有唯一的设备序列号，sn.txt 文件根据设备的序列号来指定设备在 IRF 组中的成员编码。设备通过运行 Python 脚本来解析 sn.txt 文件，然后修改设备的 IRF 成员编号，并根据自身的成员编号来完成相应的 IRF 配置。
- 软件启动包：软件启动包是设备启动、运行的必备软件，需保存在 HTTP 服务器上。如果现有设备（包括主设备和备设备）的启动软件包全部一致且不需要升级软件版本，可不需要准备该文件。

(2) 在 Device A 上配置 DHCP 服务器

开启 DHCP 服务，创建名称为 1 的 DHCP 地址池，配置地址池动态分配 IP 地址的网段为 192.168.1.0/24。

```
<DeviceA> system-view
[DeviceA] dhcp enable
[DeviceA] dhcp server ip-pool 1
[DeviceA-dhcp-pool-1] network 192.168.1.0 24
```

配置 DHCP 客户端远程启动配置文件为 HTTP 形式的 URL。

```
[DeviceA-dhcp-pool-1] bootfile-name http://192.168.1.40/device.py
[DeviceA-dhcp-pool-1] quit
```

配置接口 GigabitEthernet1/0/1 工作在 DHCP 服务器模式。

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] dhcp select server
[DeviceA-GigabitEthernet1/0/1] quit
```

(3) 设备根据 DHCP 服务器获取到 Python 脚本文件，执行 Python 脚本下载配置文件和软件启动包；解析 sn.txt 文件生成 IRF 成员编号。然后，所有设备会执行重启操作。

(4) 设备重启完毕后，连接 Router A 和 Router B 之间的线缆，连接好线缆后设备将进行 IRF 选举，选举失败的一台设备会再次重启。当设备自动重启后，Router A 和 Router B 成功组成 IRF。

4. 验证配置

下面以 Router A 为例验证设备是否成功组成 IRF，Router B 和 Router A 类似，不再赘述。

显示 IRF 中所有成员设备的相关信息。

```
<Router A> display irf
MemberID  Slot  Role    Priority  CPU-Mac         Description
   1      1     Standby 1         00e0-fc0f-8c02  ---
 *+2      1     Master  30        00e0-fc0f-8c14  ---
-------------------------------------------------
```

```
* indicates the device is the master.
+ indicates the device through which the user logs in.

The Bridge MAC of the IRF is: 000c-1000-1111
Auto upgrade                : yes
Mac persistent              : always
Domain ID                   : 0
Auto merge                  : yes
```

以上显示信息表明 IRF 已经成功建立。

目 录

1 安全域

设备各款型对于本节所描述的特性支持情况有所不同，详细差异信息如下：

型号	特性	描述
MSR810/810-W/810-W-DB/810-LM/810-W-LM/810-10-PoE/810-LM-HK/810-W-LM-HK/810-LMS/810-LUS	安全域	仅MSR810-LMS/810-LUS不支持
MSR2600-6-X1/2600-10-X1		支持
MSR 2630		支持
MSR3600-28/3600-51		支持
MSR3600-28-SI/3600-51-SI		支持
MSR3610-X1/3610-X1-DP/3610-X1-DC/3610-X1-DP-DC		支持
MSR 3610/3620/3620-DP/3640/3660		支持
MSR5620/5660/5680		支持

型号	特性	描述
MSR810-W-WiNet/810-LM-WiNet	安全域	支持
MSR830-4LM-WiNet		支持
MSR830-5BEI-WiNet/830-6EI-WiNet/830-10BEI-WiNet		支持
MSR830-6BHI-WiNet/830-10BHI-WiNet		支持
MSR2600-10-X1-WiNet		支持
MSR2630-WiNet		支持
MSR3600-28-WiNet		支持
MSR3610-X1-WiNet		支持
MSR3610-WiNet/3620-10-WiNet/3620-DP-WiNet/3620-WiNet/3660-WiNet		支持

型号	特性	描述
MSR810-LM-GL	安全域	支持
MSR810-W-LM-GL		支持
MSR830-6EI-GL		支持
MSR830-10EI-GL		支持
MSR830-6HI-GL		支持
MSR830-10HI-GL		支持

型号	特性	描述
MSR2600-6-X1-GL		支持
MSR3600-28-SI-GL		支持

1.1 安全域简介

安全域（Security Zone），是一个逻辑概念，用于管理防火墙设备上安全需求相同的多个接口。管理员将安全需求相同的接口进行分类，并划分到不同的安全域，能够实现安全策略的统一管理。

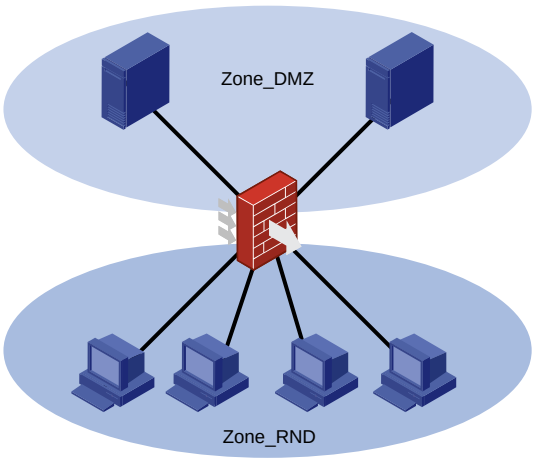
传统防火墙的安全策略配置通常是基于报文入接口、出接口的，进入和离开接口的流量基于接口上指定方向的策略规则进行过滤。这种基于接口的策略配置方式需要为每一个接口配置安全策略，给网络管理员带来配置和维护上的负担。随着防火墙技术的发展，防火墙已经逐渐摆脱了只连接外网和内网的角色，出现了内网/外网/DMZ（Demilitarized Zone，非军事区）的模式，并且向着提供高端口密度服务的方向发展。基于安全域来配置安全策略的方式可以解决上述问题。

说明

DMZ 这一术语起源于军方，指的是介于严格的军事管制区和松散的公共区域之间的一种有着部分管制的区域。安全域中引用这一术语，指代一个逻辑上和物理上都与内部网络和外部网络分离的区域。通常部署网络时，将那些需要被公共访问的设备（如 Web server、FTP server 等）放置于此。

一个安全域中，可以包含多个成员。例如，可以将公司防火墙设备上连接到研发部门不同网段的四个接口作为成员加入安全域 Zone_RND，连接服务器区的两个接口作为成员加入安全域 Zone_DMZ，这样管理员只需要部署这两个域之间的安全策略即可，此处的安全策略包括包过滤策略、ASPF 策略、对象策略等。如果后续网络环境发生了变化，则只需要调整相关域内的接口，而域间安全策略不需要修改。包过滤策略的相关配置请参考“ACL 和 QoS 配置指导”中的“ACL”。ASPF 策略的相关配置请参考“安全配置指导”中的“ASPF”。对象策略的相关配置请参考“安全配置指导”中的“对象策略”。

图1-1 安全域划分示意图



创建安全域后，设备上各接口的报文转发遵循以下规则：

- 一个安全域中的接口与一个不属于任何安全域的接口之间的报文，会被丢弃。
- 属于同一个安全域的各接口之间的报文缺省会被丢弃。
- 安全域之间的报文由域间策略进行安全检查，并根据检查结果放行或丢弃。若域间策略不存在或不生效，则报文会被丢弃。
- 非安全域的接口之间的报文被放行。
- 目的地址或源地址为本机的报文，缺省会被放行，若该报文与域间策略匹配，则由域间策略进行安全检查，并根据检查结果放行或丢弃。

1.2 配置限制和指导

安全域不支持配置回滚。

1.3 安全域配置任务简介

表1-1 安全域配置任务简介

配置任务	说明	详细配置
创建安全域	必选	1.4.1
向安全域中添加成员	必选	1.4.2
创建安全域间实例	可选	1.4.3
配置安全域内接口间报文处理的缺省动作	可选	1.4.4

1.4 配置安全域

1.4.1 创建安全域

当首次执行创建安全域或者安全域间实例的命令时，系统会自动创建以下缺省安全域：Local、Trust、DMZ、Management 和 Untrust。

缺省的安全域中没有接口，需要手工向其中添加接口，而且，缺省安全域不能被删除。

表1-2 创建安全域

操作	命令	说明
进入系统视图	**system-view**	-
创建安全域，并进入安全域视图	**security-zone name** *zone-name*	缺省情况下，设备不存在任何安全域

1.4.2 向安全域中添加成员

创建安全域后，需要给安全域添加成员。安全域的成员类型包括：

- 三层接口，包括三层以太网接口、三层以太网子接口和其它三层逻辑接口。配置该成员后，该接口收发的所有报文将由安全域下配置的安全控制策略来处理。
- 二层接口和 VLAN。配置该成员后，该接口收发的、携带了指定 VLAN Tag 的报文，将由安全域下配置的安全控制策略来处理。

表1-3 向安全域中添加成员

操作	命令	说明
进入系统视图	**system-view**	-
进入安全域视图	**security-zone name** *zone-name*	-
向安全域中添加三层接口成员	**import interface** *layer3-interface-type layer3-interface-number*	缺省情况下，安全域中不存在任何三层接口成员 可以通过多次执行本命令，向安全域中添加多个三层接口成员
向安全域中添加二层接口和VLAN成员	**import interface** *layer2-interface-type layer2-interface-number* **vlan** *vlan-list*	缺省情况下，安全域中不存在任何二层接口和VLAN成员 可以通过多次执行本命令，向安全域中添加多个二层接口和VLAN成员

1.4.3 创建安全域间实例

安全域间实例用于指定安全策略（如包过滤策略、ASPF 策略、对象策略等）需要检测的业务流的源安全域和目的安全域，它们分别描述了经过网络设备的业务流的首个数据包要进入的安全域和要离开的安全域。在安全域间实例上应用安全策略可实现对指定的业务流进行安全策略检查。

当存在 **any** 到 **any** 安全域间实例时，仅当报文未匹配对应域间实例时，才会匹配 **any** 到 **any** 安全域间实例。如未配置 **any** 到 **any** 域间实例且报文未匹配对应域间实例时，则直接丢弃报文。

Management 和 Local 安全域间之间的报文只能匹配 Local 到 Management 的安全域间实例和 Management 到 Local 的安全域间实例，不会匹配 **any** 到 **any** 的安全域间实例。

当安全域间实例上同时应用了对象策略和包过滤策略时，对象策略的优先级高于包过滤策略。

表1-4 创建安全域间实例

操作	命令	说明
进入系统视图	**system-view**	-
创建安全域间实例，并进入安全域间实例视图	**zone-pair security source** { *source-zone-name* | **any** } **destination** { *destination-zone-name* | **any** }	缺省情况下，不存在安全域间实例

1.4.4 配置安全域内接口间报文处理的缺省动作

对于同一安全域内接口间的报文，若设备上不存在当前域到当前域的安全域间实例，设备缺省会将其丢弃，可以通过配置安全域内接口间报文处理的缺省动作为 permit 来允许其通过。

表1-5 配置安全域内接口间报文处理的缺省动作

操作	命令	说明
进入系统视图	**system-view**	-
配置同一安全域内接口间报文处理的缺省动作	• permit 动作 **security-zone intra-zone default permit** • deny 动作 **undo security-zone intra-zone default permit**	缺省情况下，同一安全域内报文过滤的缺省动作为deny

1.5 安全域显示和维护

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安全域的相关信息，通过查看显示信息验证配置的效果。

表1-6 安全域显示和维护

操作	命令
显示安全域信息，包括预定义的和自定义的安全域信息	**display security-zone** [**name** *zone-name*]
显示已创建的所有安全域间实例的信息	**display zone-pair security**

1.6 安全域典型配置举例

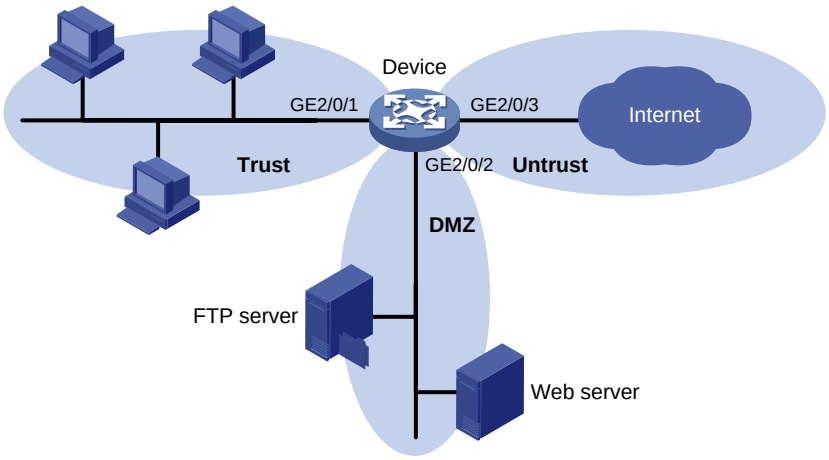
1. 组网需求

某公司以 Device 作为网络边界防火墙，连接公司内部网络和 Internet。公司需要对外提供 Web 服务和 FTP 服务。现需要在防火墙上部署安全域，并基于以下安全需求进行域间安全策略的配置。

- 与接口 GigabitEthernet2/0/1 相连的公司内部网络属于可信任网络，部署在 Trust 域，可以自由访问服务器和外部网络。
- 与接口 GigabitEthernet2/0/3 相连的外部网络属于不可信任网络，部署在 Untrust 域，访问公司内部网络和服务器时，需要受到严格的域间安全策略的限制。
- 与接口 GigabitEthernet2/0/2 相连的 Web server、FTP server 部署在 DMZ 域，可以自由访问处于 Untrust 域的外部网络，但在访问处于 Trust 域的公司内部网络时，需要受到严格的域间安全策略的限制。

2. 组网图

图1-2 安全域组网图



3. 配置步骤

向安全域 Trust 中添加接口 GigabitEthernet2/0/1。

```
<Device> system-view
[Device] security-zone name trust
[Device-security-zone-Trust] import interface gigabitethernet 2/0/1
[Device-security-zone-Trust] quit
```

向安全域 DMZ 中添加接口 GigabitEthernet2/0/2。

```
[Device] security-zone name dmz
[Device-security-zone-DMZ] import interface gigabitethernet 2/0/2
[Device-security-zone-DMZ] quit
```

向安全域 Untrust 中添加接口 GigabitEthernet2/0/3。

```
[Device] security-zone name untrust
[Device-security-zone-Untrust] import interface gigabitethernet 2/0/3
[Device-security-zone-Untrust] quit
```

配置 ACL 3500，定义规则：允许 IP 流量。

```
[Device] acl advanced 3500
[Device-acl-ipv4-adv-3500] rule permit ip
[Device-acl-ipv4-adv-3500] quit
```

创建 ASPF 策略 1，配置检测应用层协议 FTP（FTP 仅为示例，若要检测其它应用协议，可根据需要配置）。

```
[Device] aspf policy 1
[Device-aspf-policy-1] detect ftp
[Device-aspf-policy-1] quit
```

创建源安全域 Trust 到目的安全域 Untrust 的安全域间实例，并在该安全域间实例上应用 ASPF 策略和包过滤策略，可以拒绝 Untrust 域用户对 Trust 的访问，但 Trust 域用户访问 Untrust 域以及返回的报文可以通过。

