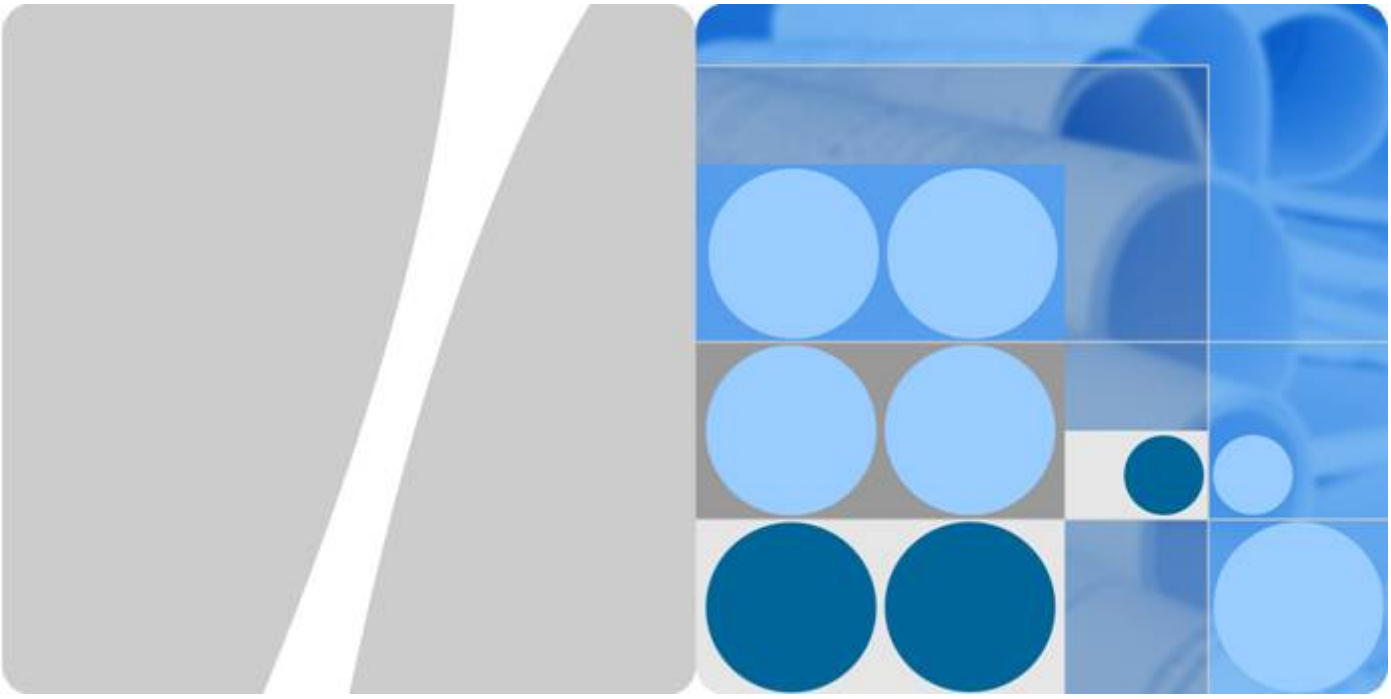


S300, S500, S2700, S5700, S6700 系列以太网交换机 V200R022C00

配置指南-基础配置

文档版本　03

发布日期　2024-02-29

华为技术有限公司

HUAWEI

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： https://e.huawei.com

前言

读者对象

本文档适用于负责配置和管理交换机的网络工程师。您应该熟悉以太网基础知识，且具有丰富的网络部署与管理经验。

符号约定

在本文中可能出现下列标志，它们所代表的含义如下。

符号	说明
注意	表示如不避免则可能导致轻微或中度伤害的具有低等级风险的危害。
须知	用于传递设备或环境安全警示信息。如不避免则可能会导致设备损坏、数据丢失、设备性能降低或其它不可预知的结果。 “须知”不涉及人身伤害。
说明	对正文中重点信息的补充说明。 “说明”不是安全警示信息，不涉及人身、设备及环境伤害信息。

命令行格式约定

在本文中可能出现下列命令行格式，它们所代表的含义如下。

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。

格式	意义
{ x | y | ... }	表示从两个或多个选项中选取一个。
[x | y | ...]	表示从两个或多个选项中选取一个或者不选。
{ x | y | ... }*	表示从两个或多个选项中选取多个，最少选取一个，最多选取所有选项。
[x | y | ...]*	表示从两个或多个选项中选取多个或者不选。
&<1-n>	表示符号&的参数可以重复1～n次。
#	由“#”开始的行表示为注释行。

接口编号约定

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

安全约定

- 密码配置约定
  - 配置密码时请尽量选择密文模式(cipher)。为充分保证设备安全，请用户不要关闭密码复杂度检查功能，并定期修改密码。
  - 配置明文模式的密码时，请不要以“%^%#.....%^%#”、“%#%#.....%#%#”、“%@%@.....%@%@”或者“@%@%.....@%@%”作为起始和结束符。因为用这些字符为起始和结束符的是合法密文（本设备可以解密的密文），配置文件会显示与用户配置相同的明文。
  - 配置密文密码时，不同特性的密文密码不能互相使用。例如AAA特性生成的密文密码不能用于配置其他特性的密文密码。
- 加密算法约定

  目前设备采用的加密算法包括3DES、AES、RSA、SHA1、SHA2和MD5。3DES、RSA和AES加密算法是可逆的，SHA1、SHA2和MD5加密算法是不可逆的。DES/3DES/RSA(1024位以下)/MD5(数字签名场景和口令加密)/SHA1(数字签名场景)加密算法安全性低，存在安全风险。在协议支持的加密算法选择范围内，建议使用更安全的加密算法，比如AES/RSA(2048位以上)/SHA2/HMAC-SHA2。具体采用哪种加密算法请根据场景而定：对于管理员类型的密码，必须采用不可逆加密算法，推荐使用安全性更高的SHA2。
- 个人数据约定

  您购买的产品、服务或特性在业务运营或故障定位的过程中将可能获取或使用用户的某些个人数据（如终端用户的MAC地址或IP地址），因此您有义务根据所适用国家的法律制定必要的用户隐私政策并采取足够的措施以确保用户的个人数据受到充分的保护。
- 本文档中出现的“镜像端口、端口镜像、流镜像、镜像”等相关词汇仅限于为了描述该产品进行检测通信传输中的故障和错误的目的而使用，不涉及采集、处理任何个人数据或任何用户通信内容。

- 可靠性设计声明

  对于网络规划和站点设计，必须严格遵守可靠性设计原则，具备设备级和方案级保护。设备级保护包括双网双平面，双机、跨板双链路的规划原则，避免出现单点，单链路故障。方案级指FRR、VRRP等快速收敛保护机制。在应用方案级保护时，应避免保护方案的主备路径经过相同链路或者传输，以免方案级保护不生效。

参考标准和协议

请登录**华为网站**，搜索“标准协议顺从表”，获取《华为S系列交换机标准协议顺从表》。获取该信息需要访问权限，如需帮助，请联系技术支持人员。

特别声明

- 本文档仅作为使用指导，其内容（如Web界面、CLI命令格式、命令输出）依据实验室设备信息编写。文档提供的内容具有一般性的指导意义，并不确保涵盖所有型号产品的所有使用场景。因版本升级、设备型号不同、配置文件不同等原因，可能造成文档中提供的内容与用户使用的设备界面不一致。请以用户设备界面的信息为准，本文档不再针对前述情况造成的差异一一说明。
- 本文档中提供的最大值是设备在实验室特定场景（例如，被测试设备上只有某种类型的单板，或者只配置了某一种协议）达到的最大值。在现实网络中，由于设备硬件配置不同、承载的业务不同等原因会使设备测试出的最大值与文档中提供的数据不一致。
- 出于特性介绍及配置示例的需要，本文档可能会使用公网IP地址，如无特殊说明出现的公网IP地址均为示意，不指代任何实际意义。

目 录

前言 ii
1 熟悉命令行 1
1.1 进入命令行视图 1
1.2 编辑命令行 3
1.3 使用命令行在线帮助 5
1.4 使用 undo 命令行 6
1.5 批处理操作 7
1.6 在系统视图下执行用户视图命令 8
1.7 使用命令行的快捷键 8
1.8 查询命令行的配置信息 9
1.9 控制命令行显示 10
1.10 使用正则表达式过滤命令行显示信息 10
1.11 设置命令级别 15
1.12 查看历史命令 17
2 登录密码管理 19
2.1 设备登录的缺省密码 19
2.2 恢复 Console 口登录密码 19
2.3 恢复 Telnet 登录密码 21
2.4 恢复 STelnet 登录密码 21
2.5 恢复 BootLoad 密码 23
2.6 恢复 Web 登录密码 23
3 EasyDeploy 配置 25
3.1 EasyDeploy 简介 25
3.2 EasyDeploy 原理描述 26
3.2.1 EasyDeploy 基本概念 26
3.2.2 通过 Option 参数或中间文件实现零配置设备部署 30
3.2.3 通过 Commander 实现零配置设备部署 36
3.2.4 通过中间文件实现带配置部署 38
3.2.5 故障设备替换 40
3.2.6 批量升级 41
3.2.7 批量配置 43
3.3 EasyDeploy 配置注意事项 44

3.4 EasyDeploy 缺省配置 49
3.5 通过 Option 参数实现零配置设备部署 49
3.5.1 配置文件服务器 49
3.5.2 配置 DHCP 50
3.6 通过中间文件实现零配置设备部署 52
3.6.1 配置文件服务器 52
3.6.2 编辑中间文件 53
3.6.3 配置 DHCP 54
3.7 通过中间文件实现带配置设备部署 56
3.7.1 配置文件服务器 56
3.7.2 编辑中间文件 57
3.7.3 配置 DHCP 58
3.7.4 带配置设备部署 59
3.8 通过 Commander 实现零配置设备部署 62
3.8.1 配置文件服务器 62
3.8.2 配置 DHCP 63
3.8.3 配置 Commander 65
3.8.3.1 配置 Commander 基本功能 65
3.8.3.2 配置文件服务器信息 65
3.8.3.3 （可选）配置网络拓扑收集功能 66
3.8.3.4 配置下载文件信息 68
3.8.3.5 配置下载后文件的激活策略 70
3.8.3.6 （可选）使能自动清理存储空间功能 71
3.8.3.7 （可选）配置自动备份配置文件功能 72
3.8.4 检查配置结果 72
3.9 通过 Commander 实现手动替换故障设备 73
3.10 通过 Commander 实现自动替换故障设备 74
3.11 通过 Commander 批量升级设备 75
3.12 通过 Commander 批量配置设备 77
3.13 将有配置设备加入 Commander 管理 79
3.14 维护 EasyDeploy 81
3.14.1 维护 Client 信息 81
3.14.2 查看能耗信息 82
3.15 EasyDeploy 配置举例 82
3.15.1 通过 Option 参数实现零配置设备部署示例 82
3.15.2 通过中间文件实现零配置设备部署示例 85
3.15.3 通过 Commander 实现零配置设备部署（不使能网络拓扑收集功能）示例 89
3.15.4 通过 Commander 实现零配置设备部署（使能网络拓扑收集功能）示例 94
3.15.5 通过 Commander 实现手动替换故障设备示例 99
3.15.6 通过 Commander 实现批量升级设备示例 102
3.15.7 通过 Commander 实现批量配置设备示例 107
3.15.8 将有配置设备加入 Commander 管理示例 109