```
[Device] zone-pair security source trust destination untrust
[Device-zone-pair-security-Trust-Untrust] aspf apply policy 1
[Device-zone-pair-security-Trust-Untrust] packet-filter 3500
```

```
[Device-zone-pair-security-Trust-Untrust] quit
```

创建源安全域 Trust 到目的安全域 DMZ 的安全域间实例，并在该安全域间实例上开启 ASPF 检测功能，可以拒绝 DMZ 域用户对 Trust 的访问，但 Trust 域用户访问 DMZ 域以及返回的报文可以通过。

```
[Device] zone-pair security source trust destination dmz
[Device-zone-pair-security-Trust-DMZ] aspf apply policy 1
[Device-zone-pair-security-Trust-DMZ] packet-filter 3500
[Device-zone-pair-security-Trust-DMZ] quit
```

4. 验证配置

以上配置完成后，内网主机可访问外部网络以及 DMZ 域内的 FTP 服务器资源。外部网络向内部网络以及 DMZ 域主动发起的连接请求将被拒绝。

目 录

1 设备管理

设备各款型使用的命令行形式有所不同，详细差异信息如下：

命令行形式	款型
集中式	• MSR810/810-W/810-W-DB/810-LM/810-W-LM/810-10-PoE/810-LM-HK/810-W-LM-HK • MSR810-LMS/810-LUS • MSR2600-6-X1/2600-10-X1/2630 • MSR3600-28/3600-51/3600-28-SI/3600-51-SI • MSR3610-X1/3610-X1-DP/3610-X1-DC/3610-X1-DP-DC • MSR 3610/3620/3620-DP/3640/3660 • MSR810-W-WiNet/810-LM-WiNet/830-4LM-WiNet • MSR830-5BEI-WiNet/830-6EI-WiNet/830-10BEI-WiNet • MSR830-6BHI-WiNet/830-10BHI-WiNet • MSR2600-10-X1-WiNet/2630-WiNet • MSR3600-28-WiNet/3610-X1-WiNet • MSR3610-WiNet/3620-10-WiNet/3620-DP-WiNet/3620-WiNet/3660-WiNet • MSR810-LM-GL/810-W-LM-GL • MSR830-6EI-GL/830-10EI-GL/830-6HI-GL/830-10HI-GL • MSR2600-6-X1-GL/3600-28-SI-GL
分布式	MSR5620/5660/5680

通过设备管理功能，用户能够查看设备当前的工作状态，配置设备运行的相关参数，实现对设备的日常维护和管理。

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

1.1 设备管理配置任务简介

配置任务	说明	详细配置
配置设备名称	必选	1.2
配置系统时间	必选	1.3
使能版权信息显示功能	可选	1.4
配置欢迎信息	可选	1.5
重启设备	可选	1.6
配置定时执行任务功能	可选	1.7
配置密码恢复功能	可选	1.8
电源管理	必选	1.9

配置任务	说明	详细配置
配置端口状态检测定时器	可选	1.10
监控CPU利用率	可选	1.11
配置内存告警门限	必选	1.12
关闭USB接口	可选	1.13
配置接口卡的工作模式	必选	1.14
可插拔接口模块的识别与诊断	必选	1.15
恢复出厂状态	可选	1.16
卸载HMIM接口模块	可选	1.17
通过FoTA方式升级Modem的固件版本	可选	1.18
配置PTP加速功能	可选	1.19
关闭蓝牙功能	可选	1.20

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**	-
配置设备名称	**sysname** *sysname*	缺省情况下，设备名称为H3C

1.3 配置系统时间

为了保证与其它设备协调工作，为了更好的监控和维护设备，请确保设备的系统时间是准确的。用系统时间的获取方式有：

- 配置 **clock protocol none** 命令后，通过 **clock datetime** 命令直接配置。**clock datetime** 命令中指定的时间即为当前的系统时间。后续，设备使用内部晶体震荡器产生的时钟信号计时。
- 配置 **clock protocol ntp** 命令后，通过 NTP 协议从网络中获取时间。该方式下，设备会周期性的同步服务器的 UTC（Coordinated Universal Time，国际协调时间）时间，并用同步得到的 UTC 时间和设备上配置的本地时区、夏令时参数运算，得出当前的系统时间。该方式获取的时间比命令行配置的时间更精准，推荐使用。关于 NTP 的详细介绍和配置，请参见“网络管理和监控配置指导”中的“NTP”。

通过 NTP 协议获取的 UTC 时间比命令行配置的 UTC 时间更精确。

表1-2 配置系统时间

操作	命令	说明
进入系统视图	**system-view**	-
通过命令行配置系统时间	**clock protocol none**	两者选其一 缺省情况下，通过NTP协议获取系统时间 多次执行**clock protocol**命令，最后一次执行的命令生效
	quit	
	clock datetime *time date*	
	system-view	
配置通过NTP协议获取时间	**clock protocol ntp**	
配置系统所在的时区	**clock timezone** *zone-name* { **add** | **minus** } *zone-offset*	缺省情况下，未配置时区 请将所有网络设备的时区和当地地理时区保持一致 修改时区后，设备会自动重新计算当前的系统时间，计算后得到的系统时间可通过**display clock**命令查看
配置夏令时	**clock summer-time** *name start-time start-date end-time end-date add-time*	缺省情况下，未配置夏令时 请将所有网络设备的夏令时和当地夏令时保持一致 修改夏令时后，设备会自动重新计算当前的系统时间，计算后得到的系统时间可通过**display clock**命令查看

1.4 开启版权信息显示功能

- 开启版权信息显示功能后，使用 Telnet 或 SSH 方式登录设备时会显示版权信息，使用 Console 口、AUX 口登录设备再退出用户视图时，由于设备会自动再次登录，因此也会显示版权信息，其它情况不显示版权信息。显示的版权信息形如：

```
******************************************************************************
* Copyright (c) 2004-2018 New H3C Technologies Co., Ltd. All rights reserved.*
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************
```

- 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1-3 使能版权信息显示功能

操作	命令	说明
进入系统视图	**system-view**	-
开启版权信息显示功能	**copyright-info enable**	缺省情况下，版权信息显示功能处于开启状态

1.5 配置欢迎信息

1.5.1 欢迎信息简介

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

系统支持如下几种欢迎信息：

- legal 欢迎信息。系统在用户登录前会给出一些版权或者授权信息，然后显示 legal 条幅，并等待用户确认是否继续登录。如果用户输入“Y”或者按<Enter>键，则继续登录过程；如果输入“N”，则断开连接，退出登录过程。“Y”和“N”不区分大小写。
- MOTD（Message Of The Day，每日提示）欢迎信息。
- login 欢迎信息。只有用户界面下配置了 password 或者 scheme 认证方式时，才显示该欢迎信息。
- shell 欢迎信息。用户登录显示 shell 欢迎信息。

以上几种欢迎信息的显示顺序为：legal 欢迎信息、MOTD 欢迎信息、login 欢迎信息或 shell 欢迎信息。

1.5.2 输入欢迎信息

输入欢迎信息时，有两种方式：

(1) 单行输入

该方式下，命令关键字与欢迎信息的所有内容在同一行中输入，输入内容 *text* 的第一个字符和最后一个字符分别作为起始符和结束符，起始符和结束符可以为任意可见字符但两者必须相同，且不属于欢迎信息的内容。此时包括命令关键字、起始符和结束符在内，一共可以输入 511 个字符。在该方式下输入欢迎信息过程中不能回车（按<Enter>键）。例如，配置 shell 欢迎信息为“Have a nice day.”，可参照如下步骤：

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

(2) 多行输入

该方式下，通过回车键将欢迎信息分多行输入，此时包括命令关键字、起始符和结束符在内，一共可以输入 2002 个字符。如果输入的内容中包括换行，则换行算两个字符。多行输入又分三种方式：

- 命令关键字后直接回车，输入欢迎信息并以“%”作为欢迎信息的结束符结束配置，“%”不属于欢迎信息的内容。例如，配置的欢迎信息为“Have a nice day.”，可参照如下步骤：

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

- 命令关键字后输入一个字符后回车，以这个字符作为欢迎信息的起始符和结束符，输入完欢迎信息以后，以结束符结束配置。起始符和结束符不属于欢迎信息的内容。例如，配置的欢迎信息为“Have a nice day.”，可参照如下步骤：

```
<System> system-view
[System] header shell A
Please input banner content, and quit with the character 'A'.
```

```
Have a nice day.A
```

- 命令关键字后输入多个字符（首尾不相同）后回车，以命令关键字后的第一个字符作为欢迎信息的起始符和结束符，输入完欢迎信息以后，以结束符结束配置。起始符和结束符不属于欢迎信息的内容。例如，配置的欢迎信息为“Have a nice day.”，可参照如下步骤：

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

说明

- 单行输入方式配置的欢迎信息本身不能包含换行符。
- 多行输入方式配置的欢迎信息本身可以包含换行符。配置欢迎信息内容时键入的回车，即对应最终显示的欢迎信息中的换行。

1.5.3 配置欢迎信息

表1-4 配置欢迎信息

操作	命令	说明
进入系统视图	**system-view**	-
配置legal欢迎信息	**header legal** *text*	缺省情况下，未配置legal欢迎信息
配置MOTD欢迎信息	**header motd** *text*	缺省情况下，未配置MOTD欢迎信息
配置login欢迎信息	**header login** *text*	缺省情况下，未配置login欢迎信息
配置shell欢迎信息	**header shell** *text*	缺省情况下，未配置shell欢迎信息

1.6 重启设备

提示

重新启动会导致业务中断，请谨慎使用。

1. 简介

重启设备的方式有以下几种：

(1) 硬件重启

通过断电后重新上电来重启设备。该方式对设备影响较大，如果对运行中的设备进行强制断电，可能会造成数据丢失。一般情况下，建议不要使用这种方式。

(2) 命令行重启

主要用于远程重启设备，而不需要到设备所在地进行断电/上电重启。该方式有两种配置方式：

- 通过 **reboot** 命令行立即重启设备。

- 通过 **scheduler reboot** 定时重启设备。该方式效果同执行 **reboot** 命令，只是使用该方式用户可以配置时间点，让设备在该时间点自动重启，或者配置一个时延，让设备经过指定时间后自动重启。比“通过 **reboot** 命令行立即重启设备”方式灵活。

2. 配置准备

- 重启前请使用 **save** 命令保存当前配置，以免重启后配置丢失。（**save** 命令的详细介绍请参见“基础配置命令参考”中的“配置文件管理”）
- 重启前请使用 **display startup** 和 **display boot-loader** 命令分别确认是否配置了合适的下次启动配置文件和下次启动文件。如果主用启动文件损坏或者不存在，则不能通过 **reboot** 命令重启设备。此时，可以通过指定新的主用启动文件再重启。**display startup** 命令的详细介绍请参见“基础配置命令参考”中的“配置文件管理”，**display boot-loader** 命令的详细介绍请参见“基础配置命令参考”中的“软件升级”。

3. 配置步骤

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。

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

(1) 通过 **reboot** 命令行立即重启设备

表1-5 通过命令行立即重启设备

操作	命令	说明
立即重启设备或者指定子卡（集中式设备—独立运行模式）	**reboot** [**force**]	该命令在用户视图下执行
立即重启指定单板、指定子卡或整台设备（分布式设备－独立运行模式）	**reboot** [**slot** *slot-number* [**subslot** *subslot-number*]] [**force**]	该命令在用户视图下执行
立即重启指定成员设备、指定子卡或所有成员设备（集中式设备—IRF模式）	**reboot** [**slot** *slot-number* [**subslot** *subslot-number*]] [**force**]	该命令在用户视图下执行
立即重启指定成员设备、指定子卡或所有成员设备（分布式设备－IRF模式）	**reboot** [**chassis** *chassis-number* [**slot** *slot-number* [**subslot** *subslot-number*]]] [**force**]	该命令在用户视图下执行

(2) 通过 **scheduler reboot** 定时重启设备

表1-6 通过命令行定时重启设备

操作	命令	说明
配置设备重启的具体时间和日期	**scheduler reboot at** *time* [*date*]	二者选其一 缺省情况下，未配置设备重启的时间
配置重启设备的延迟时间	**scheduler reboot delay** *time*	使用该方式配置定时重启后，如果发生主备倒换，则定时重启配置将自动取消（分布式设备－独立运行模式） 该配置对所有成员设备生效。配置定时重启后，如果发生主设备和从设备倒换，则定时重启配置将自动取消（集中式设备—IRF模式）

操作	命令	说明
		该配置对所有成员设备生效。配置定时重启后，如果发生全局主用主控板和全局备用主控板的主备倒换，则定时重启配置将自动取消（分布式设备－IRF模式） 两命令均在用户视图下执行

1.7 配置定时执行任务功能

1.7.1 定时执行任务功能简介

通过配置定时执行任务功能可以让设备在指定时刻或延迟指定时间后，自动执行指定命令，使设备能够在无人值守的情况下完成某些配置。该功能不但增强了设备的自动控制和管理能力，提高了易用性，而且可以起到有效节能的作用。

定时执行任务有两种类型：一次性执行方式和循环执行方式。两种方式都支持在同一任务中执行多条命令。一次性执行的配置任务不能保存到配置文件，设备重启后该任务将取消。循环执行的配置任务能保存到配置文件，等下次时间到达，任务将自动执行。

1.7.2 配置指导和注意事项

- 设备重启后，部分设备系统时间会恢复到出厂配置。请重新配置系统时间，或者配置 NTP 功能，保证设备能够获得准确的时间，以便配置的定时执行任务能够在期望的时间点执行。NTP 的配置请参见“网络管理和监控配置指导”中的“NTP”。
- 通过 **command** 分配的命令行必须是设备上可成功执行的命令行，但不能包括 **telnet**、**ftp**、**ssh2** 和 **monitor process**。由用户保证配置的正确性，否则，命令行不能自动被执行。
- 如果需要分配的命令（假设为 A）是用户视图下的命令，则直接使用 **command** 命令分配即可，比如：command 1 display interface；如果需要分配的命令（假设为 A）是非用户视图下的命令，则必须先分配进入 A 所在视图的命令（指定较小的 *id* 值），再分配 A。比如：要使用 Job 定时执行 **shutdown** 命令，则需执行三次 **command** 命令，分别分配 **system-view**、**interface**、**shutdown** 命令，且各 **command** 命令的 *id* 值逐渐增大。
- 定时执行任务时，设备不会与用户交互信息。当需要用户交互确认时，系统将自动输入“Y”或“Yes”；当需要用户交互输入字符信息时，系统将自动输入缺省字符串，没有缺省字符串的将自动输入空字符串。
- 系统将在后台定时执行任务，不显示任何输出信息（log、trap、debug 等系统信息除外）。

1.7.3 配置定时执行任务

表1-7 配置定时执行任务（一次性执行）

操作	命令	说明
进入系统视图	**system-view**	-
创建Job	**scheduler job** *job-name*	缺省情况下，不存在Job

操作	命令	说明
为Job分配命令	**command** *id command*	缺省情况下，没有为Job分配命令 多次执行该命令可以为Job分配多条命令，命令的执行顺序由*id*参数的大小决定，数值小的先执行
退回系统视图	**quit**	-
创建Schedule	**scheduler schedule** *schedule-name*	缺省情况下，不存在Schedule
为Schedule分配Job	**job** *job-name*	缺省情况下，没有为Schedule分配Job 多次执行该命令可以为Schedule分配多个Job，各个Job之间并发执行
配置执行Schedule的定时任务时使用的用户角色	**user-role** *role-name*	缺省情况下，Schedule执行定时任务时使用的用户角色，为创建该Schedule的用户的用户角色 多次执行本命令可给Schedule配置多个用户角色，系统会使用这些用户角色权限的并集去执行Schedule。同一个Schedule最多可以配置64个用户角色
配置在指定时刻执行Schedule	**time at** *time date*	三者选其一 缺省情况下，没有为Schedule配置执行时间 使用该方式配置定时执行功能后，即便执行**clock datetime**、**clock summer-time**或**clock timezone**命令调整了系统时间，也不会影响该任务的配置
为Schedule配置执行时间	**time once at** *time* [**month-date** *month-day* | **week-day** *week-day*&<1-7>]	
配置延迟执行Schedule的时间	**time once delay** *time*	

表1-8 配置定时执行任务（循环执行）

操作	命令	说明
进入系统视图	**system-view**	-
创建Job	**scheduler job** *job-name*	缺省情况下，没有创建Job
为Job分配命令	**command** *id command*	缺省情况下，没有为Job分配命令 多次执行该命令可以为Job分配多条命令，命令的执行顺序由*id*参数的大小决定，数值小的先执行
创建Schedule	**scheduler schedule** *schedule-name*	缺省情况下，未创建Schedule
为Schedule分配Job	**job** *job-name*	缺省情况下，没有为Schedule分配Job 多次执行该命令可以为Schedule分配多个Job。多个Job在Schedule指定的时间同时执行，没有先后顺序
配置执行Schedule的定时任务时使用的用户角色	**user-role** *role-name*	缺省情况下，Schedule执行定时任务时使用的用户角色，为创建该Schedule的用户的用户角色 多次执行本命令可给Schedule配置多个用户角色，系统会使用这些用户角色权限的并集去执行Schedule。同一个Schedule最多可以配置64个用户角色
为Schedule配置	**time repeating at** *time* [**month-date** [*month-day* | **last**] | **week-day**	二者选其一

操作	命令	说明
循环执行时间	*week-day*&<1-7>]	缺省情况下，未配置重复执行Schedule的时间
为Schedule配置循环执行周期	**time repeating** [**at** *time* [*date*]] **interval** *interval*	使用该方式配置定时执行功能后，即便执行**clock datetime**、**clock summer-time**或**clock timezone**命令调整了系统时间，也不会影响该任务的配置

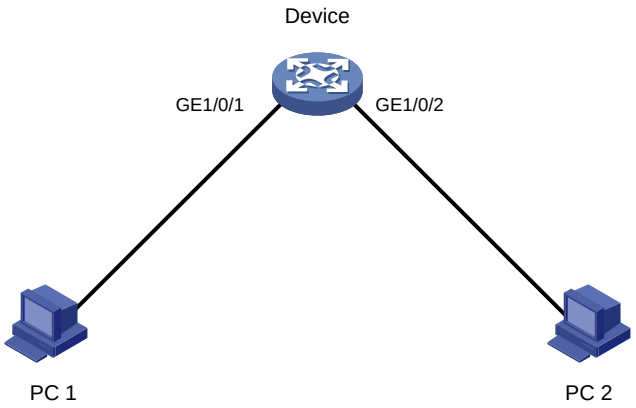
1.7.4 定时执行任务典型配置举例

1. 组网需求

对 Device 进行配置，在星期一到星期五的上午八点到下午十八点开启 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2，其它时间关闭端口，以便起到有效节能的作用。

2. 组网图

图1-1 定时执行任务典型配置举例组网图



3. 配置步骤

进入系统视图。

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

创建关闭 GigabitEthernet1/0/1 的 Job。

```
[Sysname] scheduler job shutdown-GigabitEthernet1/0/1
[Sysname-job-shutdown-GigabitEthernet1/0/1] command 1 system-view
[Sysname-job-shutdown-GigabitEthernet1/0/1] command 2 interface gigabitethernet 1/0/1
[Sysname-job-shutdown-GigabitEthernet1/0/1] command 3 shutdown
[Sysname-job-shutdown-GigabitEthernet1/0/1] quit
```

创建开启 GigabitEthernet1/0/1 的 Job。

```
[Sysname] scheduler job start-GigabitEthernet1/0/1
[Sysname-job-start-GigabitEthernet1/0/1] command 1 system-view
[Sysname-job-start-GigabitEthernet1/0/1] command 2 interface gigabitethernet 1/0/1
[Sysname-job-start-GigabitEthernet1/0/1] command 3 undo shutdown
[Sysname-job-start-GigabitEthernet1/0/1] quit
```

创建关闭 GigabitEthernet1/0/2 的 Job。

```
[Sysname] scheduler job shutdown-GigabitEthernet1/0/2
```

```
[Sysname-job-shutdown-GigabitEthernet1/0/2] command 1 system-view
[Sysname-job-shutdown-GigabitEthernet1/0/2] command 2 interface gigabitethernet 1/0/2
[Sysname-job-shutdown-GigabitEthernet1/0/2] command 3 shutdown
[Sysname-job-shutdown-GigabitEthernet1/0/2] quit
```

创建开启 GigabitEthernet1/0/2 的 Job。

```
[Sysname] scheduler job start-GigabitEthernet1/0/2
[Sysname-job-start-GigabitEthernet1/0/2] command 1 system-view
[Sysname-job-start-GigabitEthernet1/0/2] command 2 interface gigabitethernet 1/0/2
[Sysname-job-start-GigabitEthernet1/0/2] command 3 undo shutdown
[Sysname-job-start-GigabitEthernet1/0/2] quit
```

配置定时执行任务，使 Device 在星期一到星期五的上午八点开启 pc1、pc2 对应的以太网端口。

```
[Sysname] scheduler schedule START-pc1/pc2
[Sysname-schedule-START-pc1/pc2] job start-GigabitEthernet1/0/1
[Sysname-schedule-START-pc1/pc2] job start-GigabitEthernet1/0/2
[Sysname-schedule-START-pc1/pc2] time repeating at 8:00 week-day mon tue wed thu fri
[Sysname-schedule-START-pc1/pc2] quit
```

配置定时执行任务，使 Device 在星期一到星期五的下午十八点关闭 pc1、pc2 对应的以太网端口。

```
[Sysname] scheduler schedule STOP-pc1/pc2
[Sysname-schedule-STOP-pc1/pc2] job shutdown-GigabitEthernet1/0/1
[Sysname-schedule-STOP-pc1/pc2] job shutdown-GigabitEthernet1/0/2
[Sysname-schedule-STOP-pc1/pc2] time repeating at 18:00 week-day mon tue wed thu fri
[Sysname-schedule-STOP-pc1/pc2] quit
```

4. 结果验证

显示 Job 的配置信息。

```
[Sysname] display scheduler job
Job name: shutdown-GigabitEthernet1/0/1
 system-view
 interface gigabitethernet 1/0/1
 shutdown

Job name: shutdown-GigabitEthernet1/0/2
 system-view
 interface gigabitethernet 1/0/2
 shutdown

Job name: start-GigabitEthernet1/0/1
 system-view
 interface GigabitEthernet 1/0/1
 undo shutdown

Job name: start-GigabitEthernet1/0/2
 system-view
 interface gigabitethernet 1/0/2
 undo shutdown
```

显示定时任务的运行信息。

```
[Sysname] display scheduler schedule
Schedule name        : START-pc1/pc2
```

```
Schedule type        : Run on every Mon Tue Wed Thu Fri at 08:00:00
Start time           : Wed May 28 08:00:00 2016
Last execution time  : Wed May 28 08:00:00 2016
Last completion time : Wed May 28 08:00:03 2016
Execution counts     : 1
-----------------------------------------------------------------------
Job name                                        Last execution status
start-GigabitEthernet1/0/1                              Successful
start-GigabitEthernet1/0/2                              Successful

Schedule name        : STOP-pc1/pc2
Schedule type        : Run on every Mon Tue Wed Thu Fri at 18:00:00
Start time           : Wed May 28 18:00:00 2016
Last execution time  : Wed May 28 18:00:00 2016
Last completion time : Wed May 28 18:00:01 2016
Execution counts     : 1
-----------------------------------------------------------------------
Job name                                        Last execution status
shutdown-GigabitEthernet1/0/1                           Successful
shutdown-GigabitEthernet1/0/2                           Successful
```

显示 Job 运行的输出信息。

```
[Sysname] display scheduler logfile
Job name        : start-GigabitEthernet1/0/1
Schedule name   : START-pc1/pc2
Execution time  : Wed May 28 08:00:00 2016
Completion time : Wed May 28 08:00:02 2016
--------------------------------- Job output ---------------------------------
<Sysname>system-view
System View: return to User View with Ctrl+Z.
[Sysname]interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1]undo shutdown

Job name        : start-GigabitEthernet1/0/2
Schedule name   : START-pc1/pc2
Execution time  : Wed May 28 08:00:00 2016
Completion time : Wed May 28 08:00:02 2016
--------------------------------- Job output ---------------------------------
<Sysname>system-view
System View: return to User View with Ctrl+Z.
[Sysname]interface gigabitethernet 1/0/2.
[Sysname-GigabitEthernet1/0/2]undo shutdown

Job name        : shutdown-GigabitEthernet1/0/1
Schedule name   : STOP-pc1/pc2
Execution time  : Wed May 28 18:00:00 2016
Completion time : Wed May 28 18:00:01 2016
--------------------------------- Job output ---------------------------------
<Sysname>system-view
```

```
System View: return to User View with Ctrl+Z.
[Sysname]interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1]shutdown