3.15.9 通过 eSight 对园区总部进行零配置部署 111
3.15.10 通过手抄 MAC/ESN 方式对分支进行零配置部署 119
4 U 盘开局配置 124
4.1 U 盘开局简介 124
4.2 U 盘开局原理描述 124
4.3 U 盘开局配置注意事项 128
4.4 制作索引文件 131
4.5 配置 U 盘开局 137
4.6 U 盘开局配置举例 138
4.6.1 配置 U 盘开局示例 139
5 首次登录设备 141
5.1 首次登录设备简介 141
5.2 通过 Console 口首次登录设备 142
5.3 通过 Web 网管首次登录设备（传统管理模式设备） 143
5.4 通过 Web 网管首次登录设备（NETCONF 模式设备） 148
5.5 配置系统基本信息 151
5.6 配置通过 Console 口首次登录设备后进行基本配置的示例 153
6 登录设备命令行界面 157
6.1 登录方式介绍 157
6.2 用户界面介绍 158
6.3 用户认证方式和用户级别介绍 160
6.4 配置通过 Console 口登录设备 163
6.5 配置通过 Telnet 登录设备 166
6.6 配置通过 STelnet 登录设备 169
6.7 （可选）配置 ACL 限制用户通过 Telnet/STelnet 登录设备 177
6.8 命令行配置设备登录后的常用操作 178
6.9 登录设备命令行的配置举例 180
6.9.1 配置 ACL 限制用户通过 Telnet 登录设备示例 181
6.9.2 配置设备作为 Telnet 客户端登录其他设备示例 182
6.9.3 配置设备作为 STelnet 客户端登录其他设备示例（Password 认证） 184
6.9.4 配置设备作为 STelnet 客户端登录其他设备示例（Password 认证+DSA 认证） 187
6.10 登录设备命令行界面失败处理办法 192
6.10.1 通过 Console 口登录设备失败 192
6.10.2 通过 Telnet 登录设备失败 193
6.10.3 通过 STelnet 登录设备失败 194
6.11 登录设备 FAQ 196
6.11.1 为什么 SSH 方式登录设备慢? 196
7 登录设备 Web 网管界面 197
7.1 通过 Web 网管登录设备简介 197
7.2 Web 网管登录使用注意事项 199
7.3 配置通过 Web 网管登录设备 200

7.4 登录设备 Web 界面失败处理办法 205
7.5 通过 Web 网管登录设备的 FAQ 206
7.5.1 Web 网管功能对环境有什么要求? 206
7.5.2 如何获取 Web 网页文件? 206
7.5.3 为什么登录 Web 网管后只有几个操作选项? 207
7.5.4 如何修改 Web 登录密码? 207
7.5.5 Web 和 HTTP 什么区别? 207
8 文件管理 208
8.1 文件系统简介 208
8.2 设备支持的文件管理方式 209
8.3 管理本地文件 214
8.3.1 通过登录系统进行文件操作 214
8.3.2 通过 FTP 进行文件操作 217
8.3.3 通过 SFTP 进行文件操作 224
8.3.4 通过 SCP 进行文件操作 235
8.3.5 通过 FTPS 进行文件操作 244
8.4 访问其他设备的文件 251
8.4.1 配置设备作为 TFTP 客户端访问其他设备的文件 251
8.4.2 配置设备作为 FTP 客户端访问其他设备的文件 254
8.4.3 配置设备作为 SFTP 客户端访问其他设备的文件 259
8.4.4 配置设备作为 SCP 客户端访问其他设备的文件 267
8.4.5 配置设备作为 FTPS 客户端访问其他设备的文件 273
8.5 文件管理的配置举例 279
8.5.1 通过登录系统进行文件操作示例 280
8.5.2 FTP 服务器配置示例 281
8.5.3 SFTP 服务器配置示例 283
8.5.4 FTPS 服务器配置示例 285
8.5.5 TFTP 客户端配置示例 288
8.5.6 FTP 客户端配置示例 289
8.5.7 SFTP 客户端配置示例 291
8.5.8 SCP 客户端配置示例 296
8.5.9 FTPS 客户端配置示例 298
8.6 文件管理的常见配置错误 302
8.6.1 FTP 登录失败 302
8.6.2 上传文件失败 304
8.7 文件管理 FAQ 305
8.7.1 如何查看已删除文件 305
8.7.2 设备支持的 SSH 版本号 305
8.7.3 为什么 ssh 用户在配置远端认证时必须同时在设备本地配置用户才能通过认证 305
8.7.4 当存储设备出现异常时，如何修复 305
8.7.5 如何上传/下载文件 306
8.7.6 怎么限制 FTP 上传/下载速度 307

8.7.7 如何检查文件上传是否完整 307
8.7.8 各类型文件的后缀名是什么 308
8.7.9 日志文件存放在哪里 308
8.7.10 如何删除文件 308
8.7.11 怎么在两台设备之间传送文件 309
9 配置系统启动 310
9.1 系统启动简介 310
9.2 管理配置文件 314
9.2.1 保存配置文件 315
9.2.2 比较配置文件 316
9.2.3 备份配置文件 317
9.2.4 恢复配置文件 318
9.2.5 执行配置文件 320
9.2.6 清除配置 320
9.3 恢复出厂配置 321
9.4 配置系统启动文件 322
9.5 重新启动设备 324
9.6 配置系统启动的配置举例 325
9.6.1 备份配置文件示例 325
9.6.2 恢复配置文件示例 326
9.6.3 配置系统启动示例 327
10 智能升级 330
10.1 智能升级简介 330
10.2 传统升级方式与智能升级方式的对比 335
10.3 智能升级配置注意事项 336
10.4 智能升级缺省配置 337
10.5 配置智能升级功能 337
10.6 立即执行智能升级操作 338
10.7 配置交换机智能升级功能升级交换机示例 339
10.8 配置 AP 智能升级功能升级 AP 示例 342
10.9 智能升级配置失败常见处理办法 345
11 BootLoad 菜单操作 346
11.1 BootLoad 菜单 346
11.2 启动配置信息子菜单 Enter startup submenu 348
11.2.1 查看启动配置信息 Display startup configuration 349
11.2.2 修改启动配置信息 Modify startup configuration 349
11.3 以太网子菜单 Enter ethernet submenu 350
11.4 修改以太网参数 Modify ethernet interface boot parameter 351
11.5 文件系统子菜单 Enter filesystem submenu 354
11.6 密码子菜单 Enter password submenu 355
11.6.1 修改 BootLoad 密码 Modify bootload password 356

11.6.2 恢复 BootLoad 菜单密码 Reset bootload password.....357
11.7 清除 Console 登录密码 Clear password for console user.....358
11.8 BootLoad 诊断菜单.....358
11.9 通过 BootLoad 菜单升级系统软件.....363

1 熟悉命令行

1.1 进入命令行视图
1.2 编辑命令行
1.3 使用命令行在线帮助
1.4 使用undo命令行
1.5 批处理操作
1.6 在系统视图下执行用户视图命令
1.7 使用命令行的快捷键
1.8 查询命令行的配置信息
1.9 控制命令行显示
1.10 使用正则表达式过滤命令行显示信息
1.11 设置命令级别
1.12 查看历史命令

1.1 进入命令行视图

设备提供丰富的功能，相应的也提供了多样的配置和查询命令。为便于用户使用这些命令，华为交换机按功能分类将命令分别注册在不同的命令行视图下。配置某一功能时，需首先进入对应的命令行视图，然后执行相应的命令进行配置。

设备提供的命令视图有很多，下面提到的视图是最常用的视图。其他视图的进入方式在具体的命令中都有说明，请参见《S300, S500, S2700, S5700, S6700 V200R022C00 命令参考》。

常用的命令行视图

常用视图名称	进入视图	视图功能
用户视图	用户从终端成功登录至设备即进入用户视图，在屏幕上显示： <HUAWEI>	在用户视图下，用户可以完成查看运行状态和统计信息等功能。
系统视图	在用户视图下，输入命令**system-view**后回车，进入系统视图。 <HUAWEI> **system-view** Enter system view, return user view with Ctrl+Z. [HUAWEI]	在系统视图下，用户可以配置系统参数以及通过该视图进入其他的功能配置视图。
接口视图	使用**interface**命令并指定接口类型及接口编号可以进入相应的接口视图。 [HUAWEI] **interface gigabitethernet** *X/Y/Z* [HUAWEI-GigabitEthernet*X/Y/Z*] *X/Y/Z*为需要配置的接口的编号，分别对应“堆叠ID/子卡号/接口序号”。 上述举例中GigabitEthernet接口仅为示意。	配置接口参数的视图称为接口视图。在该视图下可以配置接口相关的物理属性、链路层特性及IP地址等重要参数。

命令行提示符“HUAWEI”是缺省的主机名（sysname）。通过提示符可以判断当前所处的视图，例如：“<>”表示用户视图，“[]”表示除用户视图以外的其它视图。

用户可以在任意视图中，执行！或#加字符串，此时的用户输入将全部（包括！和#在内）作为系统的注释行内容，不会产生对应的配置信息。

说明

- 有些在系统视图下执行的命令，在其它视图下也可以执行，但实现的功能与命令视图密切相关。例如**lldp enable**命令在系统视图表示使能全局的LLDP功能，在接口视图下，表示使能某一接口的LLDP功能。
- 在系统视图下，可以执行命令**diagnose**进入诊断视图。诊断命令行主要用于设备的故障诊断，在此视图下执行某些命令可能导致设备异常或业务中断。如果您需要使用此类命令行，请联系技术支持人员，在技术支持人员指导下谨慎使用。
- 用户可以在任意视图中，执行！或#加字符串，此时的用户输入将全部（包括！和#在内）作为系统的注释行内容，可以正常下发，不报错，不会产生对应的配置信息。
- 命令输入后会立刻执行，在5秒之内。

退出命令行视图

执行**quit**命令，即可从当前视图退出至上一层视图。

例如，执行**quit**命令从AAA视图退回到系统视图，再执行**quit**命令退回到用户视图。

```
[HUAWEI-aaa] quit
[HUAWEI] quit
<HUAWEI>
```

如果需要从AAA视图直接退回到用户视图，则可以在键盘上键入快捷键<Ctrl+Z>或者执行**return**命令。

使用快捷键<Ctrl+Z>直接退回到用户视图。

```
[HUAWEI-aaa]          //键入<Ctrl+Z>
<HUAWEI>
```

执行**return**命令直接退回到用户视图。

```
[HUAWEI-aaa] return
<HUAWEI>
```

命令行智能回退

缺省情况下，命令行具有智能回退功能。在当前视图下执行某条命令，如果命令行匹配失败，会自动退到上一级视图进行匹配，如果仍然失败则继续退到上一级视图匹配，直到退到系统视图为止。可根据需要，通过**undo terminal command forward matched upper-view**命令关闭命令行智能回退功能，且该命令只对执行此命令的当前登录用户有效。