Job name        : shutdown-GigabitEthernet1/0/2
Schedule name   : STOP-pc1/pc2
Execution time  : Wed May 28 18:00:00 2016
Completion time : Wed May 28 18:00:01 2016
--------------------------------- Job output ---------------------------------
<Sysname>system-view
System View: return to User View with Ctrl+Z.
[Sysname]interface gigabitethernet 1/0/2
[Sysname-GigabitEthernet1/0/2]shutdown
```

1.8 配置密码恢复功能

配置密码恢复功能后，当用户忘记 Console 口认证密码或者登录认证失败，导致无法使用 Console 口登录设备时，可通过 Console 口连接设备，硬件重启设备，并在启动过程中根据提示按<Ctrl+B>进入 Boot ROM 菜单，再选择对应的 Boot ROM 菜单选项来修复这个问题。关闭密码恢复功能后，设备将处于一个安全性更高的状态，即当出现上述情况时，若想继续使用 Console 口登录设备，只能通过 Boot ROM 菜单选择将设备恢复为出厂配置之后方可继续操作，这样可以有效地防止非法用户获取启动配置文件。

Boot ROM 菜单的详见介绍，请参见产品的版本说明书。

表1-9 配置密码恢复功能

操作	命令	说明
进入系统视图	**system-view**	-
使能密码恢复功能	**password-recovery enable**	缺省情况下，密码恢复功能处于使能状态

1.9 电源管理

设备各款型对于本节所描述的特性的支持情况有所不同，详细差异信息如下：

型号	特性	描述
MSR810/810-W/810-W-DB/810-LM/810-W-LM/810-10-PoE/810-LM-HK/810-W-LM-HK/810-LMS/810-LUS	电源管理	不支持
MSR2600-6-X1/2600-10-X1		不支持
MSR 2630		不支持
MSR3600-28/3600-51		不支持
MSR3600-28-SI/3600-51-SI		不支持
MSR3610-X1/3610-X1-DP/3610-X1-DC/3610-X1-DP-DC		不支持
MSR 3610/3620/3620-DP/3640/3660		不支持

型号	特性	描述
MSR5620/5660/5680		支持

型号	特性	描述
MSR810-W-WiNet/810-LM-WiNet	电源管理	不支持
MSR830-4LM-WiNet		不支持
MSR830-5BEI-WiNet/830-6EI-WiNet/830-10BEI-WiNet		不支持
MSR830-6BHI-WiNet/830-10BHI-WiNet		不支持
MSR2600-10-X1-WiNet		不支持
MSR2630-WiNet		不支持
MSR3600-28-WiNet		不支持
MSR3610-X1-WiNet		不支持
MSR3610-WiNet/3620-10-WiNet/3620-DP-WiNet/3620-WiNet/3660-WiNet		不支持

型号	特性	描述
MSR810-LM-GL	电源管理	不支持
MSR810-W-LM-GL		不支持
MSR830-6EI-GL		不支持
MSR830-10EI-GL		不支持
MSR830-6HI-GL		不支持
MSR830-10HI-GL		不支持
MSR2600-6-X1-GL		不支持
MSR3600-28-SI-GL		不支持

某些电源模块发生过载、过流、过压、过温、短路等故障时，会进行自我硬件保护，比如：当电源由于输出过压而告警时，电源可能进入锁死状态、停止对整个机框进行供电，以便保护电源和设备不被损坏。这样虽然保护了电源和设备的安全使用，但会对设备的正常使用造成一定的影响，严重时将导致业务全部中断。为了尽可能减小这种影响，用户可使用电源管理功能，来尽可能的避免电源模块过载现象的发生。

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

用户可通过以下方法来加强电源模块的管理：

- 配置冗余电源，给设备预留功率。
- 手工给单板供电/断电，避免过载现象的发生。

1.9.1 配置冗余电源

注意

设备支持多种类型的电源模块，为了设备和电源的稳定，请使用相同类型的电源模块，不要将 AC 电源和 DC 电源混插。

冗余电源技术通过部署多余的电源模块，来避免电源过载。比如，设备至少需要 N 个电源才能运行，我们通常会给设备配备 M（M 大于 N）个电源，多余的（M-N）个电源可配置为冗余电源。正常情况下，这 M 个电源负载均衡，共同为设备输出功率。当其中某个电源故障时，其余电源能立即接管其工作，从而避免发生电源过载，这就是电源的冗余备份。

配置冗余电源后，如果有接口板插入，系统会先比较待上电接口板的最大功耗和系统的剩余功率：

- 当最大功耗小于等于剩余功率时，直接给接口板供电。
- 当最大功耗大于剩余功率时，不会给接口板供电，接口板不能启动。此时，可增加电源模块，或者减少冗余电源的数量。

表1-10 配置冗余电源（分布式设备－独立运行模式）

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

表1-11 配置冗余电源（分布式设备－IRF 模式）

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

1.9.2 手工给单板供电与断电

当系统供电不足时，设备会根据单板的供电优先级自动对单板供电，用户也可以通过 **display power-supply** 命令随时了解电源的使用情况以及各单板的供电情况，再结合网络业务情况，手工对单板进行供电和断电操作，来调节系统可用功率。

表1-12 手工给单板供电/断电（分布式设备－独立运行模式）

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

表1-13 手工给单板供电/断电（分布式设备－IRF 模式）

操作	命令	说明
手工给指定单板供电	**power-supply on chassis** *chassis-number* **slot** *slot-number* [**subslot** *subslot-number*]	本命令在用户视图下执行
强制给指定单板断电	**power-supply off chassis** *chassis-number* **slot** *slot-number* [**subslot** *subslot-number*]	本命令在用户视图下执行 在IRF中，当成员设备上处于up状态的IRF物理端口都位于同一接口板上时，则不允许强制给该接口板断电，以免导致IRF分裂

1.10 配置端口状态检测定时器

某些协议模块（比如 STP 等）在特定情况下会自动关闭某个端口。此时，可以配置一个端口状态检测定时器。当定时器超时，如果该端口仍处于关闭状态，则协议模块会自动取消关闭动作，使端口恢复到真实的物理状态。

表1-14 配置端口状态检测定时器

操作	命令	说明
进入系统视图	**system-view**	-
配置端口状态检测定时器的时长	**shutdown-interval** *time*	缺省情况下，端口状态检测定时器时长为30秒

1.11 监控CPU利用率

系统每隔 1 分钟会对 CPU 的利用率进行采样，并将采样值和用户配置的 CPU 利用率阈值比较。当采样值大时，则认为 CPU 利用率过高，设备会发送 Trap 报文，并通知业务模块进行相应处理。

开启 CPU 利用率历史记录功能后，系统会每隔一定时间（可通过 **monitor cpu-usage interval** 命令配置）对 CPU 的利用率进行采样，并把采样结果保存到历史记录区。这些记录可通过 **display cpu-usage history** 命令查看，以便用户监控设备近期的运行情况。

系统每隔 1 分钟会对 CPU 核的利用率进行采样，并将采样值和用户配置的 CPU 核利用率阈值比较，当采样值大于或等于 CPU 核利用率阈值时，则认为 CPU 核利用率过高，设备会生成日志信息。

表1-15 监控 CPU 利用率（集中式设备—独立运行模式）

操作	命令	说明
进入系统视图	**system-view**	-
配置CPU利用率阈值	**monitor cpu-usage threshold** *cpu-threshold*	缺省情况下，CPU利用率阈值为99%
开启CPU利用率历史记录功能	**monitor cpu-usage enable**	缺省情况下，CPU使用率历史记录功能处于开启状态
配置CPU利用率历史记录的采样周期	**monitor cpu-usage interval** *interval*	缺省情况下，CPU使用率历史记录采样周期为1分钟
退回用户视图	**quit**	-
显示CPU利用率的统计信息	**display cpu-usage** [**summary**]	该命令在任意视图下执行
显示CPU利用率历史信息记录功能相关配置	**display cpu-usage configuration**	该命令在任意视图下执行
以图表方式显示CPU利用率的历史记录	**display cpu-usage history** [**job** *job-id*]	该命令在任意视图下执行

表1-16 监控 CPU 利用率（分布式设备－独立运行模式/集中式设备—IRF 模式）

操作	命令	说明
进入系统视图	**system-view**	-
开启CPU利用率历史记录功能	**monitor cpu-usage enable** [**slot** *slot-number* [**cpu** *cpu-number*]]	缺省情况下，CPU使用率历史记录功能处于开启状态
配置CPU利用率历史记录的采样周期	**monitor cpu-usage interval** *interval* [**slot** *slot-number* [**cpu** *cpu-number*]]	缺省情况下，CPU使用率历史记录采样周期为1分钟
配置CPU利用率阈值	**monitor cpu-usage threshold** *cpu-threshold* [**slot** *slot-number* [**cpu** *cpu-number*]]	缺省情况下，CPU利用率阈值为99%
退回用户视图	**quit**	-
显示CPU利用率的统计信息	**display cpu-usage** [**summary**] [**slot** *slot-number* [**cpu** *cpu-number*]]	该命令在任意视图下执行
显示CPU利用率历史信息记录功能相关配置	**display cpu-usage configuration** [**slot** *slot-number* [**cpu** *cpu-number*]]	该命令在任意视图下执行
以图表方式显示CPU利用率的历史记录	**display cpu-usage history** [**job** *job-id*] [**slot** *slot-number* [**cpu** *cpu-number*]]	该命令在任意视图下执行

表1-17 监控 CPU 利用率（分布式设备－IRF 模式）

操作	命令	说明
进入系统视图	**system-view**	-
开启CPU利用率历史记录功能	**monitor cpu-usage enable** [**chassis** *chassis-number* **slot** *slot-number* [**cpu** *cpu-number*]]	缺省情况下，CPU使用率历史记录功能处于开启状态

操作	命令	说明
配置CPU利用率历史记录的采样周期	**monitor cpu-usage interval** *interval* [**chassis** *chassis-number* **slot** *slot-number* [**cpu** *cpu-number*]]	缺省情况下，CPU使用率历史记录采样周期为1分钟
配置CPU利用率阈值	**monitor cpu-usage threshold** *cpu-threshold* [**chassis** *chassis-number* **slot** *slot-number* [**cpu** *cpu-number*]]	缺省情况下，CPU利用率阈值为99%
退回用户视图	**quit**	-
显示CPU利用率的统计信息	**display cpu-usage** [**summary**] [**chassis** *chassis-number* **slot** *slot-number* [**cpu** *cpu-number*]]	该命令在任意视图下执行
显示CPU利用率历史信息记录功能相关配置	**display cpu-usage configuration** [**chassis** *chassis-number* **slot** *slot-number* [**cpu** *cpu-number*]]	该命令在任意视图下执行
以图表方式显示CPU利用率的历史记录	**display cpu-usage history** [**job** *job-id*] [**chassis** *chassis-number* **slot** *slot-number* [**cpu** *cpu-number*]]	该命令在任意视图下执行

1.12 配置内存告警门限

系统每隔 1 分钟会对内存利用率进行采样，并将采样值和用户配置的内存利用率阈值比较。当采样值大时，则认为内存利用率过高，设备会发送 Trap 报文。

同时系统还会实时监控系统剩余空闲内存大小，当条件达到时，就产生相应的告警/告警解除通知，以便通知关联的业务模块/进程采取相应的措施，以便最大限度的利用内存，又能保证设备的正常运行。

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

- 当系统剩余空闲内存第一次小于等于一级告警门限时，产生一级告警；
- 当系统剩余空闲内存第一次小于等于二级告警门限时，产生二级告警；
- 当系统剩余空闲内存第一次小于等于三级告警门限时，产生三级告警。
- 当系统剩余空闲内存大于等于二级告警门限时，产生三级告警解除通知；
- 当系统剩余空闲内存大于等于一级告警门限时，产生二级告警解除通知；
- 当系统剩余空闲内存大于等于正常内存大小时，产生一级告警解除通知。

同一级别的告警/告警解除通知是交替进行的：当系统剩余空闲内存小于等于某级告警门限，设备产生相应级别的告警，后续只有该告警解除了，系统剩余空闲内存再次小于等于某级告警门限时，才会再次生成该级别的告警。

当系统的剩余空闲内存大小如图 1-2 中曲线所示时，会生成如图 1-2 所示的告警和解除告警通知。

图1-2 内存告警示意图

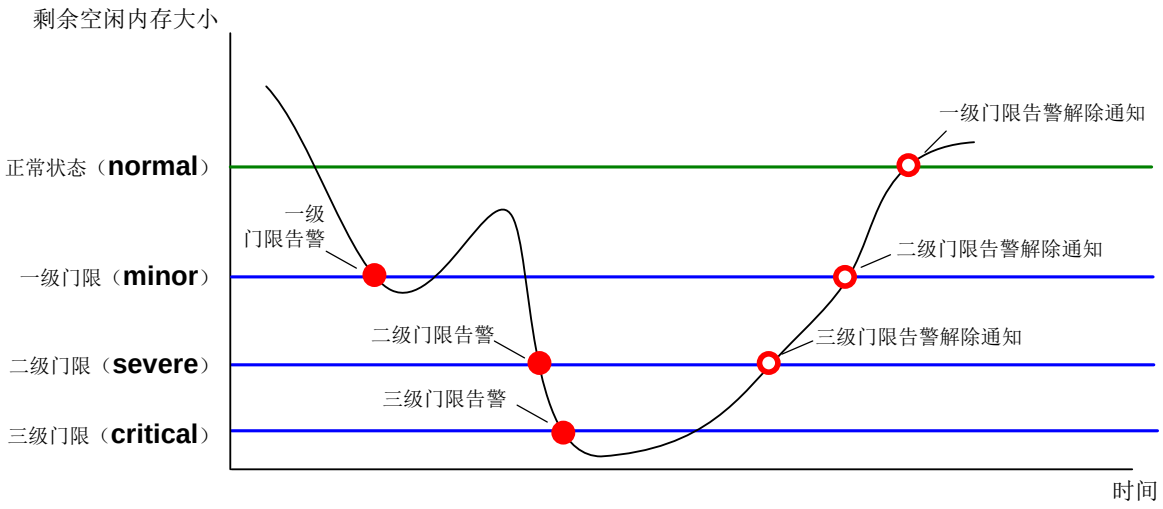


表1-18 配置内存告警门限

操作	命令	说明
进入系统视图	**system-view**	-
配置内存利用率阈值（集中式设备—独立运行模式）	**memory-threshold usage** *memory-threshold*	缺省情况下，内存利用率阈值为100%
配置空闲内存告警的门限值（集中式设备—独立运行模式）	**memory-threshold minor** *minor-value* **severe** *severe-value* **critical** *critical-value* **normal** *normal-value*	缺省情况下，不同设备的空闲内存告警的门限值可能不同，请先使用**undo memory-threshold**命令恢复缺省情况后，再通过**display memory-threshold**命令查看设备的缺省空闲内存告警门限值
配置内存利用率阈值（分布式设备—独立运行模式/集中式设备—IRF模式）	**memory-threshold** [**slot** *slot-number* [**cpu** *cpu-number*]] **usage** *memory-threshold*	缺省情况下，内存利用率阈值为100%
配置空闲内存告警的门限值（分布式设备—独立运行模式/集中式设备—IRF模式）	**memory-threshold** [**slot** *slot-number* [**cpu** *cpu-number*]] **minor** *minor-value* **severe** *severe-value* **critical** *critical-value* **normal** *normal-value*	缺省情况下，不同设备的空闲内存告警的门限值可能不同，请先使用**undo memory-threshold**命令恢复缺省情况后，再通过**display memory-threshold**命令查看设备的缺省空闲内存告警门限值
配置内存利用率阈值（分布式设备—IRF模式）	**memory-threshold** [**chassis** *chassis-number* **slot** *slot-number* [**cpu** *cpu-number*]] **usage** *memory-threshold*	缺省情况下，内存利用率阈值为100%
配置空闲内存告警的门限值（分布式设备—IRF模式）	**memory-threshold** [**chassis** *chassis-number* **slot** *slot-number* [**cpu** *cpu-number*]] **minor** *minor-value* **severe** *severe-value* **critical** *critical-value* **normal** *normal-value*	缺省情况下，不同设备的空闲内存告警的门限值可能不同，请先使用**undo memory-threshold**命令恢复缺省情况后，再通过**display memory-threshold**命令查看设备的缺省空闲内存告警门限值

1.13 关闭USB接口

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

表1-19 关闭 USB 接口

操作	命令	说明
进入系统视图	**system-view**	-
关闭设备上所有的USB接口	**usb disable**	缺省情况下，设备上所有的USB接口处于开启状态 在执行**usb disable**命令前，请先使用**umount**命令卸载所有USB文件系统，否则命令执行失败。有关**umount**命令的详细介绍，请参见“基础配置命令参考”中的“文件系统管理”

1.14 配置接口卡的工作模式

设备各款型对于本节所描述的特性的支持情况有所不同，详细差异信息如下：

型号	特性	描述
MSR810/810-W/810-W-DB/810-LM/810-W-LM/810-10-PoE/810-LM-HK/810-W-LM-HK/810-LMS/810-LUS	配置接口卡的工作模式	不支持
MSR2600-6-X1/2600-10-X1		支持
MSR 2630		支持
MSR3600-28/3600-51		支持
MSR3600-28-SI/3600-51-SI		支持
MSR3610-X1/3610-X1-DP/3610-X1-DC/3610-X1-DP-DC		支持
MSR 3610/3620/3620-DP/3640/3660		支持
MSR5620/5660/5680		支持

型号	特性	描述
MSR810-W-WiNet/810-LM-WiNet	配置接口卡的工作模式	不支持
MSR830-4LM-WiNet		不支持
MSR830-5BEI-WiNet/830-6EI-WiNet/830-10BEI-WiNet		不支持
MSR830-6BHI-WiNet/830-10BHI-WiNet		不支持
MSR2600-10-X1-WiNet		支持
MSR2630-WiNet		支持
MSR3600-28-WiNet		支持
MSR3610-X1-WiNet		支持

型号	特性	描述
MSR3610-WiNet/3620-10-WiNet/3620-DP-WiNet/3620-WiNet/3660-WiNet		支持

型号	特性	描述
MSR810-LM-GL	配置接口卡的工作模式	不支持
MSR810-W-LM-GL		不支持
MSR830-6EI-GL		不支持
MSR830-10EI-GL		不支持
MSR830-6HI-GL		不支持
MSR830-10HI-GL		不支持
MSR2600-6-X1-GL		支持
MSR3600-28-SI-GL		支持

注意

模式切换后是必须重启设备或热插拔接口卡（如果接口卡支持热插拔），新配置的模式才会生效。

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

表1-20 □配置接口卡的工作模式（集中式设备—独立运行模式）

操作	命令	说明
进入系统视图	**system-view**	-
（可选）配置接口卡的工作模式	**card-mode slot** *slot-number mode-name*	-

表1-21 配置接口卡的工作模式（分布式设备－独立运行模式/集中式设备—IRF 模式）

操作	命令	说明
进入系统视图	**system-view**	-
（可选）配置接口卡的工作模式	**card-mode slot** *slot-number* **subslot** *subslot-number mode-name*	-

表1-22 配置接口卡的工作模式（分布式设备－IRF 模式）

操作	命令	说明
进入系统视图	**system-view**	-

操作	命令	说明
（可选）配置接口卡的工作模式	**card-mode chassis** *chassis-number* **slot** *slot-number* **subslot** *subslot-number mode-name*	-

1.15 可插拔接口模块的识别与诊断

1.15.1 识别可插拔接口模块

可以通过显示可插拔接口模块的主要特征参数或者电子标签信息来识别可插拔接口模块。

- 可插拔接口模块的主要特征参数包括：模块型号、连接器类型、发送激光的中心波长、信号的有效传输距离、模块生产厂商名称等信息。
- 电子标签信息也可以称为永久配置数据或档案信息，在单板或者设备的调试、测试过程中被写入到设备的存储器件中，包括单板的名称、生产序列号、MAC 地址、制造商等信息。

另外，当设备上插入的光模块的生产厂商不是 H3C 时，设备会打印 Log 信息提醒用户，要求用户更换成 H3C 的光模块，以便管理和维护光模块。关于 Log 输出规则的配置请参见“网络管理和监控配置指导”中的“信息中心”。

表1-23 识别可插拔接口模块信息

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

1.15.2 诊断可插拔接口模块

系统提供故障告警信息描述了可插拔接口模块的故障来源，以便用户诊断和解决故障。系统还提供了数字诊断功能，其原理是对影响光模块工作的关键参数进行监控（这些关键参数包括：温度、电压、激光偏置电流、发送光功率和接收光功率等），当这些参数的值异常时，用户可以采取相应的措施，预防故障发生。

表1-24 诊断可插拔接口模块

操作	命令	说明
显示可插拔接口模块的当前故障告警信息	**display transceiver alarm interface** [*interface-type interface-number*]	本命令在任意视图下执行
显示可插拔光模块的数字诊断参数的当前测量值	**display transceiver diagnosis interface** [*interface-type interface-number*]	本命令在任意视图下执行

1.16 恢复出厂状态

当设备使用场景更改，或者设备出现故障时，可以使用本特性将设备恢复到出厂状态。

执行本命令时，设备会自动强制重启，以便恢复到出厂状态，请谨慎使用本特性。

表1-25 恢复出厂状态

操作	命令	说明
将设备恢复到出厂状态	**restore factory-default**	执行该命令后，设备会自动强制重启才能使该命令生效 本命令在用户视图下执行

1.17 卸载HMIM接口模块

设备各款型对于本节所描述的特性的支持情况有所不同，详细差异信息如下：

型号	特性	描述
MSR810/810-W/810-W-DB/810-LM/810-W-LM/810-10-PoE/810-LM-HK/810-W-LM-HK/810-LMS/810-LUS	卸载HMIM接口模块	不支持
MSR2600-6-X1/2600-10-X1		• MSR2600-6-X1：支持 • MSR2600-10-X1：不支持
MSR 2630		不支持
MSR3600-28/3600-51		不支持
MSR3600-28-SI/3600-51-SI		不支持
MSR3610-X1/3610-X1-DP/3610-X1-DC/3610-X1-DP-DC		支持
MSR 3610/3620/3620-DP/3640/3660		支持
MSR5620/5660/5680		支持

型号	特性	描述
MSR810-W-WiNet/810-LM-WiNet	卸载HMIM接口模块	不支持
MSR830-4LM-WiNet		不支持
MSR830-5BEI-WiNet/830-6EI-WiNet/830-10BEI-WiNet		不支持
MSR830-6BHI-WiNet/830-10BHI-WiNet		不支持
MSR2600-10-X1-WiNet		不支持
MSR2630-WiNet		不支持
MSR3600-28-WiNet		不支持
MSR3610-X1-WiNet		支持
MSR3610-WiNet/3620-10-WiNet/3620-DP-WiNet/3620-WiNet/3660-WiNet		支持

型号	特性	描述
MSR810-LM-GL	卸载HMIM接口模块	不支持
MSR810-W-LM-GL		不支持
MSR830-6EI-GL		不支持
MSR830-10EI-GL		不支持
MSR830-6HI-GL		不支持
MSR830-10HI-GL		不支持
MSR2600-6-X1-GL		支持
MSR3600-28-SI-GL		不支持

对于支持热插拔功能的设备，在运行状态下直接拔出 HMIM 接口模块时，必须先使用 **remove** 命令从系统中卸载掉 HMIM 接口模块，否则可能会引起设备故障或损坏。

注意

- 该命令会使接口模块不可用，从而导致业务中断，请谨慎使用。
- **remove** 接口模块后，接口不可见，不可配置。

表1-26 卸载 HMIM 接口模块

操作	命令	说明
卸载HMIM接口模块（集中式设备—独立运行模式）	**remove subslot** *subslot-number*	本命令在用户视图下执行
卸载HMIM接口模块（集中式设备—IRF模式/分布式设备—独立运行模式）	**remove slot** *slot-number* **subslot** *subslot-number*	本命令在用户视图下执行
卸载HMIM接口模块（分布式设备－IRF模式）	**remove chassis** *chassis-number* **slot** *slot-number* **subslot** *subslot-number*	本命令在用户视图下执行

1.18 通过FoTA方式升级Modem的固件版本

说明

本命令仅 MSR810-LMS、MSR810-LUS 及安装了 SIC-D4G-CNED 卡或 SIC-4G-CNED 卡的设备支持。

设备进行 FoTA 升级时，会影响业务传输，并且会消耗 SIM 卡流量，请谨慎操作。

操作	命令	说明