说明

在端口组视图和VLAN-Range视图下不进行智能回退。

如果在当前视图下由于模糊匹配发生歧义导致匹配失败时，不进行智能回退。

智能回退功能可能会出现命令行在非预期视图执行，可能会影响业务运行。配置命令行前请仔细确认本视图下是否存在即将配置的命令行，如果不存在请在正确的视图执行该命令行。

下面分别举例，1为退入上一级视图即匹配对应视图，2为必须匹配到系统视图才能执行。

1. 在一个OSPF区域视图下不退到OSPF视图，直接进入另一个OSPF区域视图。

```
<HUAWEI> system-view
[HUAWEI] ospf 100
[HUAWEI-ospf-100] area 1
[HUAWEI-ospf-100-area-0.0.0.1] area 2
[HUAWEI-ospf-100-area-0.0.0.2]
```

2. 在OSPF区域视图直接进入接口视图。

```
<HUAWEI> system-view
[HUAWEI] ospf 100
[HUAWEI-ospf-100] area 1
[HUAWEI-ospf-100-area-0.0.0.1] interface gigabitEthernet 0/0/3
[HUAWEI-GigabitEthernet0/0/3]
```

1.2 编辑命令行

命令行编辑功能

设备的命令行接口提供基本的命令行编辑功能。设备支持多行编辑，每条命令最大长度为510个字符，命令关键字不区分大小写，命令参数是否区分大小写则由各命令定义的参数决定。

一些常用的编辑功能如**表1-1**所示。

表 1-1 编辑功能表

功能键	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，否则，响铃告警。
退格键Backspace	删除光标位置的前一个字符，光标左移，若已经到达命令首，则响铃告警。
左光标键←或<Ctrl+B>	光标向左移动一个字符位置，若已经到达命令首，则响铃告警。
右光标键→或<Ctrl+F>	光标向右移动一个字符位置，若已经到达命令尾，则响铃告警。

编辑命令行时的操作技巧

不完整关键字输入

设备支持不完整关键字输入，即在当前视图下，当输入的字符能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**display current-configuration**命令，可以输入**d cu**、**di cu**或**dis cu**等都可以执行此命令，但不能输入**d c**或**dis c**等，因为以**d c**、**dis c**开头的命令不唯一。

须知

系统可正确执行的命令长度最大为510个字符，包括使用不完整格式的情况。如果使用不完整格式进行配置，由于命令保存到配置文件中时使用的是完整格式，可能导致配置文件中存在长度超过510个字符的命令。系统重启时，这类命令将无法恢复。因此，在使用不完整格式的命令进行配置时，也需要注意命令的总长度。

Tab键的使用

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，光标距词尾空一格。例如：
  a. 输入不完整的关键字。
  ```
  [HUAWEI] info-
  ```
  b. 按下Tab键。
  则系统用此完整的关键字替代原输入并换行显示，光标距词尾空一格。
  ```
  [HUAWEI] info-center
  ```
- 如果与之匹配的关键字不唯一，反复按<Tab>键可循环显示所有以输入字符串开头的关键字，此时光标距词尾不空格。例如：
  a. 输入不完整的关键字。
  ```
  [HUAWEI] info-center log
  ```
  b. 按下Tab键。
  系统首先显示所有匹配的关键字的前缀，本例中前缀是“log”。

```
[HUAWEI] info-center loghost
```

继续按Tab键循环翻词，此时光标距词尾不空格。

```
[HUAWEI] info-center logbuffer
```

找到所需要的关键字后，停止按Tab键。

- 如果没有与之匹配的关键字，按Tab键后，换行显示，输入的关键字不变。例如：
  a. 输入错误的关键字。

     ```
     [HUAWEI] info-center loglog
     ```

  b. 按下Tab键。

     ```
     [HUAWEI] info-center loglog
     ```

     系统换行显示，但输入的关键字loglog不变，而且光标距词尾不空格，说明无此关键字。

1.3 使用命令行在线帮助

在线帮助通过键入“?”来获取，在命令行输入过程中，用户可以随时键入“?”以获得在线帮助。命令行在线帮助可分为完全帮助和部分帮助。

完全帮助

当用户输入命令时，可以使用命令行的完全帮助获取全部关键字和参数的提示。下面给出几种完全帮助的实例供参考：

- 在任一命令视图下，键入“?”获取该命令视图下所有的命令及其简单描述。举例如下：

```
<HUAWEI> ?
User view commands:
  backup         Backup electronic elabel
  cd             Change current directory
  check          Check information
  clear          Clear information
  clock          Specify the system clock
  compare        Compare function
...
```

- 键入一条命令的部分关键字，后接以空格分隔的“?”，如果该位置为关键字，则列出全部关键字及其简单描述。举例如下：

```
<HUAWEI> system-view
[HUAWEI] user-interface vty 0 4
[HUAWEI-ui-vty0-4] authentication-mode ?
  aaa       AAA authentication, and this authentication mode is recommended
  password  Authentication through the password of a user terminal interface
[HUAWEI-ui-vty0-4] authentication-mode aaa ?
  <cr>

[HUAWEI-ui-vty0-4] authentication-mode aaa
```

  - 其中“aaa”和“password”是关键字，“AAA authentication”和“Authentication through the password of a user terminal interface”是对关键字的描述。
  - “<cr>”表示该位置没有关键字或参数，直接键入回车即可执行。

- 键入一条命令的部分关键字，后接以空格分隔的“?”，如果该位置为参数，则列出有关的参数名和参数描述。举例如下：

```
<HUAWEI> system-view
[HUAWEI] ftp timeout ?
  INTEGER<1-35791>  The value of FTP timeout, the default value is 30 minutes
[HUAWEI] ftp timeout 35 ?
  <cr>
```



```
[HUAWEI] ftp timeout 35
```

其中，“INTEGER<1-35791>”是参数取值的说明，“The value of FTP timeout, the default value is 30 minutes”是对参数作用的简单描述。

部分帮助

当用户输入命令时，如果只记得此命令关键字的开头一个或几个字符，可以使用命令行的部分帮助获取以该字符串开头的所有关键字的提示。下面给出几种部分帮助的实例供参考：

- 键入一字符串，其后紧接“?”，列出以该字符串开头的所有关键字。举例如下：

```
<HUAWEI> d?
  debugging                     delete    dir                           display
<HUAWEI> d
```

- 键入一条命令，后接一字符串紧接“?”，列出命令以该字符串开头的所有关键字。举例如下：

```
<HUAWEI> display b?
  bpdu                          bridge
  buffer
```

- 输入命令的某个关键字的前几个字母，按下**<tab>**键，可以显示出完整的关键字，前提是这几个字母可以唯一标示出该关键字，否则，连续按下<tab>键，可出现不同的关键字，用户可以从中选择所需要的关键字。

说明

以上获取的在线帮助的显示信息仅为示意，请以设备实际显示为准。

1.4 使用 undo 命令行

在命令前加**undo**关键字，即为**undo**命令行。**undo**命令行一般用来恢复缺省情况、禁用某个功能或者删除某项配置。几乎每条配置命令都有对应的**undo**命令行。

下面给出使用undo命令行的示例供参考：

- 使用**undo**命令行恢复缺省情况

  sysname命令是用来设置设备的主机名。举例如下：

```
<HUAWEI> system-view
[HUAWEI] sysname Server
[Server] undo sysname
[HUAWEI]
```

- 使用**undo**命令禁用某个功能

  ftp server enable命令是用来开启设备的FTP服务器功能。举例如下：

```
<HUAWEI> system-view
[HUAWEI] ftp server enable
Warning: FTP is not a secure protocol, and it is recommended to use SFTP.
Info: Succeeded in starting the FTP server.
[HUAWEI] undo ftp server
Info: Succeeded in closing the FTP server.
```

- 使用**undo**命令删除某项设置

  header命令是用来设置用户登录设备时终端上显示的标题信息。举例如下：

```
<HUAWEI> system-view
[HUAWEI] header login information "Hello,Welcome to HUAWEI!"
```

退出设备后重新登录，在验证用户前，会出现“Hello,Welcome to **HUAWEI**!”，然后执行相应的**undo header login**命令：

```
Hello,Welcome to HUAWEI!

Login authentication


Password:
Info: The max number of VTY users is 20, and the number
      of current VTY users on line is 5.
      The current login time is 2012-06-09 04:46:00.
<HUAWEI> system-view
[HUAWEI] undo header login
```

再次退出设备后重新登录，在验证用户前，则不会出现任何标题信息：

```
Login authentication


Password:
Info: The max number of VTY users is 20, and the number
      of current VTY users on line is 5.
      The current login time is 2012-06-09 04:52:10.
<HUAWEI>
```

说明

以上示例中设备的显示信息仅为示意，请以设备实际显示为准。

1.5 批处理操作

背景信息

设备支持自动批处理方式。用户将需要批处理的命令行编辑在批处理文件中，将批处理文件上传至设备，配置设备定时自动执行批处理文件，从而实现设备自动批量执行大量命令。

自动批处理是通过维护助手任务实现的，设备支持最多同时配置5个维护助手任务，每个维护助手任务下可以绑定一个批处理文件，并配置相应的执行时间，当到达执行时间时，设备会自动逐条执行批处理文件中的命令。自动批处理常用于系统定时升级或定时配置。

批处理文件是可执行命令的集合，为***.bat**格式。当批处理文件被执行时，相当于手工逐条执行这些命令。

前置任务

在配置自动批处理方式之前，需要完成以下子任务：

- 在PC上编辑好批处理文件。
- 把批处理文件上传到设备。

说明

如果文件名的后缀不是**.bat**，须修改后缀为**.bat**再上传，或者上传后使用**rename**命令修改。

操作步骤

1. 执行命令**system-view**，进入系统视图。

2. 执行命令**assistant task** *task-name*，创建维护助手任务。
3. 执行命令**if-match timer cron** *seconds minutes hours days-of-month months days-of-week* [*years*]，配置在指定的时间执行维护助手任务。
4. 执行命令**perform** *priority* **batch-file** *filename*，设置维护助手执行的批处理文件。
5. （可选）执行命令**display assistant task history** [*task-name*]，查看维护助手任务历史执行情况。

1.6 在系统视图下执行用户视图命令

背景信息

对于某些命令只能在用户视图下执行，当用户需要执行该类命令时，必须退出到用户视图才能成功执行。为了便于用户在非用户视图下也能够执行用户视图命令，设备提供了**run**命令，使得用户在不用切换视图的情况下，可实现在其他视图下执行用户视图命令。

操作步骤

步骤1 执行命令**run** *command-line*，执行用户视图命令。

参数*command-line*即为用户视图下的命令，目前不支持联想帮助，需手动完整输入。

----结束

1.7 使用命令行的快捷键

系统快捷键是系统中固定的快捷键，不由用户定义，代表固定功能。常用的系统快捷键如表1-2所示。

说明

快捷键的功能可能受用户所用的终端影响，例如用户终端本身自定义的快捷键与设备系统中的快捷键功能发生冲突，此时如果用户键入快捷键将会被终端程序截获而不能执行它所对应的命令行。

系统快捷键

表 1-2 系统快捷键

功能键	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。

功能键	功能
<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+J>	换行功能。
<Ctrl+K>	在连接建立阶段终止呼出的连接。
<Ctrl+M>	换行功能。
<Ctrl+N>	显示历史命令缓冲区中的后一条命令。
<Ctrl+P>	显示历史命令缓冲区中的前一条命令。
<Ctrl+R>	重新显示当前行信息。
<Ctrl+T>	终止呼出的连接。
<Ctrl+V>	粘贴剪贴板的内容。
<Ctrl+W>	删除光标左侧的一个字符串（字）。
<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>	返回到用户视图。
<Ctrl+]>	终止呼入的连接或重定向连接。
<Esc+B>	将光标向左移动一个字符串（字）。
<Esc+D>	删除光标右侧的一个字符串（字）。
<Esc+F>	将光标向右移动一个字符串（字）。
<Esc+N>	将光标向下移动一行。
<Esc+P>	将光标向上移动一行。

1.8 查询命令行的配置信息

当用户在某一视图下完成一组配置之后，需要检查配置是否正确。例如，在完成FTP服务器的各项配置后，可以执行命令**display ftp-server**，查看当前FTP服务器的各项参数。**display**命令的用法和功能可参见相应特性的命令参考。

同时，系统支持查看当前生效的配置信息和当前视图下的配置信息，命令如下：

- 查看当前生效的配置信息：

  display current-configuration

  对于某些正在生效的配置参数，如果与缺省参数相同，则不显示。
- 查看当前视图下生效的配置信息：

  display this

  对于某些正在生效的配置参数，如果与缺省参数相同，则不显示。

如果还需要显示当前视图下未被修改的缺省配置，可以执行命令**display this include-default**进行查看。

1.9 控制命令行显示

- 当终端屏幕上显示的信息过多时，可以使用<PageUp>和<PageDown>显示上一页信息和下一页信息。
- 当执行某一命令后，如果显示的信息超过一屏时，系统会自动暂停，以方便用户查看。此时用户可以通过功能键控制命令行的显示方式，如表1-3所示。

  表 1-3 控制命令行显示方式

功能键	功能
键入<Ctrl+C>或<Ctrl+Z>	停止显示或命令执行。 **说明** 也可以键入除空格键、回车键外的其他键（可以是数字键或字母键）停止显示和命令执行。
键入空格键	继续显示下一屏信息。
键入回车键	继续显示下一行信息。

  screen-length *screen-length* **temporary**命令可以用来设置当前终端屏幕每屏显示的行数，如果*screen-length*取值为0则关闭分屏功能，即当显示的信息超过一屏时，系统不会自动暂停。
- 设备除提供了命令执行后的信息显示控制方法，还可以控制命令行输入时的回显模式。

  命令行回显模式分为字符模式和行模式，可通过**terminal echo-mode** { **character** | **line** }，设置命令行回显模式，缺省情况下为字符模式。
  - **character**：指定命令行回显模式是字符模式。输入命令行时，用户输入一个字符系统回显一个字符。
  - **line**：指定命令行回显模式是行模式。输入命令行时，用户输入字符后，只有键入回车键、Tab键或？键，系统才回显输入的字符。

  通过网管操作设备时，为了提高网管操作设备的效率，可将命令行回显模式修改为**line**模式。普通用户建议使用**character**模式，否则会影响命令行使用习惯，从而降低了操作设备的效率。

1.10 使用正则表达式过滤命令行显示信息

正则表达式

使用display命令查看设备的配置信息和运行状态信息时，可以通过正则表达式过滤不需要的信息。正则表达式（regular-expression）是一种模式匹配工具，用户根据一定的规则构建匹配模式，然后将匹配模式与目标对象进行匹配。正则表达式格式上是由1～256个普通字符和特殊字符组成的字符串。

- 普通字符

普通字符匹配的对象是普通字符本身。包括所有的大写和小写字母、数字、下划线、标点符号以及一些特殊符号。例如：a匹配abc中的a，20匹配20.1.1.1中的20，@匹配xxx@xxx.com中的@。

- 特殊字符

  为帮助用户灵活地构建匹配模式，正则表达式提供了一些具有特殊含义的专用字符，也称为“元字符”（metacharacter）。这些特殊字符用来规定其它字符在目标对象中的出现模式。表1-4是对特殊字符及其语法意义的使用描述。

表 1-4 特殊字符及其语法意义描述

特殊字符	功能	举例
\	转义字符。将下一个字符（特殊字符或者普通字符）标记为普通字符。	*匹配*
^	匹配行首的位置。	^10匹配10.10.10.1，不匹配20.10.10.1
$	匹配行尾的位置。	1$匹配10.10.10.1，不匹配10.10.10.2
*	匹配前面的子正则表达式零次或多次。	10*可以匹配1、10、100、1000、…… (10)*可以匹配空、10、1010、101010、……
+	匹配前面的子正则表达式一次或多次。	10+可以匹配10、100、1000、…… (10)+可以匹配10、1010、101010、……
?	匹配前面的子正则表达式零次或一次。 **说明** 当前，在华为公司数据通信设备上运用正则表达式输入？时，系统显示为命令行帮助功能。华为公司数据通信设备不支持正则表达式输入？特殊字符。	10?可以匹配1或者10 (10)?可以匹配空或者10
.	匹配任意单个字符。	0.0可以匹配0x0、020、…… .oo.可以匹配book、look、tool、……
()	一对圆括号内的正则表达式作为一个子正则表达式，匹配子表达式并获取这一匹配。圆括号内也可以为空。	100(200)+可以匹配100200、100200200、……
x|y	匹配x或y。	100|200匹配100或者200 1(2|3)4匹配124或者134，而不匹配1234、14、1224、1334

特殊字符	功能	举例
[xyz]	匹配正则表达式中包含的任意一个字符。	[123]匹配255中的2
[^xyz]	匹配正则表达式中未包含的字符。	[^123]匹配除123之外的任何字符
[a-z]	匹配正则表达式指定范围内的任意字符。	[0-9]匹配0到9之间的所有数字
[^a-z]	匹配正则表达式指定范围外的任意字符。	[^0-9]匹配所有非数字字符

最简单的正则表达式不包含任何特殊字符，例如，可以定义一个正则表达式“hello”，它只匹配字符串“hello”。实际应用中，往往是由多个普通字符和特殊字符组合使用，匹配某些特征的字符串。

- 特殊字符的退化

  某些特殊字符如果处在如下的正则表达式的特殊位置时，会引起退化，成为普通字符。

  - 特殊字符处在转义符号‘\’之后，则发生转义，变为匹配该字符本身。
  - 特殊字符“*”、“+”、“?”，处于正则表达式的第一个字符位置。例如：+45匹配+45，abc(*def)匹配abc*def。
  - 特殊字符“^”，不在正则表达式的第一个字符位置。例如：abc^匹配abc^。
  - 特殊字符“$”，不在正则表达式的最后一个字符位置。例如：12$2匹配12$2。
  - 右括号“)”或者“]”没有对应的左括号“(”或“[”。例：abc)匹配abc)，0-9]匹配0-9]。

  说明

  除非特别说明，特殊字符的退化也适用于括号“（ ）”内包含的子正则表达式。

正则表达式的使用方法

须知

交换机采用正则表达式实现管道符的过滤功能。并非所有display命令均支持指定过滤方式，一般只有显示信息较多的命令才支持。

如果显示信息较多，查看过滤后的配置信息时系统需要较长的时间才能获取正确的信息，因此需要用户等待一段时间。

使用正则表达式过滤命令行显示信息的方法有两种：

- 在命令中指定过滤方式：在命令行中通过输入**begin**、**exclude**或**include**关键字加正则表达式的方式来过滤显示。

- 在分屏显示时指定过滤方式：在分屏显示时，使用“/”、“-”或“+”符号加正则表达式的方式，可以对还未显示的信息进行过滤显示。其中，“/”等同关键字**begin**；“-”等同关键字**exclude**；“+”等同关键字**include**。

在命令中指定过滤方式

系统支持使用**| count**，显示使用过滤条件后输出的结果的行数。可以与过滤方式配合使用。

在支持正则表达式的命令中，有三种过滤方式可供选择：

- **| begin** *regular-expression*：输出以匹配指定正则表达式的行开始的所有行。

  即过滤掉所有待输出字符串，直到出现指定的字符串（此字符串区分大小写）为止，其后的所有字符串都会显示到界面上。
- **| exclude** *regular-expression*：输出不匹配指定正则表达式的所有行。

  即待输出的字符串中没有包含指定的字符串（此字符串区分大小写），则会显示到界面上；否则过滤不显示。
- **| include** *regular-expression*：只输出匹配指定正则表达式的所有行。

  即待输出的字符串中如果包含指定的字符串（此字符串区分大小写），则会显示到界面上；否则过滤不显示。

  *regular-expression*为字符串形式（不包括中文），长度范围是1～255。

说明

对于某些输出信息较多的display命令，可以指定输出信息的过滤方式。

系统对命令的显示信息进行过滤后，还支持上下文显示规则。上下文显示规则有如下几种：

- **before** *before-line-number*：输出符合过滤规则的行和其前面*before-line-number*行的数据信息。
- **after** *after-line-number*：输出符合过滤规则的行和其后面*after-line-number*行的数据信息。
- **before** *before-line-number* + **after** *after-line-number*或者**after** *after-line-number* + **before** *before-line-number*：输出符合过滤规则的行和其前面*before-line-number*行、后面*after-line-number*行的数据信息。

  *before-line-number*和*after-line-number*参数均为整数形式，取值范围是1～999。

下面举例来说明在命令中指定过滤方式的用法。

例1：执行命令**display interface brief**，显示不匹配“Ethernet”、“NULL”或“Tunnel”的所有行。

```
<HUAWEI> display interface brief | exclude Ethernet|NULL|Tunnel
PHY: Physical
*down: administratively down
^down: standby
(l): loopback
(s): spoofing
(b): BFD down
(e): ETHOAM down
(dl): DLDP down
(d): Dampening Suppressed
InUti/OutUti: input utility/output utility
Interface                   PHY    Protocol InUti OutUti   inErrors  outErrors
Eth-Trunk1                  down   down       0%     0%          0          0
Eth-Trunk17                 down   down       0%     0%          0          0
```

```
LoopBack1               up    up(s)      0%     0%         0         0
Vlanif1                 up    down       --     --         0         0
MEth0/0/1               down  down       0%     0%         0         0
Vlanif2                 down  down       --     --         0         0
Vlanif10                down  down       --     --         0         0
Vlanif12                down  down       --     --         0         0
Vlanif13                down  down       --     --         0         0
Vlanif20                up    up         --     --         0         0
Vlanif22                down  down       --     --         0         0
Vlanif222               down  down       --     --         0         0
Vlanif4094              down  down       --     --         0         0
```