进入系统视图	**system-view**	-
进入Cellular接口视图	**controller cellular** *cellular-number*	-
通过FoTA方式升级Modem的固件版本	**firmware update fota**	-

1.19 配置PTP加速功能

设备各款型对于本节所描述的特性的支持情况有所不同，详细差异信息如下：

型号	特性	描述
MSR810/810-W/810-W-DB/810-LM/810-W-LM/810-10-PoE/810-LM-HK/810-W-LM-HK/810-LMS/810-LUS	PTP加速功能	不支持
MSR2600-6-X1/2600-10-X1		• MSR2600-6-X1：支持 • MSR2600-10-X1：不支持
MSR 2630		不支持
MSR3600-28/3600-51		不支持
MSR3600-28-SI/3600-51-SI/3610-I-DP/3610-IE-DP		不支持
MSR3610-X1/3610-X1-DP/3610-X1-DC/3610-X1-DP-DC		• MSR3610-X1：支持 • MSR3610-X1-DP/3610-X1-DC/3610-X1-DP-DC：不支持
MSR 3610/3620/3620-DP/3640/3660		• MSR 3610/3620/3620-DP/3660：不支持 • MSR3640：支持
MSR5620/5660/5680		不支持

型号	特性	描述
MSR810-W-WiNet/810-LM-WiNet	PTP加速功能	不支持
MSR830-4LM-WiNet		不支持
MSR830-5BEI-WiNet/830-6EI-WiNet/830-10BEI-WiNet		不支持
MSR830-6BHI-WiNet/830-10BHI-WiNet		不支持
MSR2600-10-X1-WiNet		不支持
MSR2630-WiNet		不支持
MSR3600-28-WiNet		不支持
MSR3610-X1-WiNet		支持
MSR3610-WiNet/3620-10-WiNet/3620-DP-WiNet/3620-		不支持

型号	特性	描述
WiNet/3660-WiNet		

型号	特性	描述
MSR810-LM-GL	PTP加速功能	不支持
MSR810-W-LM-GL		不支持
MSR830-6EI-GL		不支持
MSR830-10EI-GL		不支持
MSR830-6HI-GL		不支持
MSR830-10HI-GL		不支持
MSR2600-6-X1-GL		不支持
MSR3600-28-SI-GL		不支持

说明

开启本命令后会使得设备的 CPU 利用率提高，请谨慎使用。

设备开启 PTP 加速功能后能够加速 PTP 报文转发。开启 PTP 功能后，设备处于对 PTP 报文快速转发状态，可以使报文被快速转发。

表1-27 配置 PTP 加速功能

操作	命令	说明
进入系统视图	**system-view**	-
配置PTP加速功能	**ptp acceleration enable**	缺省情况下，PTP加速功能处于关闭状态

1.20 关闭蓝牙功能

设备各款型对于本节所描述的特性的支持情况有所不同，详细差异信息如下：

型号	特性	描述
MSR810/810-W/810-W-DB/810-LM/810-W-LM/810-10-PoE/810-LM-HK/810-W-LM-HK/810-LMS/810-LUS	关闭蓝牙功能	• MSR810/810-W/810-W-DB/810-LM/810-W-LM/810-10-PoE：支持 • MSR810-LM-HK/810-W-LM-HK/810-LMS/810-LUS：不支持
MSR2600-6-X1/2600-10-X1		• MSR2600-6-X1：不支持 • MSR2600-10-X1：支持
MSR 2630		支持

型号	特性	描述
MSR3600-28/3600-51		不支持
MSR3600-28-SI/3600-51-SI		不支持
MSR3610-X1/3610-X1-DP/3610-X1-DC/3610-X1-DP-DC		支持
MSR 3610/3620/3620-DP/3640/3660		• MSR 3610/3620/3640/3660：不支持 • MSR3620-DP：支持
MSR5620/5660/5680		不支持

型号	特性	描述
MSR810-W-WiNet/810-LM-WiNet	关闭蓝牙功能	支持
MSR830-4LM-WiNet		支持
MSR830-5BEI-WiNet/830-6EI-WiNet/830-10BEI-WiNet		• MSR830-5BEI-WiNet/830-10BEI-WiNet：支持 • MSR830-6EI-WiNet：不支持
MSR830-6BHI-WiNet/830-10BHI-WiNet		支持
MSR2600-10-X1-WiNet		支持
MSR2630-WiNet		支持
MSR3600-28-WiNet		支持
MSR3610-X1-WiNet		支持
MSR3610-WiNet/3620-10-WiNet/3620-DP-WiNet/3620-WiNet/3660-WiNet		支持

型号	特性	描述
MSR810-LM-GL	关闭蓝牙功能	不支持
MSR810-W-LM-GL		不支持
MSR830-6EI-GL		不支持
MSR830-10EI-GL		不支持
MSR830-6HI-GL		不支持
MSR830-10HI-GL		不支持
MSR2600-6-X1-GL		不支持
MSR3600-28-SI-GL		不支持

配置本命令后将关闭设备蓝牙功能，请谨慎使用。

设备关闭蓝牙功能后，将无法通过蓝牙功能进行连接和操作。

表1-28 配置关闭蓝牙功能

操作	命令	说明
进入系统视图	**system-view**	-
关闭蓝牙功能	**bluetooth disable**	缺省情况下，蓝牙功能处于开启状态

1.21 设备管理显示和维护

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

请在用户视图下执行 **reset scheduler logfile** 命令。

表1-29 设备管理显示和维护（集中式设备—独立运行模式）

操作	命令
显示设备的告警信息	**display alarm** [**slot** *slot-number*]
显示系统版本信息	**display version**
显示系统当前的时间、日期、本地时区以及夏令时配置	**display clock**
显示系统软件和硬件的详细版权信息	**display copyright**
显示设备信息	**display device** [**cf-card** | **harddisk** | **sd-card** | **usb**] [**slot** *slot-number* | **verbose**]
显示设备的电子标签信息	**display device manuinfo** [**slot** *slot-number*]
显示指定电源的电子标签信息	**display device manuinfo power** *power-id*
收集诊断信息	**display diagnostic-information** [**hardware** | **infrastructure** | **l2** | **l3** | **service**] [**key-info**] [*filename*]
显示设备的温度信息	**display environment**
显示设备风扇的工作状态	**display fan** [*fan-id* | **verbose**]
显示设备的内存使用状态	**display memory** [**summary**]
显示内存告警门限相关信息	**display memory-threshold**
显示设备电源的信息	**display power-supply** [**verbose**]
显示Job的配置信息	**display scheduler job** [*job-name*]
显示Schedule日志文件的相关信息	**display scheduler logfile**
显示定时重启功能的相关配置	**display scheduler reboot**
显示Schedule的相关信息	**display scheduler schedule** [*schedule-name*]
显示系统的稳定状态	**display system stable state**
显示设备启动软件包版本更新操作的记录	**display version-update-record**

操作	命令
清除Schedule日志文件的相关信息	**reset scheduler logfile**

表1-30 设备管理显示和维护（分布式设备－独立运行模式/集中式设备—IRF 模式）

操作	命令
显示设备的告警信息	**display alarm** [**slot** *slot-number*]
显示业务板管理接口模块流量的工作模式（分布式设备－独立运行模式）	**display card-forwarding-mode**
显示系统版本信息	**display version**
显示系统当前的时间、日期、本地时区以及夏令时配置	**display clock**
显示系统软件和硬件的详细版权信息	**display copyright**
显示设备信息	**display device** [**cf-card** | **harddisk** | **sd-card** | **usb**] [**slot** *slot-number* [**subslot** *subslot-number*] | **verbose**]
显示设备的电子标签信息	**display device manuinfo** [**slot** *slot-number* [**subslot** *subslot-number*]]
显示指定风扇的电子标签信息（集中式设备—IRF模式）	**display device manuinfo slot** *slot-number* **fan** *fan-id*
显示指定电源的电子标签信息（分布式设备－独立运行模式）	**display device manuinfo power** *power-id*
显示指定电源的电子标签信息（集中式设备—IRF模式）	**display device manuinfo slot** *slot-number* **power** *power-id*
显示指定电源监控模块的电子标签信息（集中式设备—IRF模式）	**display device manuinfo slot** *slot-number* **power-monitor** *pm-id*
收集诊断信息	**display diagnostic-information** [**hardware** | **infrastructure** | **l2** | **l3** | **service**] [**key-info**] [*filename*]
显示设备的温度信息	**display environment** [**slot** *slot-number*]
显示设备风扇的工作状态（分布式设备－独立运行模式）	**display fan** [*fan-id*]
显示设备风扇的工作状态（集中式设备—IRF模式）	**display fan** [**slot** *slot-number* [*fan-id*]]
显示设备的内存使用状态	**display memory** [**summary**] [**slot** *slot-number* [**cpu** *cpu-number*]]
显示内存告警门限相关信息	**display memory-threshold** [**slot** *slot-number* [**cpu** *cpu-number*]]
显示设备电源的信息（分布式设备－独立运行模式）	**display power-supply** [**verbose**]
显示设备电源的信息（集中式设备—IRF模式）	**display power-supply** [**slot** *slot-number*] [**verbose**]
显示Job的配置信息	**display scheduler job** [*job-name*]
显示Schedule日志文件的相关信息	**display scheduler logfile**

操作	命令
显示定时重启功能的相关配置	**display scheduler reboot**
显示Schedule的相关信息	**display scheduler schedule** [*schedule-name*]
显示系统的稳定状态	**display system stable state**
显示主用主控板启动软件包版本更新操作的记录（分布式设备－独立运行模式）	**display version-update-record**
显示主设备启动软件包版本更新操作的记录（集中式设备—IRF模式）	**display version-update-record**
清除Schedule日志文件的相关信息	**reset scheduler logfile**

表1-31 设备管理显示和维护（分布式设备－IRF 模式）

操作	命令
显示设备的告警信息	**display alarm** [**chassis** *chassis-number* **slot** *slot-number*]
显示业务板管理接口模块流量的工作模式（分布式设备－独立运行模式）	**display card-forwarding-mode**
显示系统版本信息	**display version**
显示系统当前的时间、日期、本地时区以及夏令时配置	**display clock**
显示系统软件和硬件的详细版权信息	**display copyright**
显示设备信息	**display device** [**cf-card** | **harddisk** | **sd-card** | **usb**] [**chassis** *chassis-number* [**slot** *slot-number* [**subslot** *subslot-number*]] | **verbose**]
显示设备的电子标签信息	**display device manuinfo** [**chassis** *chassis-number* [**slot** *slot-number* [**subslot** *subslot-number*]]]
显示指定风扇的电子标签信息	**display device manuinfo chassis** *chassis-number* **fan** *fan-id*
显示指定电源的电子标签信息	**display device manuinfo chassis** *chassis-number* **power** *power-id*
显示指定电源监控模块的电子标签信息	**display device manuinfo chassis** *chassis-number* **power-monitor** *pm-id*
收集诊断信息	**display diagnostic-information** [**hardware** | **infrastructure** | **l2** | **l3** | **service**] [**key-info**] [*filename*]
显示设备的温度信息	**display environment** [**chassis** *chassis-number* [**slot** *slot-number*]]
显示设备风扇的工作状态	**display fan** [**chassis** *chassis-number* [*fan-id*]]
显示设备的内存使用状态	**display memory** [**summary**] [**chassis** *chassis-number* **slot** *slot-number* [**cpu** *cpu-number*]]
显示内存告警门限相关信息	**display memory-threshold** [**chassis** *chassis-number* **slot** *slot-number* [**cpu** *cpu-number*]]
显示设备电源的信息	**display power-supply** [**chassis** *chassis-number*] [**verbose**]
显示Job的配置信息	**display scheduler job** [*job-name*]

操作	命令
显示Schedule日志文件的相关信息	**display scheduler logfile**
显示定时重启功能的相关配置	**display scheduler reboot**
显示Schedule的相关信息	**display scheduler schedule** [*schedule-name*]
显示系统的稳定状态	**display system stable state**
显示全局主用主控板启动软件包版本更新操作的记录	**display version-update-record**
清除Schedule日志文件的相关信息	**reset scheduler logfile**

目 录

1 Tcl

ComwareV7 系统内嵌了 Tcl（Tool Command Language，工具命令语言）解析器，支持直接在设备上执行 Tcl 脚本命令。

在用户视图下执行 **tclsh** 命令，会进入 Tcl 配置视图。为兼容 Comware 配置方式，在 Tcl 配置视图下，用户可以直接输入 Tcl 脚本命令，也可以输入 Comware 系统的命令。命令输入完成后，直接回车即可执行。

Tcl 配置视图下，支持 Tcl8.5 版本的所有命令。

对于 Comware 系统的命令，Tcl 配置视图相当于用户视图，配置方式同用户视图下的配置。

1.1 通过Tcl脚本配置设备

1.1.1 配置限制和指导

在 Tcl 配置视图下编辑命令时，遵循以下约定：

- 用户需保证输入的 Tcl 脚本命令可以正确执行。由于执行 Tcl 脚本命令过程无法中断，如果用户通过 Telnet/SSH 方式登录设备并执行脚本命令时出现问题，需要关闭当前连接来终止执行过程；如果用户通过 Console 口/AUX 口方式登录设备并执行脚本命令时出现问题，则可以通过重启设备或者通过其他方式登陆设备执行 **free line** 命令断开该 Console/AUX 用户线的连接。因此建议用户通过 Telnet/SSH 方式登录设备并进入 Tcl 视图执行脚本命令。有关 **free line** 命令的详细介绍，请参见“基础配置命令”中的“登录设备”。）
- 在 Tcl 中定义的环境变量可以应用到 Comware 系统的命令。
- Tcl 脚本命令不支持输入“?”键获得在线帮助和 Tab 键补全功能。
- 已经成功执行的 Tcl 脚本命令不会记录在历史命令缓冲区中。
- 通过 Tcl 脚本命令 **read stdin** 进行读取操作时，可以通过<Ctrl+D>结束读取。

1.1.2 通过Tcl脚本配置设备

表1-1 通过 Tcl 脚本配置设备

操作	命令	说明
进入Tcl配置视图	**tclsh**	该命令在用户视图下执行
执行Tcl脚本	*Tcl command*	在该视图下，用户可以根据需求执行对应的Tcl脚本
从Tcl配置视图退回到用户视图	**tclquit**	该命令在Tcl配置视图下执行

说明

在 Tcl 配置视图下执行 **quit** 命令和 **tclquit** 命令都可以退出 Tcl 配置视图，如果在 Tcl 配置视图下使用了 Comware 命令进入了子视图，则只能用 **quit** 命令退回到上一级视图，不能执行 **tclquit** 命令。

1.2 在Tcl配置视图下执行Comware命令

1.2.1 配置限制和指导

在 Tcl 配置视图下执行 Comware 命令时，遵循以下约定：

- 当 Comware 命令配置的字符串被特殊字符""或{}包围时，只有在特殊字符前加上\，该特殊字符才有效。例如，在接口视图下设置描述信息为"a"时，需要执行 **description \"a\"**；如果执行 **description "a"**，配置结果为 **description a**。
- Comware 系统的命令支持输入“?”键获得在线帮助和 Tab 键补全功能。关于输入“?”键获得在线帮助和 Tab 键补全功能的详细描述，请参见“基础配置指导”中的“CLI 配置”。
- **cli** 命令是 Tcl 脚本命令，不支持输入“?”键获得在线帮助和 Tab 键补全功能。
- 已经成功执行的 Comware 系统的命令会记录在历史命令缓冲区中，使用上下光标键可以调用执行过的命令。
- 通过以下三种方式，可以一次执行多条 Comware 命令：
  - 在同一行连续键入多条 Comware 系统的命令，命令间用分号隔开，多条命令会一起下发，按照下发顺序执行。例如 **ospf 100**;**area 0**。
  - 在 **cli** 命令后连续键入需要执行的多条 Comware 命令，每条 Comware 命令之间使用空格加分号进行分隔，在第一条 Comware 命令的前方和最后一条 Comware 命令的后方添加英文格式的双引号。例如 **cli** "**ospf 100** ; **area 0**"。
  - 多次输入 **cli** 命令和 Comware 命令的组合，每组之间使用空格加分号分隔。例如 **cli ospf 100** ; **cli area 0**。

1.2.2 在Tcl配置视图下执行Comware命令

在 Tcl 配置视图下执行 Comware 命令有两种方式：一种是直接在 Tcl 配置视图下直接输入 Comware 命令，如果 Tcl 命令与 Comware 命令的命令字冲突，则执行 Tcl 命令；另一种是在 Comware 命令前添加 **cli** 命令关键字，该方式在 Tcl 命令与 Comware 命令的命令字冲突时能够优先执行 Comware 命令。

表1-2 在 Tcl 配置视图下执行 Comware 命令

操作	命令	说明
进入Tcl配置视图	**tclsh**	-
直接执行Comware命令	*Command*	二者必选其一
通过增加**cli**命令关键字执行Comware命令	**cli** *command*	

目 录

1 Python

设备各款型使用的命令行形式有所不同，详细差异信息如下：

命令行形式	款型
集中式	• MSR810/810-W/810-W-DB/810-LM/810-W-LM/810-10-PoE/810-LM-HK/810-W-LM-HK • MSR810-LMS/810-LUS • MSR2600-6-X1/2600-10-X1/2630 • MSR3600-28/3600-51/3600-28-SI/3600-51-SI • MSR3610-X1/3610-X1-DP/3610-X1-DC/3610-X1-DP-DC • MSR 3610/3620/3620-DP/3640/3660 • MSR810-W-WiNet/810-LM-WiNet/830-4LM-WiNet • MSR830-5BEI-WiNet/830-6EI-WiNet/830-10BEI-WiNet • MSR830-6BHI-WiNet/830-10BHI-WiNet • MSR2600-10-X1-WiNet/2630-WiNet • MSR3600-28-WiNet/3610-X1-WiNet • MSR3610-WiNet/3620-10-WiNet/3620-DP-WiNet/3620-WiNet/3660-WiNet • MSR810-LM-GL/810-W-LM-GL • MSR830-6EI-GL/830-10EI-GL/830-6HI-GL/830-10HI-GL • MSR2600-6-X1-GL/3600-28-SI-GL
分布式	MSR5620/5660/5680

设备各款型对于本手册所描述的特性支持情况有所不同，详细差异信息如下：

型号	特性	描述
MSR810/810-W/810-W-DB/810-LM/810-W-LM/810-10-PoE/810-LM-HK/810-W-LM-HK/810-LMS/810-LUS	Python	MSR810/810-W/810-W-DB/810-LM/810-W-LM/810-10-PoE/810-LM-HK/810-W-LM-HK：支持 MSR810-LMS/810-LUS：不支持
MSR2600-6-X1/2600-10-X1		支持
MSR 2630		支持
MSR3600-28/3600-51		支持
MSR3600-28-SI/3600-51-SI		不支持
MSR3610-X1/3610-X1-DP/3610-X1-DC/3610-X1-DP-DC		支持
MSR 3610/3620/3620-DP/3640/3660		支持
MSR5620/5660/5680		支持

型号	特性	描述
MSR810-W-WiNet/810-LM-WiNet	Python	支持

型号	特性	描述
MSR830-4LM-WiNet		支持
MSR830-5BEI-WiNet/830-6EI-WiNet/830-10BEI-WiNet		支持
MSR830-6BHI-WiNet/830-10BHI-WiNet		支持
MSR2600-10-X1-WiNet		支持
MSR2630-WiNet		支持
MSR3600-28-WiNet		支持
MSR3610-X1-WiNet		支持
MSR3610-WiNet/3620-10-WiNet/3620-DP-WiNet/3620-WiNet/3660-WiNet		支持

型号	特性	描述
MSR810-LM-GL	Python	支持
MSR810-W-LM-GL		支持
MSR830-6EI-GL		支持
MSR830-10EI-GL		支持
MSR830-6HI-GL		支持
MSR830-10HI-GL		支持
MSR2600-6-X1-GL		支持
MSR3600-28-SI-GL		不支持

Python 是一种简单易学，功能强大的编程语言，它有高效率的高层数据结构，简单而有效地实现了面向对象编程。Python 简洁的语法和对动态输入的支持，再加上解释性语言的本质，使得它在大多数平台上的许多领域都是一个理想的脚本语言，特别适用于快速的应用程序开发。

Comware V7 系统内嵌了 Python 解释器，可以直接在设备上使用 Python2.7 版本的命令和标准 API。为了方便用户进行系统配置，Comware 对 Python 进行了扩展，用户可以使用这些扩展功能。关于 Comware 的 Python 扩展，可以参考“2 附录：Comware Python API”。

1.1 通过Python配置设备

Comware V7 系统内嵌了 Python 解释器。用户可以进入 Python shell，使用 Python 的命令、标准 API 和扩展 API；还可以直接在设备上执行 Python 脚本，以方便自动化配置系统。

1.1.1 进入Python shell

表1-1 进入 Python shell

操作	命令	说明
进入Python shell	**python**	该命令在用户视图下执行

1.1.2 执行Python脚本文件

表1-2 执行 Python 脚本文件

操作	命令	说明
执行Python脚本文件	**python** *filename*	该命令在用户视图下执行

1.2 Python典型配置举例

1. 组网需求

使用 Python 脚本，下载 main.cfg 和 backup.cfg 两个配置文件到设备上，并设置为下次主用配置文件和备用配置文件。

2. 组网图

图1-1 Python 典型配置举例组网图

3. 配置步骤

在 PC 上使用写字板编辑 Python 脚本文件 test.py，内容如下：

```
#!usr/bin/python
import comware

comware.Transfer('tftp', '192.168.1.26', 'main.cfg', 'flash:/main.cfg')
comware.Transfer('tftp', '192.168.1.26', 'backup.cfg', 'flash:/backup.cfg')
comware.CLI('startup saved-configuration flash:/main.cfg main ;startup saved-configuration
flash:/backup.cfg backup')
```

通过 TFTP 将 test.py 文件下载到设备上

```
<Sysname> tftp 192.168.1.26 get test.py
```

执行 Python 脚本文件

```
<Sysname> python flash:/test.py
<Sysname> startup saved-configuration flash:/main.cfg main
Please wait..... Done.
```

```
<Sysname> startup saved-configuration flash:/backup.cfg backup
Please wait...... Done.
```

4. 验证结果

使用 **display startup** 命令查看下次启动文件已经变为 main.cfg 和 backup.cfg。

```
<Sysname> display startup
 Current startup saved-configuration file: flash:/startup.cfg
 Next main startup saved-configuration file: flash:/main.cfg
 Next backup startup saved-configuration file: flash:/backup.cfg
```

2 附录：Comware Python API

本文描述在 Comware V7 中提供的扩展 Python API，扩展 Python API 必须遵循标准 Python 语言语法。在使用扩展 Python API 时，必须先导入 Comware 包，导入方法有两种：

- 方法一：用 import comware 引入整个 Comware 包，在执行具体 API 的时候用 comware.*API*。例如，下面的举例表示：使用 API Transfer 将 TFTP 服务器（192.168.1.26）上的文件 test.cfg 下载到设备上。

```
<Sysname> python
Python 2.7.3 (default)
[GCC 4.4.1] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> import comware
>>> comware.Transfer('tftp', '192.168.1.26', 'test.cfg', 'flash:/test.cfg', user='',
password='')
<comware.Transfer object at 0xb7eab0e0>
```

- 方法二：用 from comware import *API* 引入单个 API。例如，下面的举例表示：使用 API Transfer 将 TFTP 服务器（192.168.1.26）上的文件 test.cfg 下载到设备上。

```
<Sysname> python
Python 2.7.3 (default)
[GCC 4.4.1] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> from comware import Transfer
>>> Transfer('tftp', '192.168.1.26', 'test.cfg', 'flash:/test.cfg', user='', password='')
<comware.Transfer object at 0xb7e5e0e0>
```

2.1 CLI类

2.1.1 CLI

用来执行 Comware V7 系统的命令并创建 CLI 对象。

【命令】

CLI(*command*='', *do_print*=True)

【参数】

command：表示要下发的命令，缺省为空。多条命令之间以空格加分号分隔，如'system-view ;local-user test class manage'。

do_print：表示是否输出执行结果，True 表示输出执行结果，False 表示不输出执行结果。缺省值为 True。

【返回值】

CLI 对象

【使用指导】

需要注意下发命令是从用户视图开始，如果需要在其它视图下下发命令，需要首先进入该视图。

如果 *command* 中不指定视图，直接输入命令，表示该命令在用户视图下执行；当需要执行其它视图的命令时，需要先输入进视图的命令，再输入具体的配置命令。

需要注意的是，**CLI** 仅支持 Comware 命令，不支持 Linux、Python、Tcl 命令。

【举例】

使用 API CLI 添加本地用户 test。

```
<Sysname> python
Python 2.7.3 (default)
[GCC 4.4.1] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> import comware
>>> comware.CLI('system-view ;local-user test class manage')
```

【结果】

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] local-user test class manage
New local user added.
<comware.CLI object at 0xb7f680a0>
```

2.1.2 get_output

用来获取命令执行的输出信息。

【命令】

CLI.get_output()

【返回值】

命令执行的输出信息

【举例】

使用 API CLI 添加本地用户，并输出命令行执行结果。

```
<Sysname> python
Python 2.7.3 (default)
[GCC 4.4.1] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> import comware
>>> c = comware.CLI('system-view ;local-user test class manage', False)
>>> c.get_output()
```

【结果】

```
['<Sysname>system-view', 'System View: return to User View with Ctrl+Z.',
'[Sysname]local-user test class manage', 'New local user added.']
```

2.2 Transfer类

2.2.1 Transfer

用来将指定文件通过指定协议下载到本地。

【命令】

Transfer(*protocol*='', *host*='', *source*='', *dest*='', *vrf*='',*login_timeout*=10, *user*='', *password*='')