例2：执行命令**display current-configuration**，只显示匹配正则表达式“vlan”的所有行。

```
<HUAWEI> display current-configuration | include vlan
vlan batch 2 10 101 to 102 800 1000
vlan 2
vlan 10
 port trunk pvid vlan 800
 undo port trunk allow-pass vlan 1
 port trunk allow-pass vlan 10 101 800
 undo port hybrid vlan 1
 undo port hybrid vlan 1
 port hybrid untagged vlan 10
 undo port hybrid vlan 1
 undo port hybrid vlan 1
```

例3：通过使用after，输出符合过滤规则的行和对应的数据信息（before用法相同）。

```
<HUAWEI> display ip routing-table | after 2 include
0.0.0.0
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 16        Routes : 16

Destination/Mask    Proto   Pre  Cost      Flags NextHop
Interface

######## The information is filtered ########
      10.3.0.0/16  Static  60   0           D   0.0.0.0         NULL0
      10.8.0.0/16  Static  60   0           D   0.0.0.0         NULL0
    10.18.20.0/24  Direct  0    0           D   10.18.20.254    Vlanif20
  10.18.20.254/32  Direct  0    0           D   127.0.0.1       Vlanif20
######## The information is filtered ########
     120.0.0.0/8   Static  60   0          RD   120.51.55.1     MEth0/0/1
   120.51.55.0/24  Direct  0    0           D   120.51.55.44    MEth0/0/1
  120.51.55.44/32  Direct  0    0           D   127.0.0.1       MEth0/0/1
```

说明

以上举例的显示信息仅为示意，请以设备实际显示为准。

在分屏显示时指定过滤方式

支持在分屏显示时指定过滤方式的命令行有：

- **display current-configuration**
- **display interface**
- **display arp**

采用分屏显示时，可以在分屏提示符“---- More ----”中指定过滤类型：

- /*regular-expression*：输出以匹配指定正则表达式的行开始的所有行。
- -*regular-expression*：输出不匹配指定正则表达式的所有行。

- *+regular-expression*：只输出匹配指定正则表达式的所有行。

例如：执行命令**display current-configuration**，当分屏显示时，在余下的回显中仅显示Vlanif相关的信息。

```
<HUAWEI> display current-configuration
!Software Version V200R022C00
#
sysname HUAWEI
#
vlan batch 10 to 11 100
#
hotkey CTRL_G "display tcp status"
#
lldp enable
#
undo http server enable
undo http secure-server enable
#
dhcp enable
#
dhcp snooping enable
+Vlanif          //输入过滤方式

Filtering...
interface Vlanif10
interface Vlanif100
```

1.11 设置命令级别

背景信息

为了限制不同用户对设备的访问权限，系统对用户也进行了分级管理。用户的级别与命令级别对应，不同级别的用户登录后，只能使用等于或低于自己级别的命令。缺省情况下，命令级别按0～3级进行注册，用户级别按0～15级进行注册，用户级别和命令级别对应关系如表1-5所示。

表 1-5 命令级别与用户级别的关系

命令级别	说明	举例	用户级别
参观级（0级）	网络诊断命令	• **tracert** • **ping**	所有级别（0～15级）
	访问外部设备命令	• **telnet** • **stelnet**	
监控级（1级）	系统维护命令	**display**命令 **说明** 并不是所有display命令都是监控级，比如**display current-configuration**命令和**display saved-configuration**命令是3级管理级。	不低于监控级（1～15级）
配置级（2级）	业务配置命令	路由配置命令	不低于配置级（2～15级）

命令级别	说明	举例	用户级别
管理级（3级）	系统基本运行命令	• 用户管理 • 命令级别设置 • 系统参数设置 • **debugging**命令	管理级（3～15级）
	系统支撑模块命令	• 文件系统 • FTP/TFTP下载 • 配置文件切换命令	

各命令的级别请参见《S300, S500, S2700, S5700, S6700 V200R022C00 命令参考》。

缺省的命令级别设置已基本可以满足用户对操作权限的控制，一般不需要重新设置。如果对用户操作权限有特殊要求，需要调整某级别的用户可进行的操作，例如希望只有4级及以上用户才可以执行**stelnet**命令，设备提供了调整命令行级别的功能，可以将**stelnet**命令的级别提升至4级。

调整命令行级别，不仅可以提升命令行的级别，也包含降低命令行的级别。

说明

不建议随意修改缺省的命令级别，否则会影响其他用户对命令的使用。另外某条命令的级别被单独修改后，批量提升命令级别，此时命令级别将保持不变，所以需要同时进行命令的批量提升和逐条提升时，建议先执行批量提升。

由于某些命令是否能够执行需要依赖其他条件，如只有配置其他命令后才能配置该命令，或该命令本身为升级兼容命令等，当执行**command-privilege level**命令对这些命令进行级别调整后，调整后的命令不一定能够执行。即命令级别的调整与该命令是否能够执行没有必然联系。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 设置命令级别。

- 执行命令**command-privilege level** *level* **view** *view-name command-key*，设置指定视图内命令的级别。
- 执行命令**command-privilege level rearrange**，批量提升命令的级别。
  - 对于没有单独调整过级别的命令，批量提升命令级别后，按以下原则自动调整：
    - 0级和1级命令保持级别不变。
    - 2级命令提升到10级，3级命令提升到15级。
    - 2～9级和11～14级这些命令级别中没有命令行。用户可以单独调整需要的命令行到这些级别中，以实现用户权限的精细化管理。
  - 对于执行**command-privilege level** *level* **view** *view-name command-key* 命令修改过命令级别的命令，批量提升命令级别后，维持原来级别不变。

在执行此命令之前，用户需要确保自己的级别为15级，否则无法执行该命令。

----结束

1.12 查看历史命令

设备能够自动保存用户键入的历史命令。当用户需要输入之前已经执行过的命令时，可以调用设备保存的历史命令。

缺省情况下，为每个登录用户保存10条历史命令。可以通过**history-command max-size** *size-value*命令在相应的用户界面视图下重新设置保存历史命令的条数，最大设置为256。

说明

不推荐用户将此值设置过大，因为可能会花费较长时间才查看到所需要的历史命令，反而影响配置效率。

对历史命令的操作如表1-6所示。

表 1-6 访问历史命令

操作	命令或功能键	结果
显示历史命令	**display history-command** [**all-users**]	• 不指定**all-users**，显示当前用户键入的历史命令。 • 指定**all-users**，显示的是所有登录用户键入的历史命令。（3级及3级以上的用户才能执行此参数）
访问上一条历史命令	上光标键或者<Ctrl+P>	如果还有更早的历史命令，则取出上一条历史命令，否则响铃警告。
访问下一条历史命令	下光标键或者<Ctrl+N>	如果还有更新的历史命令，则取出下一条历史命令，否则显示为空，响铃警告。

说明

对于Windows 9X的超级终端，↑光标键无效，这是由于Windows 9X的超级终端对这个键作了不同解释，这时可以用快捷键<Ctrl+P>代替↑光标键达到同样目的。

在使用历史命令功能时，需要注意：

- 保存的历史命令与用户输入的命令格式相同，如果用户使用了命令的不完整形式，保存的历史命令也是不完整形式。
- 如果用户多次执行同一条命令，则历史命令中只保留最近的一次。但如果执行时输入的形式不同，将作为不同的命令对待。

例如：多次执行**display current-configuration**命令，历史命令中只保存一条。如果执行**display current-configuration**和**dis curr**，将保存为两条历史命令。

- 当前用户的历史命令可以在所有视图下通过**reset history-command**命令进行清除，清除后则无法显示和访问之前执行过的历史命令。如果需要清除所有用户的历史命令，则需要3级及3级以上的用户执行**reset history-command** [**all-users**]命令进行清除。

2 登录密码管理

本章节主要介绍了基于框&盒交换机多个版本的登录密码相关内容。

2.1 设备登录的缺省密码
2.2 恢复Console口登录密码
2.3 恢复Telnet登录密码
2.4 恢复STelnet登录密码
2.5 恢复BootLoad密码
2.6 恢复Web登录密码

2.1 设备登录的缺省密码

您可以在《S系列交换机缺省帐号与密码》（**企业网**、**运营商**）文档中获取各种缺省帐号与密码信息。获取该文档需要权限，如需升级权限，请查看网站帮助。

说明

为充分保证设备安全，请定期修改密码。

2.2 恢复 Console 口登录密码

如果忘记了Console口登录密码或者希望修改Console口登录密码，用户可以通过以下两种方式来设置新的Console口登录密码。

通过 STelnet/Telnet 登录交换机设置新的 Console 口登录密码

须知

使用Telnet协议存在安全风险，建议用户使用STelnet V2登录设备。

这种方法的前提是：用户拥有STelnet/Telnet账号并且具有管理员的权限。以下涉及的命令行及回显信息以STelnet登录设备修改Console口密码为例。用户通过STelnet账号登录交换机后，请按照如下步骤进行配置。

以登录用户界面的认证方式为密码认证，密码为YsHsjx_202206为例，配置如下。

```
<HUAWEI> system-view
[HUAWEI] user-interface console 0
[HUAWEI-ui-console0] authentication-mode password
[HUAWEI-ui-console0] set authentication password cipher YsHsjx_202206
[HUAWEI-ui-console0] return
<HUAWEI> save
```

#以登录用户界面的认证方式为AAA认证，用户名为**admin123**，密码为YsHsjx_202206为例，配置如下。

```
<HUAWEI> system-view
[HUAWEI] user-interface console 0
[HUAWEI-ui-console0] authentication-mode aaa
[HUAWEI-ui-console0] quit
[HUAWEI] aaa
[HUAWEI-aaa] local-user admin123 password irreversible-cipher YsHsjx_202206
[HUAWEI-aaa] local-user admin123 service-type terminal
[HUAWEI-aaa] return
<HUAWEI> save
```

通过 BootLoad 清除 Console 口登录密码

说明

多台设备堆叠情况下，先将成员交换机下电，在主交换机上完成以下操作后，执行save命令，以保证启动其他成员设备后能同步主交换机上的配置。

交换机的BootLoad提供了清除Console口登录密码的功能，用户可以在交换机启动后修改Console口登录密码，然后保存配置。请按照如下步骤进行配置。

1. 通过Console口连接交换机，并重启交换机。

   当界面出现以下打印信息时，及时按下快捷键“Ctrl+B”并输入BootLoad密码，进入BootLoad主菜单。

   ```
   Press Ctrl+B to enter BootLoad menu ... 2
   password:     //输入BootLoad密码
   ```

   说明

   不同版本和不同形态的设备回显有差异，请以实际设备显示为准。

   您可以在《S系列交换机缺省帐号与密码》（企业网、运营商）文档中获取各种缺省帐号与密码信息。获取该文档需要权限，如需升级权限，请查看网站帮助。

2. 在BootLoad主菜单下选择“Clear password for console user”清除Console口登录密码。
3. 根据交换机的提示，在BootLoad主菜单下选择“Boot with default mode”启动设备。

   说明

   请注意，此处不要选择“Reboot”选项，否则此次清除密码将失效。

4. 完成系统启动后，通过Console口登录时不需要认证，登录后按照系统提示配置验证密码。（V200R009及之后版本，完成系统启动后，通过Console口登录时认证方式为None，系统启动后不会提示配置验证密码。）
5. 登录交换机后，用户可以根据需要配置Console用户界面的认证方式及密码。

相关信息

视频

如何恢复Console口密码

2.3 恢复 Telnet 登录密码

如果忘记了Telnet登录密码或者希望修改Telnet登录密码，用户可以通过Console口登录交换机后设置新的Telnet登录密码。

说明

以下涉及的命令行以V200R008C00版本的S7700交换机为例。

通过Console口登录设备。

1. 将Console通信电缆的DB9（孔）插头插入PC机的串口（COM）中，再将RJ-45插头端插入设备的Console口中。
2. 在PC上打开终端仿真软件，新建连接，设置连接的接口，配置通信参数如下：
   - 波特率：9600
   - 数据位：8
   - 停止位：1
   - 奇偶校验位：无
   - 流控：无
3. 单击“Connect”，根据提示输入或配置登录密码，完成登录。

以登录VTY0的验证方式为密码验证，密码为YsHsjx_202206为例，配置如下。

```
<HUAWEI> system-view
[HUAWEI] user-interface vty 0
[HUAWEI-ui-vty0] protocol inbound telnet  //V200R006及之前版本缺省使用的协议为Telnet协议，可以不配置该项；V200R007及之后版本缺省使用的协议为SSH协议，必须配置。
[HUAWEI-ui-vty0] authentication-mode password
[HUAWEI-ui-vty0] set authentication password cipher YsHsjx_202206
[HUAWEI-ui-vty0] user privilege level 15
[HUAWEI-ui-vty0] return
<HUAWEI> save
```

以登录VTY0的验证方式为AAA授权验证，用户名为**admin123**，密码为YsHsjx_202206为例，配置如下。

```
<HUAWEI> system-view
[HUAWEI] user-interface vty 0
[HUAWEI-ui-vty0] protocol inbound telnet  //V200R006及之前版本缺省使用的协议为Telnet协议，可以不配置该项；V200R007及之后版本缺省使用的协议为SSH协议，必须配置。
[HUAWEI-ui-vty0] authentication-mode aaa
[HUAWEI-ui-vty0] quit
[HUAWEI] aaa
[HUAWEI-aaa] local-user admin123 password irreversible-cipher YsHsjx_202206
[HUAWEI-aaa] local-user admin123 service-type telnet
[HUAWEI-aaa] local-user admin123 privilege level 15
Warning: This operation may affect online users, are you sure to change the user privilege level ?[Y/N]y
[HUAWEI-aaa] return
<HUAWEI> save
```

2.4 恢复 STelnet 登录密码

如果忘记了STelnet登录密码或者希望修改STelnet登录密码，用户可以通过Console口登录交换机后设置新的STelnet登录密码。

通过Console口登录设备。

1. 将Console通信电缆的DB9（孔）插头插入PC机的串口（COM）中，再将RJ-45插头端插入设备的Console口中。
2. 在PC上打开终端仿真软件，新建连接，设置连接的接口，配置通信参数如下：
   - 波特率：9600
   - 数据位：8
   - 停止位：1
   - 奇偶校验位：无
   - 流控：无
3. 单击“Connect”，根据提示输入或配置登录密码，完成登录。

以登录VTY0的验证方式为密码验证，用户名为**admin123**，密码为YsHsjx_202206为例，配置如下。

```
<HUAWEI> system-view
[HUAWEI] user-interface vty 0
[HUAWEI-ui-vty0] authentication-mode aaa
[HUAWEI-ui-vty0] user privilege level 15
[HUAWEI-ui-vty0] quit
[HUAWEI] ssh user admin123
[HUAWEI] ssh user admin123 service-type stelnet
[HUAWEI] ssh user admin123 authentication-type password
[HUAWEI] aaa
[HUAWEI-aaa] local-user admin123 password irreversible-cipher YsHsjx_202206
[HUAWEI-aaa] local-user admin123 privilege level 15
[HUAWEI-aaa] local-user admin123 service-type ssh
[HUAWEI-aaa] quit
[HUAWEI] ecc local-key-pair create
Info: The key name will be: HUAWEI_Host_ECC.
Info: The key modulus can be any one of the following: 256, 384, 521.
Info: If the key modulus is greater than 512, it may take a few minutes.
Please input the modulus [default=521]:521
Info: Generating keys.....
Info: Succeeded in creating the ECC host keys.
[HUAWEI] return
<HUAWEI> save
```

以登录VTY0的验证方式为ECC验证（RSA、DSA认证类似，不再赘述），用户名为**admin123**，密码为YsHsjx_202206为例，配置如下。

```
<HUAWEI> system-view
[HUAWEI] user-interface vty 0
[HUAWEI-ui-vty0] authentication-mode aaa
[HUAWEI-ui-vty0] user privilege level 15
[HUAWEI-ui-vty0] quit
[HUAWEI] ssh user admin123
[HUAWEI] ssh user admin123 service-type stelnet
[HUAWEI] ssh user admin123 authentication-type ecc
[HUAWEI] ecc peer-public-key key01 encoding-type pem
Enter "ECC public key" view, return system view with "peer-public-key end".
[HUAWEI-ecc-public-key] public-key-code begin    //进入公共密钥编辑视图
Enter "ECC key code" view, return last view with "public-key-code end".
[HUAWEI-ecc-public-code] 308188   //拷贝复制客户端的公钥，为十六进制字符串
[HUAWEI-ecc-public-code] 028180
[HUAWEI-ecc-public-code] B21315DD 859AD7E4 A6D0D9B8 121F23F0 006BB1BB
[HUAWEI-ecc-public-code] A443130F 7CDB95D8 4A4AE2F3 D94A73D7 36FDFD5F
[HUAWEI-ecc-public-code] 411B8B73 3CDD494A 236F35AB 9BBFE19A 7336150B
[HUAWEI-ecc-public-code] 40A35DE6 2C6A82D7 5C5F2C36 67FBC275 2DF7E4C5
[HUAWEI-ecc-public-code] 1987178B 8C364D57 DD0AA24A A0C2F87F 474C7931
[HUAWEI-ecc-public-code] A9F7E8FE E0D5A1B5 092F7112 660BD153 7FB7D5B2
[HUAWEI-ecc-public-code] 171896FB 1FFC38CD
[HUAWEI-ecc-public-code] 0203
[HUAWEI-ecc-public-code] 010001
[HUAWEI-ecc-public-code] public-key-code end  //退回到公共密钥视图
[HUAWEI-ecc-public-key] peer-public-key end   //退回到系统视图
```



```
[HUAWEI] ssh user admin123 assign ecc-key key01  //为用户admin123分配一个已经存在的公钥key01
[HUAWEI] ecc local-key-pair create
Info: The key name will be: HUAWEI_Host_ECC.
Info: The key modulus can be any one of the following: 256, 384, 521.
Info: If the key modulus is greater than 512, it may take a few minutes.
Please input the modulus [default=521]:521
Info: Generating keys.....
Info: Succeeded in creating the ECC host keys.
[HUAWEI] return
<HUAWEI> save
```

2.5 恢复 BootLoad 密码

如果希望修改BootLoad登录密码，用户可以通过以下方式重置或设置新的BootLoad密码。

通过 BootLoad 修改 BootLoad 密码

说明

此方法是在已知BootLoad密码的前提下才可使用。

如果交换机是双主控，则需要在执行以下操作前将备用主控板拔下，待执行完以下操作后，再插上备用主控板，执行save命令以保证主用主控板和备用主控板配置一致。

多台设备堆叠情况下，先将成员交换机下电，在主交换机上完成以下操作后，执行**save**命令，以保证启动其他成员设备后能同步主交换机上的配置。

交换机的BootLoad提供了重置BootLoad密码的功能，用户可以在交换机启动过程中修改BootLoad密码，然后保存配置。请按照如下步骤进行配置。

1. 通过Console口连接交换机，并重启交换机。

   当界面出现以下打印信息时，及时按下快捷键“Ctrl+B”或者“Ctrl+E”并输入BootLoad密码，进入BootLoad主菜单。

   ```
   Press Ctrl+B to enter BootLoad menu ... 2
   password:     //输入BootLoad密码
   ```

   说明

   不同版本和不同形态的设备回显有差异，请以实际设备显示为准。

2. 在BootLoad主菜单下选择“Enter password submenu”进入密码子菜单。
3. 请根据交换机的提示，在密码子菜单下选择“Reset bootload password”或者“Modify bootload password”，对BootLoad密码进行修改。