【参数】

protocol：表示下载文件时使用的协议。取值为：

- **ftp**：表示使用 FTP 协议传输文件。
- **tftp**：表示使用 TFTP 协议传输文件。
- **http**：表示使用 HTTP 协议传输文件。

host：表示远程服务器的 IP 地址。

source：表示服务器上源文件的名称。

dest：表示保存到本地的目的文件的名称。

vrf：指定目的端所属的 MPLS L3VPN 的 VPN 实例名称，为 1～31 个字符的字符串，区分大小写。如果未指定本参数，则表示目的端位于公网中。

login_timeout：表示下载文件时登录的超时时间，单位为秒，缺省值为 10。

user：表示登录时使用的用户名称。

password：表示登录时使用的用户密码。

【返回值】

Transfer 对象

【举例】

使用 API Transfer 将 TFTP 服务器（192.168.1.26）上的文件 test.cfg 下载到设备上。

```
<Sysname> python
Python 2.7.3 (default)
[GCC 4.4.1] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> import comware
>>> comware.Transfer('tftp', '192.168.1.26', 'test.cfg', 'flash:/test.cfg', user='',
password='')
```

【结果】

```
<comware.Transfer object at 0xb7f700e0>
```

2.2.2 get_error

用来获取下载文件过程中的错误信息。

【命令】

Transfer.get_error()

【返回值】

下载文件过程中的错误信息，若没有错误信息则返回 None。

【举例】

使用 API Transfer 将 TFTP 服务器（1.1.1.1）上的文件 test.cfg 下载到设备上。

```
<Sysname> python
Python 2.7.3 (default)
```

```
[GCC 4.4.1] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> import comware
>>> c = comware.Transfer('tftp', '1.1.1.1', 'test.cfg', 'flash:/test.cfg', user='',
password='')
>>> c.get_error()
```

【结果】

```
“Couldn’t connect to server”
```

2.3 API get_self_slot

2.3.1 get_self_slot

get_self_slot 接口用来获取主用主控板所在的槽位号。（集中式设备－独立运行模式）

get_self_slot 接口用来获取主用主控板所在的槽位号。（分布式设备－独立运行模式）

get_self_slot 接口用来获取主设备的成员编号。（集中式设备－IRF 模式）

get_self_slot 接口用来获取全局主用主控板所在的槽位号。（分布式设备－IRF 模式）

【命令】

get_self_slot()

【返回值】

- 集中式设备－独立运行模式

设备上无主用主控板，返回一个列表对象，值始终为[-1,-1]。

- 分布式设备－独立运行模式

返回一个列表对象，格式为：[-1,*slot-number*]，其中 *slot-number* 表示主用主控板所在的槽位号。

- 集中式设备－IRF 模式

返回一个列表对象，格式为：[-1,*slot-number*]，其中 *slot-number* 表示主设备在 IRF 中的成员编号。

- 分布式设备－IRF 模式

返回一个列表对象，格式为：[*chassis-number*,*slot-number*]，其中：*chassis-number* 表示全局主控板所在设备的成员编号，*slot-number* 表示全局主控板在成员设备上的槽位号。

【举例】

使用 API 获取全局主用主控板所在的槽位号。

```
<Sysname> python
Python 2.7.3 (default)
[GCC 4.4.1] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> import comware
>>> comware.get_self_slot()
```

【结果】

```
[-1,0]
```

2.4 API get_standby_slot

2.4.1 get_standby_slot

get_standby_slot 接口用来获取所有备用主控板所在的槽位号。（集中式设备－独立运行模式）

get_standby_slot 接口用来获取所有备用主控板所在的槽位号。（分布式设备－独立运行模式）

get_standby_slot 接口用来获取所有从设备的成员编号。（集中式设备－IRF 模式）

get_standby_slot 接口用来获取所有全局备用主控板所在的槽位号。（分布式设备－IRF 模式）

【命令】

get_standby_slot()

【返回值】

- 集中式设备－独立运行模式

设备上无备用主控板，返回一个列表对象，返回值始终为[ ]。

- 分布式设备－独立运行模式

返回一个列表对象，格式为：[[-1,*slot-number*]]，其中 *slot-number* 表示备用主控板所在的槽位号。如果设备上没有备用主控板，则返回[ ]。

- 集中式设备－IRF 模式

返回一个列表对象，格式为：[[-1,*slot-number*]]，其中 *slot-number* 表示从设备在 IRF 中的成员编号。如果 IRF 中没有从设备，则返回[ ]；当 IRF 中有多个从设备时，则返回：[[-1,*slot-number1*],[-1,*slot-number2*],……]。

- 分布式设备－IRF 模式

返回一个列表对象，格式为：[[*chassis-number*,*slot-number*]]，其中：*chassis-number* 表示全局备用主控板所在设备的成员编号，*slot-number* 表示全局备用主控板在成员设备上的槽位号。如果 IRF 中没有全局备用主控板，则返回[ ]；当 IRF 中有多个全局备用主控板时，则返回：[[*chassis-number1*,*slot-number1*],[*chassis-number2*,*slot-number2*],……]。

【举例】

使用 API 获取从设备所在的槽位号。

```
<Sysname> python
Python 2.7.3 (default)
[GCC 4.4.1] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> import comware
>>> comware.get_standby_slot()
```

【结果】

[[-1, 1], [-1, 2]]

2.5 API get_slot_range

2.5.1 get_slot_range

get_slot_range 接口用来获取当前系统所支持的槽位号范围。

【命令】

get_slot_range()

【返回值】

返回一个字典对象，返回值始终为{'MaxSlot': *max-slot-number*, 'MinSlot': *min-slot-number* }。*max-slot-number* 表示设备支持的最大槽位号，*min-slot-number* 表示设备支持的最小槽位号。

【举例】

使用 API 获取系统槽位号范围。

```
<Sysname> python
Python 2.7.3 (default)
[GCC 4.4.1] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> import comware
>>> comware. get_slot_range()
```

【结果】

{'MaxSlot': 7, 'MinSlot': 0}

2.6 API get_slot_info

2.6.1 get_slot_info

get_slot_info 接口用来获取指定单板的信息。(分布式设备－独立运行模式/分布式设备－IRF 模式)

【命令】

get_slot_info()

【返回值】

返回一个字典对象，返回值始终为{'Slot': *slot-number*, 'Status': '*status*', 'Chassis': *chassis-number*, 'Role': '*role*', 'Cpu': *CPU-number* }。*slot-number* 表示单板所在的槽位号，*status* 表示单板的状态，*chassis-number* 表示设备在 IRF 中的成员编号，*role* 表示单板的角色，*CPU-number* 表示单板上主 CPU 的编号，取值为 0。

【举例】

使用 API 获取槽位号信息。

```
<Sysname> python
Python 2.7.3 (default)
[GCC 4.4.1] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> import comware
>>> comware.get_slot_info(1)
```

【结果】

```
{'Slot': 1, 'Status': 'Normal', 'Chassis': 0, 'Role': 'Master', 'Cpu': 0}
```

目 录

1 简介

说明

本文描述的不支持表示的是路由器不需要申请 License 即可支持该软件包或特性。

H3C MSR 路由器的 License 分为软件包 License 和特性 License。两种 License 的激活和安装流程相同，均可以通过 H3C 官方网站申请 License 激活文件，将 License 激活文件安装到设备上，就可以使用相应的软件功能。

1.1 软件包License

设备各款型对于本节所描述的特性支持情况有所不同，详细差异信息如下：

型号	特性	描述
MSR810/810-W/810-W-DB/810-LM/810-W-LM/810-10-PoE/810-LM-HK/810-W-LM-HK/810-LMS/810-LUS	软件包License	不支持
MSR2600-6-X1/2600-10-X1		不支持
MSR 2630		支持
MSR3600-28/3600-51		支持
MSR3600-28-SI/3600-51-SI		不支持
MSR3610-X1/3610-X1-DP/3610-X1-DC/3610-X1-DP-DC		不支持
MSR 3610/3620/3620-DP/3640/3660		• MSR 3610/3620/3640/3660：支持 • MSR3620-DP：不支持
MSR5620/5660/5680		• MSR 5660/5680：安装 MPU-100 时支持；安装 MPU-100-X1 时不支持 • MSR5620：不支持

型号	特性	描述
MSR810-W-WiNet/810-LM-WiNet	软件包License	不支持
MSR830-4LM-WiNet		不支持
MSR830-5BEI-WiNet/830-6EI-WiNet/830-10BEI-WiNet		不支持
MSR830-6BHI-WiNet/830-10BHI-WiNet		不支持
MSR2600-10-X1-WiNet		不支持

型号	特性	描述
MSR2630-WiNet		支持
MSR3600-28-WiNet		支持
MSR3610-X1-WiNet		不支持
MSR3610-WiNet/3620-10-WiNet/3620-DP-WiNet/3620-WiNet/3660-WiNet		• MSR3610-WiNet/3620-10-WiNet/3620-WiNet/3660-WiNet：支持 • MSR3620-DP-WiNet：不支持

型号	特性	描述
MSR810-LM-GL	软件包License	不支持
MSR810-W-LM-GL		不支持
MSR830-6EI-GL		不支持
MSR830-10EI-GL		不支持
MSR830-6HI-GL		不支持
MSR830-10HI-GL		不支持
MSR2600-6-X1-GL		不支持
MSR3600-28-SI-GL		不支持

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

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

说明

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

设备正确安装完成软件包 License 后会自动进行一次搜索并安装对应软件包操作：

- 若不存在对应软件包，需要用户加载软件包并手动安装。
- 若存在对应软件包，在软件包安装过程中设备断电或重启导致安装失败，则设备再次上电时，仍需要手动安装软件包。关于软件包是否安装成功，可通过 **display boot-loader** 命令进行查看。

在软件包安装过程中，请勿执行 **save** 命令保持配置，否则会导致配置丢失。

1.2 特性License

1.2.1 空管License

设备各款型对于本节所描述的特性支持情况有所不同，详细差异信息如下：

型号	特性	描述
MSR810/810-W/810-W-DB/810-LM/810-W-LM/810-10-PoE/810-LM-HK/810-W-LM-HK/810-LMS/810-LUS	空管License	不支持
MSR2600-6-X1/2600-10-X1		不支持
MSR 2630		不支持
MSR3600-28/3600-51		不支持
MSR3600-28-SI/3600-51-SI		不支持
MSR3610-X1/3610-X1-DP/3610-X1-DC/3610-X1-DP-DC		支持
MSR 3610/3620/3620-DP/3640/3660		支持
MSR5620/5660/5680		支持

型号	特性	描述
MSR810-W-WiNet/810-LM-WiNet	空管License	不支持
MSR830-4LM-WiNet		不支持
MSR830-5BEI-WiNet/830-6EI-WiNet/830-10BEI-WiNet		不支持
MSR830-6BHI-WiNet/830-10BHI-WiNet		不支持
MSR2600-10-X1-WiNet		不支持
MSR2630-WiNet		不支持
MSR3600-28-WiNet		不支持
MSR3610-X1-WiNet		支持

型号	特性	描述
MSR3610-WiNet/3620-10-WiNet/3620-DP-WiNet/3620-WiNet/3660-WiNet		支持

型号	特性	描述
MSR810-LM-GL	空管License	不支持
MSR810-W-LM-GL		不支持
MSR830-6EI-GL		不支持
MSR830-10EI-GL		不支持
MSR830-6HI-GL		不支持
MSR830-10HI-GL		不支持
MSR2600-6-X1-GL		不支持
MSR3600-28-SI-GL		不支持

当安装了空管 License 激活文件时，用户可以使用 RTC 终端接入功能，否则，用户不能使用 RTC 终端接入功能。

1.2.2 IP POS License

设备各款型对于本节所描述的特性支持情况有所不同，详细差异信息如下：

型号	特性	描述
MSR810/810-W/810-W-DB/810-LM/810-W-LM/810-10-PoE/810-LM-HK/810-W-LM-HK/810-LMS/810-LUS	IP POS License	不支持
MSR2600-6-X1/2600-10-X1		不支持
MSR 2630		不支持
MSR3600-28/3600-51		不支持
MSR3600-28-SI/3600-51-SI		不支持
MSR3610-X1/3610-X1-DP/3610-X1-DC/3610-X1-DP-DC		不支持
MSR 3610/3620/3620-DP/3640/3660		不支持
MSR5620/5660/5680		支持

型号	特性	描述
MSR810-W-WiNet/810-LM-WiNet	IP POS License	不支持
MSR830-4LM-WiNet		不支持
MSR830-5BEI-WiNet/830-6EI-WiNet/830-10BEI-WiNet		不支持

型号	特性	描述
MSR830-6BHI-WiNet/830-10BHI-WiNet		不支持
MSR2600-10-X1-WiNet		不支持
MSR2630-WiNet		不支持
MSR3600-28-WiNet		不支持
MSR3610-X1-WiNet		不支持
MSR3610-WiNet/3620-10-WiNet/3620-DP-WiNet/3620-WiNet/3660-WiNet		不支持

型号	特性	描述
MSR810-LM-GL	IP POS License	不支持
MSR810-W-LM-GL		不支持
MSR830-6EI-GL		不支持
MSR830-10EI-GL		不支持
MSR830-6HI-GL		不支持
MSR830-10HI-GL		不支持
MSR2600-6-X1-GL		不支持
MSR3600-28-SI-GL		不支持

IP POS License 用来控制设备与 POS 终端之间支持建立的 TCP 连接数量，当安装了 IP POS License 激活文件时，设备与 POS 终端之间可以支持建立 256 条 TCP 连接，否则，设备与 POS 终端之间无法建立 TCP 连接。IP POS License 支持数量累加。

E1POS 接口模块，不受该 License 控制，即使没有安装 IP POS License 激活文件，安装 E1POS 接口模块，E1POS 功能正常。

1.2.3 AC License

设备各款型对于本节所描述的特性支持情况有所不同，详细差异信息如下：

型号	特性	描述
MSR810/810-W/810-W-DB/810-LM/810-W-LM/810-10-PoE/810-LM-HK/810-W-LM-HK/810-LMS/810-LUS	AC License	MSR810/810-W/810-W-DB/810-LM/810-W-LM/810-10-PoE/810-LM-HK/810-W-LM-HK：支持 MSR810-LMS/810-LUS：不支持
MSR2600-6-X1/2600-10-X1		支持
MSR 2630		支持
MSR3600-28/3600-51		支持
MSR3600-28-SI/3600-51-SI		不支持
MSR3610-X1/3610-X1-DP/3610-X1-		支持

型号	特性	描述
DC/3610-X1-DP-DC		
MSR 3610/3620/3620-DP/3640/3660		支持
MSR5620/5660/5680		不支持

型号	特性	描述
MSR810-W-WiNet/810-LM-WiNet	AC License	支持
MSR830-4LM-WiNet		不支持
MSR830-5BEI-WiNet/830-6EI-WiNet/830-10BEI-WiNet		不支持
MSR830-6BHI-WiNet/830-10BHI-WiNet		不支持
MSR2600-10-X1-WiNet		支持
MSR2630-WiNet		支持
MSR3600-28-WiNet		支持
MSR3610-X1-WiNet		支持
MSR3610-WiNet/3620-10-WiNet/3620-DP-WiNet/3620-WiNet/3660-WiNet		支持

型号	特性	描述
MSR810-LM-GL	AC License	不支持
MSR810-W-LM-GL		不支持
MSR830-6EI-GL		不支持
MSR830-10EI-GL		不支持
MSR830-6HI-GL		不支持
MSR830-10HI-GL		不支持
MSR2600-6-X1-GL		不支持
MSR3600-28-SI-GL		不支持