2.6 恢复 Web 登录密码

如果忘记了Web登录密码或者希望修改Web登录密码，用户可以通过Console口、Telnet或STelnet方式登录交换机后设置新的Web登录密码。

须知

Telnet协议存在安全风险，建议用户通过Console口或STelnet V2方式登录设备。

以用户名为**admin123**，密码为YsHsjx_202206为例，配置如下。

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] local-user admin123 password irreversible-cipher YsHsjx_202206
[HUAWEI-aaa] local-user admin123 service-type http
[HUAWEI-aaa] local-user admin123 privilege level 15
Warning: This operation may affect online users, are you sure to change the user privilege level ?[Y/N]y
[HUAWEI-aaa] return
<HUAWEI> save
```


3 EasyDeploy 配置

3.1 EasyDeploy简介
3.2 EasyDeploy原理描述
3.3 EasyDeploy配置注意事项
3.4 EasyDeploy缺省配置
3.5 通过Option参数实现零配置设备部署
3.6 通过中间文件实现零配置设备部署
3.7 通过中间文件实现带配置设备部署
3.8 通过Commander实现零配置设备部署
3.9 通过Commander实现手动替换故障设备
3.10 通过Commander实现自动替换故障设备
3.11 通过Commander批量升级设备
3.12 通过Commander批量配置设备
3.13 将有配置设备加入Commander管理
3.14 维护EasyDeploy
3.15 EasyDeploy配置举例

3.1 EasyDeploy 简介

定义

EasyDeploy是一系列易操作和易维护功能的集合，为方便用户对设备进行简单的运维操作提供了解决方案。

EasyDeploy使设备能够自动加载版本文件，包括系统软件、补丁文件、Web文件和配置文件。它简化了网络配置，实现了远程服务部署和集中管理。

目的

EasyDeploy可以提高设备部署、日常维护和故障处理的效率，降低人力成本。

EasyDeploy可以应用于以下场景：

- 零配置设备部署

  在现网部署交换机设备，当设备安装完成后，无需网络管理员到安装现场对设备进行软件调试，在设备满足零配置的条件下，设备上电后即可自动加载配置文件、补丁文件等系统文件。零配置设备部署时，可以不指定配置文件。

  零配置是指设备本次使用的配置文件和下次启动时使用的配置文件为空。

  在零配置部署场景中，兼容了原有的Auto-Config特性的功能和流程。

- 带配置设备部署

  在现网中部署交换机设备，设备出厂时可以自带定制化的配置文件，配置文件中包含了带配置部署相关的命令行，用以指定文件服务器地址、开局使用的中间文件名、设备与SNMP主机的共享密钥等。用户仅需简单地配置设备上线，设备就可以自动获取并加载正确的配置，减少用户的操作成本。

  带配置是指设备出厂时已经带有包含带配置部署相关命令的配置文件。

- 故障设备替换

  在现网日常维护中，EasyDeploy可以实现定时保存配置文件到文件服务器。当设备发生故障时，更换后的新的零配置设备按照替换信息下载原设备的配置文件并激活，保证设备的即插即用。

- 批量升级

  在现网日常维护中，EasyDeploy可以将升级文件相同的设备规划为一个Group，网络管理员只需要给Group指定升级文件，即可实现批量升级设备的功能。

- 批量配置

  在现网日常维护中，EasyDeploy可以将命令行编辑成脚本，集中下发到设备执行，而无需用户一条一条进行配置。

- 有配置设备加入Commander管理

  在运行EasyDeploy功能的网络中，如果希望对有配置设备进行监控和管理，则可以将有配置设备加入Commander的管理。

说明

在有配置的设备上，EasyDeploy支持DTLS（Datagram Transport Layer Security）加密，DTLS加密默认开启。零配置设备部署场景，不受DTLS加密是否开启的限制，可以正常部署。

相关信息

视频

（多媒体）S系列交换机ZTP特性介绍

3.2 EasyDeploy 原理描述

3.2.1 EasyDeploy 基本概念

EasyDeploy特性中涉及的基本概念如下。

Commander

作为管理者的角色。Commander与Client间的通信是采用UDP单播报文，默认的端口号60000。

Commander的作用如下：

- 管理Client的与部署相关的信息，建立信息数据库。
- 给网络中的Client分配文件服务器地址、用户名、密码、系统软件名、配置文件名、License文件名、补丁文件名，Web网页文件名、自定义文件名。
- 统一控制和管理Client，控制和信息查询都在Commander上完成。

Client

作为被管理者的角色。Client从Commander上获取下载文件信息后，再根据这些信息从文件服务器上下载指定文件，最终实现指定文件的自动加载。

说明

若没有特殊说明，本文中的Client专指Commander方式中的待配置设备，是相对于Commander的一种角色。

Group

为了进一步简化配置，可以将需要下载的文件相同的Client划分到一个设备群组Group中。Commander上支持配置多种自定义Group，用户可以根据网络设备的部署情况，选择适合的匹配方式。

Group有两种方式：

- 内置Group：根据设备类型匹配。适合相同设备类型的Client加载相同的系统文件、补丁文件或Web网页文件等其他相同文件。
- 自定义Group：可以根据MAC地址、ESN序列号、IP地址、设备型号和设备类型匹配。用户可以根据网络中设备的部署自行选择相应类型的Group。此处的设备类型是用来兼容新的Client的设备类型。

文件服务器

支持SFTP/FTP/TFTP服务器。文件服务器存放待配置设备需要加载的文件，包括系统软件、配置文件、License文件、补丁文件和Web文件等。

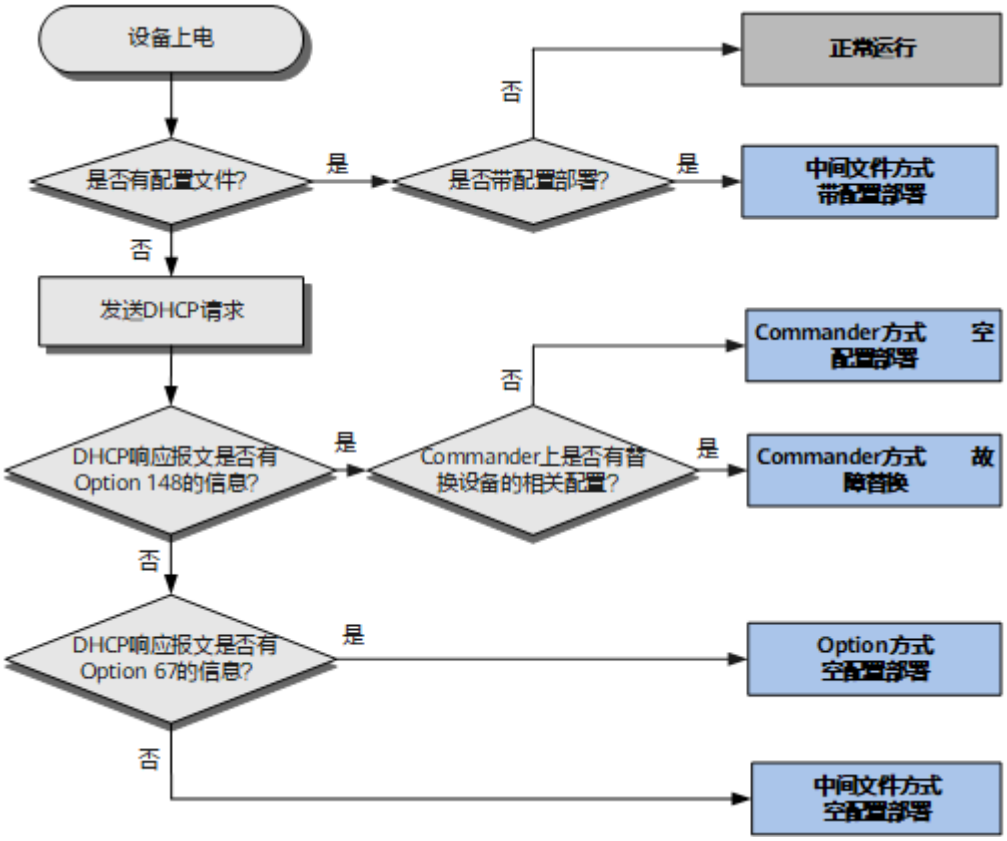
说明

由于文件服务器需要占用设备的存储资源，因此用户在决定使用S系列交换机作为文件服务器时，需要预留充足的存储空间。

DHCP 服务器

在零配置部署、带配置部署和故障替换场景下，DHCP服务器可以为待配置设备分配IP地址。当设备上电启动EasyDeploy流程后，待配置设备会根据设备上是否有配置文件以及DHCP服务器上Option参数的配置选择不同的实现方式，判断流程如图3-1所示。

图 3-1 EasyDeploy 启动后的流程判断机制



中间文件

可以通过中间文件解析出需要下载的版本文件信息实现零配置部署或带配置部署的功能。中间文件存放在文件服务器上，文件内容为下载文件信息，格式为设备MAC地址或ESN序列号与待下载文件的对应关系。带配置部署场景下，中间文件中还应包括SNMP主机的IP地址。

S系列交换机的中间文件名称可以编辑，后缀为.cfg。

当有多台设备需要配置时，中间文件的每行对应一台设备的配置信息。

例如：一台设备的MAC地址为xxxx-xxxx-xxxx，对应这台设备应下载的系统软件名称为easy_V200R022C00.cc，版本号信息为V200R022C00SPC100，补丁文件为easy_V200R022C00.pat，配置文件名称为easy_V200R022C00.cfg，Web文件名称为easy.web.7z。则中间文件内容为：

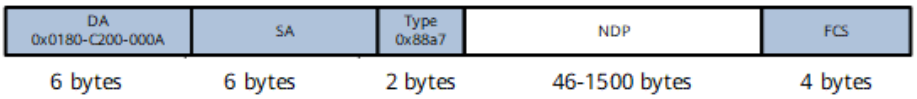
```
mac=xxxx-xxxx-
xxxx;vrpfile=easy_V200R022C00.cc;vrpver=V200R022C00SPC100;patchfile=easy_V200R022C00.pat;cfgfile=easy_V200R022C00.cfg;webfile=easy.web.7z;
```

NDP

邻居发现协议NDP（Neighbor Discovery Protocol），是华为公司的私有协议，用来收集邻居设备的信息，如邻居设备的连接接口和软件版本等。

NDP报文承载于Ethernet-II帧，以组播目的MAC地址周期性发送。设备根据收到的邻居的NDP报文生成NDP信息表。NDP报文结构如图3-2所示。

图 3-2 NDP 报文结构



各字段含义如下：

- DA（Destination MAC Address）：目的MAC地址，为固定的组播MAC地址0x0180-C200-000A。
- SA（Source MAC Address）：源MAC地址，为固定的MAC地址0x00e0-fc09-bcf9。
- Type：报文类型，NDP报文中该字段的值为0x88a7。
- NDP：NDP数据单元，NDP信息交换的主体。
- FCS：帧检验序列。

NDP协议在维护NDP信息表时使用两个定时器：

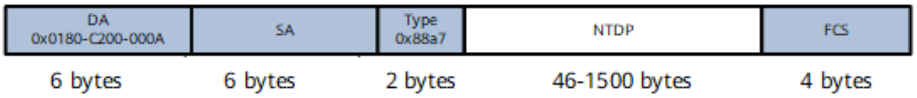
- 更新定时器：当此定时器超时，设备立即发送更新报文。
- 老化定时器：设备如果在老化时间内没有收到邻居发来的NDP报文，相应NDP表项将被自动删除。

NTDP