AC License 用来控制允许上线的 AP 数，根据允许 AP 数量不同，分为 1 个、4 个、8 个、16 个、32 个和 128 个六种 License，并且支持 License 数量累加。未安装 AC License 激活文件时，AC 不允许 AP 上线。

MSR810/810-W/810-W-DB/810-LM/810-W-LM/810-10-PoE 路由器支持的最大 AP 数量为 16 个；MSR2600-6-X1/2600-10-X1 路由器支持的最大 AP 数量为 32 个；MSR 2630/3600-28/3600-51 路由器支持的最大 AP 数量为 64 个；MSR3610/3610-X1/3610-X1-DP/3610-X1-DC/3610-X1-DP-DC/3620/3620-DP/3640/3660 路由器支持的最大 AP 数量为 256 个。

1.2.4 IPS License

设备各款型对于本节所描述的特性支持情况有所不同，详细差异信息如下：

型号	特性	描述
MSR810/810-W/810-W-DB/810-LM/810-W-LM/810-10-PoE/810-LM-HK/810-W-LM-HK/810-LMS/810-LUS	IPS License	MSR810/810-W/810-W-DB/810-LM/810-W-LM/810-10-PoE/810-LM-HK/810-W-LM-HK：支持 MSR810-LMS/810-LUS：不支持
MSR2600-6-X1/2600-10-X1		支持
MSR 2630		支持
MSR3600-28/3600-51		支持
MSR3600-28-SI/3600-51-SI		不支持
MSR3610-X1/3610-X1-DP/3610-X1-DC/3610-X1-DP-DC		支持
MSR 3610/3620/3620-DP/3640/3660		支持
MSR5620/5660/5680		支持

型号	特性	描述
MSR810-W-WiNet/810-LM-WiNet	IPS License	支持
MSR830-4LM-WiNet		不支持
MSR830-5BEI-WiNet/830-6EI-WiNet/830-10BEI-WiNet		不支持
MSR830-6BHI-WiNet/830-10BHI-WiNet		不支持
MSR2600-10-X1-WiNet		支持
MSR2630-WiNet		支持
MSR3600-28-WiNet		支持
MSR3610-X1-WiNet		支持
MSR3610-WiNet/3620-10-WiNet/3620-DP-WiNet/3620-WiNet/3660-WiNet		支持

型号	特性	描述
MSR810-LM-GL	IPS License	不支持
MSR810-W-LM-GL		不支持
MSR830-6EI-GL		不支持
MSR830-10EI-GL		不支持
MSR830-6HI-GL		不支持
MSR830-10HI-GL		不支持

型号	特性	描述
MSR2600-6-X1-GL		不支持
MSR3600-28-SI-GL		不支持

IPS License 用来控制 IPS 特征库的升级，当安装了 IPS License 激活文件时，允许升级 IPS 特征库，否则，不允许升级 IPS 特征库。

IPS License 为时间型特性 License，分为 1 年有效和 3 年有效两种 License，并且支持时间累加。

1.2.5 ACG License

设备各款型对于本节所描述的特性支持情况有所不同，详细差异信息如下：

型号	特性	描述
MSR810/810-W/810-W-DB/810-LM/810-W-LM/810-10-PoE/810-LM-HK/810-W-LM-HK/810-LMS/810-LUS	ACG License	MSR810/810-W/810-W-DB/810-LM/810-W-LM/810-10-PoE/810-LM-HK/810-W-LM-HK：支持 MSR810-LMS/810-LUS：不支持
MSR2600-6-X1/2600-10-X1		支持
MSR 2630		支持
MSR3600-28/3600-51		支持
MSR3600-28-SI/3600-51-SI		不支持
MSR3610-X1/3610-X1-DP/3610-X1-DC/3610-X1-DP-DC		支持
MSR 3610/3620/3620-DP/3640/3660		支持
MSR5620/5660/5680		支持

型号	特性	描述
MSR810-W-WiNet/810-LM-WiNet	ACG License	支持
MSR830-4LM-WiNet		不支持
MSR830-5BEI-WiNet/830-6EI-WiNet/830-10BEI-WiNet		不支持
MSR830-6BHI-WiNet/830-10BHI-WiNet		不支持
MSR2600-10-X1-WiNet		支持
MSR2630-WiNet		支持
MSR3600-28-WiNet		支持
MSR3610-X1-WiNet		支持
MSR3610-WiNet/3620-10-WiNet/3620-DP-WiNet/3620-WiNet/3660-WiNet		支持

型号	特性	描述
MSR810-LM-GL	ACG License	不支持
MSR810-W-LM-GL		不支持
MSR830-6EI-GL		不支持
MSR830-10EI-GL		不支持
MSR830-6HI-GL		不支持
MSR830-10HI-GL		不支持
MSR2600-6-X1-GL		不支持
MSR3600-28-SI-GL		不支持

ACG License 用来控制 ACG 特征库的升级，当安装了 ACG License 激活文件时，允许升级 ACG 特征库，否则，不允许特征库升级。

ACG License 为时间型特性 License，分为 1 年有效和 3 年有效两种 License，并且支持时间累加。

1.2.6 SSL VPN License

设备各款型对于本节所描述的特性支持情况有所不同，详细差异信息如下：

型号	特性	描述
MSR810/810-W/810-W-DB/810-LM/810-W-LM/810-10-PoE/810-LM-HK/810-W-LM-HK/810-LMS/810-LUS	SSL VPN License	MSR810/810-W/810-W-DB/810-LM/810-W-LM/810-10-PoE/810-LM-HK/810-W-LM-HK：支持 MSR810-LMS/810-LUS：不支持
MSR2600-6-X1/2600-10-X1		支持
MSR 2630		支持
MSR3600-28/3600-51		支持
MSR3600-28-SI/3600-51-SI		不支持
MSR3610-X1/3610-X1-DP/3610-X1-DC/3610-X1-DP-DC		支持
MSR 3610/3620/3620-DP/3640/3660		支持
MSR5620/5660/5680		支持

型号	特性	描述
MSR810-W-WiNet/810-LM-WiNet	SSL VPN License	支持
MSR830-4LM-WiNet		不支持
MSR830-5BEI-WiNet/830-6EI-WiNet/830-10BEI-WiNet		不支持
MSR830-6BHI-WiNet/830-10BHI-WiNet		不支持
MSR2600-10-X1-WiNet		支持

型号	特性	描述
MSR2630-WiNet		支持
MSR3600-28-WiNet		支持
MSR3610-X1-WiNet		支持
MSR3610-WiNet/3620-10-WiNet/3620-DP-WiNet/3620-WiNet/3660-WiNet		支持

型号	特性	描述
MSR810-LM-GL	SSL VPN License	不支持
MSR810-W-LM-GL		不支持
MSR830-6EI-GL		不支持
MSR830-10EI-GL		不支持
MSR830-6HI-GL		不支持
MSR830-10HI-GL		不支持
MSR2600-6-X1-GL		不支持
MSR3600-28-SI-GL		不支持

SSL VPN License 用来控制 SSL VPN 允许上线的用户数，分为 30 个用户和 200 个用户两种 License，并且 License 支持数量累加。未安装 SSL VPN License 激活文件时，不允许用户上线。

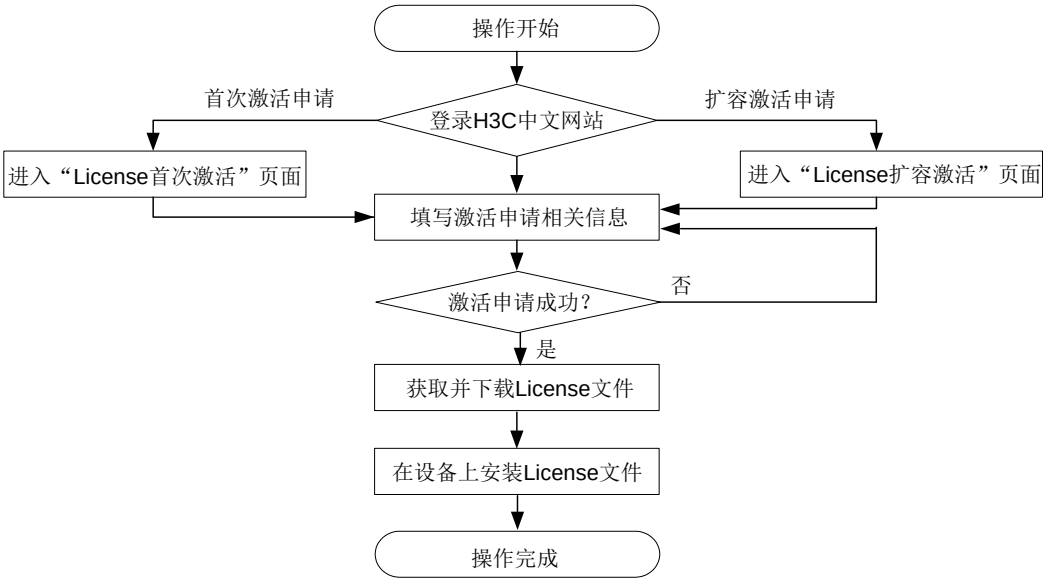
2 License的激活和安装流程

License 的激活申请有两种类型：

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

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

图2-1 License 激活示意图



3 License的激活申请

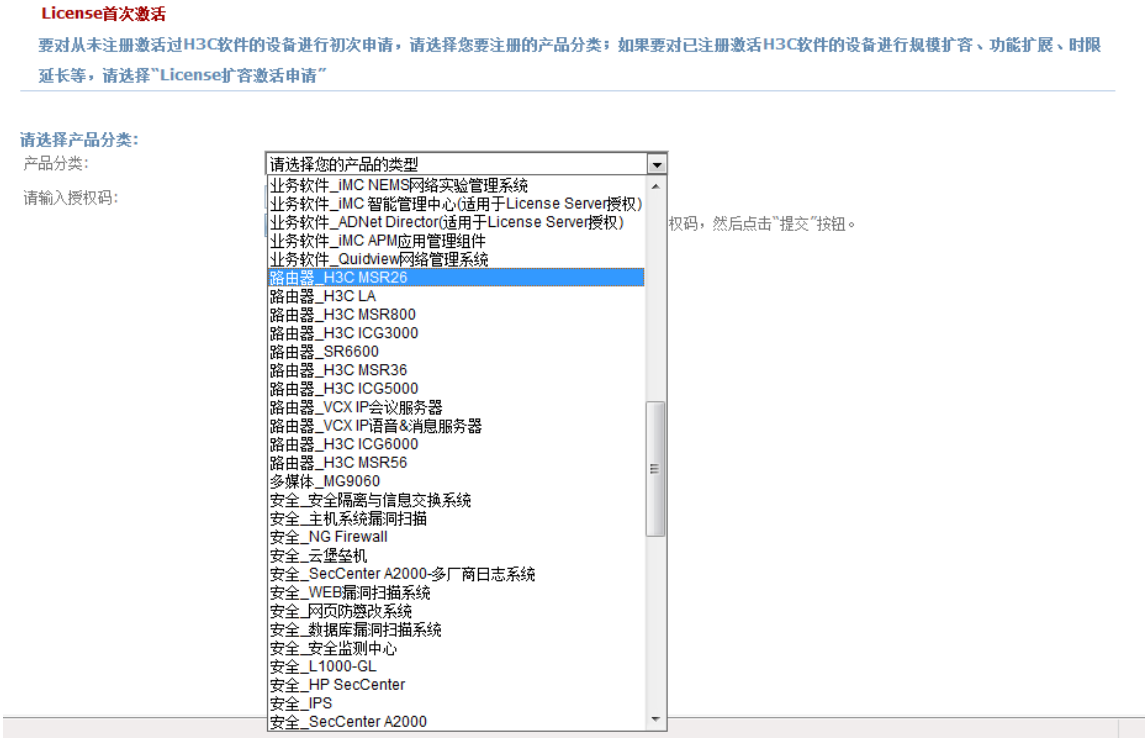
3.1 License首次激活申请

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

图3-1 License 首次激活页面

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

图3-2 选择产品类型



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

图3-3 输入 License 首次激活信息

表3-1 License 首次激活申请信息说明

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

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

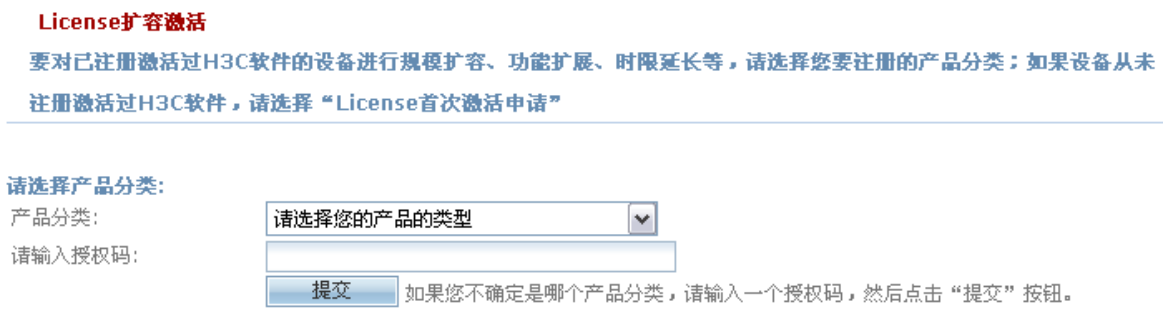
步骤4 如果步骤 3 的信息填写无误，系统将提示如图 3-4 所示的对话框，并且对话框中附有已经申请下来的 License 文件的链接，点击并下载 License 文件到本地 PC，然后按照 License 激活文件的安装中所述的方法，完成 License 文件的安装。

图3-4 License 首次激活申请操作成功

3.2 License扩容激活申请

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

图3-5 License 扩容激活页面



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

图3-6 选择产品类型

步骤3 在弹出的“设备信息”对话框中，根据表 3-2 的说明，输入相应的信息，然后点击<提交>按钮。

图3-7 输入 License 扩容激活用户信息

表3-2 License 扩容激活申请用户信息说明

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

步骤4 在弹出来的 “授权信息”和“用户信息”对话框中，根据表 3-3 中的说明，输入相应的信息，然后勾选“已阅读并同意法律声明所述服务条款各项内容”，最后点击按钮<获取激活码（文件）>。

图3-8 输入 License 扩容激活授权和用户信息

表3-3 License 扩容激活申请授权和用户信息说明

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

步骤5 如果步骤 4 的信息填写无误，系统将提示如图 3-9 所示的对话框，并且对话框中附有已经申请下来的 License 文件的链接，点击并下载 License 文件到本地 PC，然后按照 License 激活文件的安装中所述的方法，完成 License 文件的安装。

图3-9 License 扩容激活申请操作成功

4 License激活文件的安装

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

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

```
<H3C> system-view
[H3C] license activation-file install cfa0:/210235A0W8B13300004120130731102846937735.ak
```

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

```
<H3C> display license
cfa0:/license/210235A0W8B133000041201307311028469373 5.ak
Feature: pkg_license
Product Description: H3C MSR 56 Data Software License
Registered at: 2017-03-03 03:56:53
License Type: Trial (days restricted)
Trial Time Left (days): 30
Current State: In use
```