网络拓扑发现协议NTDP（Network Topology Discovery Protocol），是华为公司的私有协议，用来在一定网络范围内收集拓扑信息。NTDP收集的信息包括NDP表项信息等。

NTDP报文承载于Ethernet-II帧，以组播目的MAC地址周期性发送请求报文，以单播目的MAC地址发送响应报文。NTDP报文结构如图3-3所示。

图 3-3 NTDP 报文结构

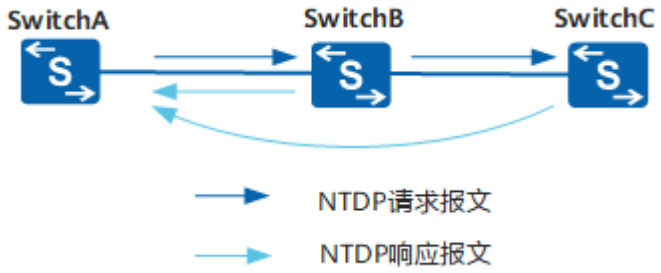


各字段含义如下：

- DA（Destination MAC Address）：目的MAC地址，为固定的组播MAC地址0x0180-C200-000A。
- SA（Source MAC Address）：源MAC地址，为固定的MAC地址0x00e0-fc09-bcf9。
- Type：报文类型，NTDP报文中该字段的值为0x88a7。
- NTDP：NTDP数据单元，NTDP信息交换的主体。
- FCS：帧检验序列。

如图3-4所示，拓扑收集设备SwitchA发送NTDP请求报文。SwitchB收到该请求报文立即发送响应报文，并转发此请求报文给与它相邻的设备SwitchC，SwitchC收到请求后将执行同样的操作，以此类推，网络中的每个设备都会收到此请求，都会向拓扑收集设备响应请求。因此，SwitchA可以收集到所有设备的NDP信息和设备之间的互连信息，可以依据这些信息构造出网络拓扑图。

图 3-4 NTDP 协议的网络拓扑信息收集流程



网络拓扑收集

网络拓扑收集功能是基于NDP和NTDP协议的，由Commander作为网络拓扑收集设备。通过网络拓扑收集功能实现零配置设备部署，无需用户手动收集设备MAC地址或ESN序列号等信息，零配置设备上电启动完成后，Commander可自动收集到这些信息并为设备分配Client ID，完成设备信息与设备的绑定，即收集到网络拓扑信息，并根据网络拓扑信息来配置下载文件信息。通过网络拓扑收集功能完成零配置设备部署后，还可以基于网络拓扑信息自动进行故障设备替换。

3.2.2 通过 Option 参数或中间文件实现零配置设备部署

通过Option参数或中间文件实现零配置设备部署时，零配置设备获取文件信息的方式分别是：

- Option方式：根据Option信息获取文件信息。
- 中间文件方式：从文件服务器获取中间文件并解析出文件信息。

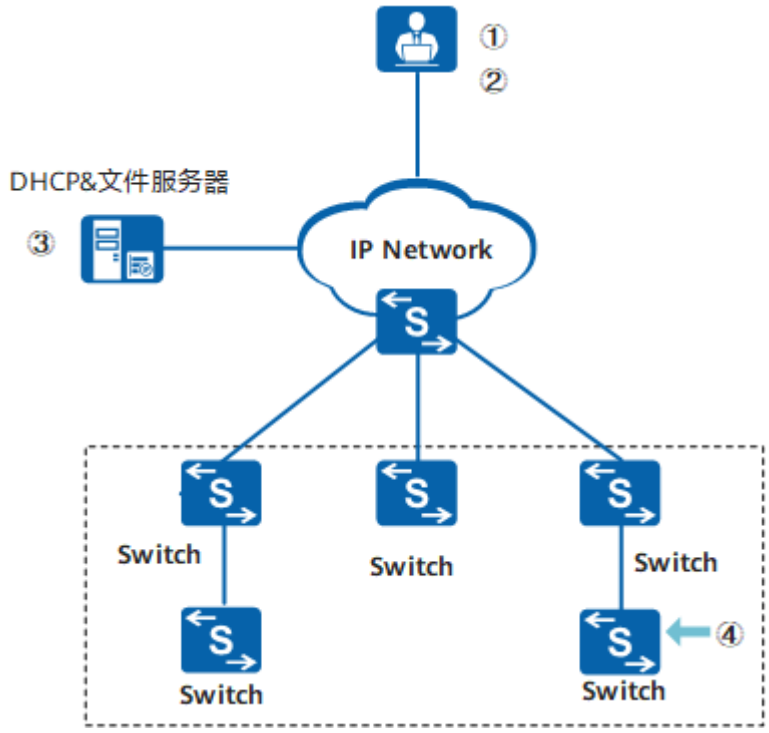
通过Option或中间文件方式只适用于零配置设备部署场景，且对网络设备没有后期维护的功能，建议配置通过Commander的方式来实现。

如图3-5所示，黑色框内的Switch为新加入的零配置设备。下面以其中一台Switch为例，说明通过Option参数或中间文件实现零配置设备部署的配置及实现流程。

说明

此种方式即为原Auto-Config的零配置设备部署的实现方式，没有Commander和Client两种角色。

图 3-5 零配置设备部署组网示意图

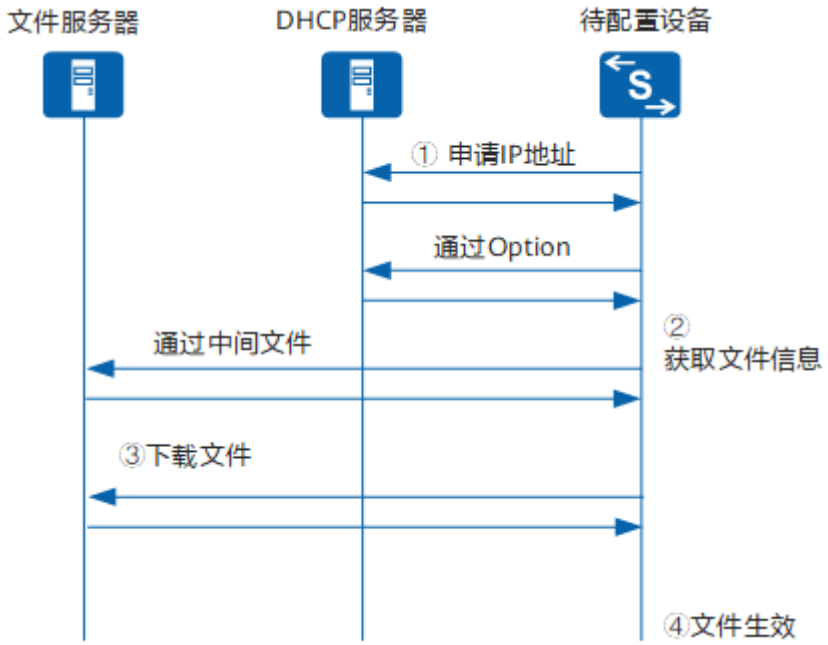


1. 网络管理员进行网络规划：包括待配置设备的物理位置、管理IP、管理VLAN以及其他网络和基本业务配置参数，生成待配置设备的离线配置文件。
2. 根据待配置设备的情况，选择待配置设备通过Option参数还是中间文件获取下载文件信息。
   - 如果待配置设备较少，且不同设备加载相同的配置文件，则可以采用Option参数。此时待配置设备需要下载的文件信息都需要通过指定DHCP服务器上的Option参数来配置。
   - 如果待配置设备较多，且不同设备加载不同的配置文件，则可以采用中间文件。此时待配置设备需要下载的文件信息都在中间文件上指定，中间文件需要离线创建完成。
3. 部署DHCP服务器（包括Option参数）及文件服务器。将生成的待配置设备的配置文件及其他需要加载的文件保存至文件服务器中。如果采用中间文件方式，则也需要将中间文件保存至文件服务器。

   如果待配置设备与DHCP服务器不在同一网段，还需要部署DHCP中继。
4. 配置完成以后，待配置设备启动零配置设备部署流程。

零配置部署流程启动后，内部实现流程如图3-6所示。

图 3-6 零配置部署内部实现流程



零配置部署内部实现流程分为以下4个阶段：

1. 申请IP地址阶段：待配置设备发送DHCP请求，DHCP服务器回应，并携带文件服务器的信息。
2. 获取文件信息阶段：待配置设备根据DHCP应答报文中的Option参数的值来判断，文件信息是从Option参数获取还是从中间文件获取。
3. 下载文件阶段：根据获取到的信息从文件服务器分别下载相应文件。

   待配置设备下载文件的顺序：系统文件->补丁文件->Web网页文件->配置文件。
4. 配置文件生效：用户可以在DHCP服务器上指定Option 146来配置配置文件的激活策略。

如果待配置设备为堆叠环境，下载的系统软件、补丁文件及Web网页文件会从主交换机拷贝到从交换机。文件同步完成后，开始激活文件，此后待配置设备进入正常运行状态。

通过 Option 或中间文件实现零配置部署中的 Option 参数

通过Option或中间文件实现零配置部署时，必须在DHCP服务器上指定相关的Option参数，如果参数为多个时，两个参数之间必须用“;”隔开。Option参数的详细介绍如**表3-1**所示。

⚠ 注意

- DHCP服务器不支持认证，存在被仿冒的风险，建议用户在安全组网环境中使用信任的DHCP服务器进行开局。
- DHCP协议是非加密传输，通过Option开局或升级时，
  - 如果待开局或升级设备是V200R020C10及之后版本，SFTP/FTP服务器的用户名密码通过Option66传输，安全性存在一定的风险，建议用户在安全组网环境中使用。
  - 如果待开局或升级设备是V200R020C10之前版本，SFTP/FTP服务器的用户名密码通过Option141、Option142传输，安全性存在一定的风险，建议用户在安全组网环境中使用。
- Option参数中，Option 66只用于V200R020C10及之后版本的设备，Option 141、Option 142、Option 143、Option 149只用于V200R020C10之前版本的设备。

  如果待配置设备中既有V200R020C10版本之前的设备，也有V200R020C10版本之后的设备，则待配置设备的配置文件中可以同时配置Option 66、Option 141、Option 142、Option 143、Option 149，V200R020C10之前版本的设备，通过Option 141、Option 142、Option 143、Option 149解析到正确的FTP信息，V200R020C10及之后版本的设备，通过Option 66解析到正确的FTP信息。

表 3-1 Option 参数说明表

Option编号	描述	说明
Option 66	表示为DHCP客户端分配的SFTP/FTP服务器URL地址，其中包含SFTP/FTP用户名、密码、IP地址（不支持域名）、端口号（SFTP默认端口号为22，FTP默认端口号为21）。 格式为：sftp://username:password@1.1.1.1:22或ftp://username:password@1.1.1.1:21 用户名、密码、IP地址、端口号请以实际为准。	Option方式实现零配置部署：必选。如果指定了此参数，表示以Option方式实现零配置部署。 中间文件方式实现零配置部署：无需配置
Option 67	表示为DHCP客户端分配的配置文件名称，支持指定文件路径，指定的路径和文件名不能超过69字符，不支持空格，如：easy/vrpcfg.cfg，easy为文件所在的路径。	
Option 141	表示为DHCP客户端分配的SFTP/FTP用户名。	Option方式和中间文件方式实现零配置部署，均是必选，至少配置一种文件服务器 • 配置Option 141、142和143，待配置设备可以获取FTP用户名、FTP密码、FTP服务器的IP地址。 • 配置Option 141、142和149，待配置设备可

Option编号	描述	说明
Option 142	表示为DHCP客户端分配的SFTP/FTP用户密码。可采用以下两种格式配置： ● **option 142 ascii** *password* ● **option 142 cipher** *password* 采用ascii格式时，密码明文存储；采用cipher格式时，密码密文存储。以不同方式多次执行该命令时，以最近一次的配置作为最终配置。为保证密码安全，建议采用cipher格式配置密码。	以获取SFTP用户名、SFTP密码、SFTP服务器的IP地址和端口号。 ● 配置Option 150，待配置设备可以获取TFTP服务器的IP地址。 当DHCP服务器配置了多种文件服务器的Option参数时，选用文件服务器顺序依次为SFTP->TFTP->FTP。 待配置设备获取的文件服务器账号仅用于EasyDeploy场景。待配置设备不会保存文件服务器的用户名和密码。
Option 143	表示为DHCP客户端分配的FTP服务器IP地址。	

Option 149	表示为DHCP客户端分配的SFTP服务器IP地址和端口号。例如，若SFTP服务器IP地址为10.10.10.1，采用默认端口号22，则Option149的格式用下面两种方式表示都可以：
	option 149 ascii ipaddr=10.10.10.1;
	option 149 ascii ipaddr=10.10.10.1;port=22;	

Option 150	表示为DHCP客户端分配的TFTP服务器IP地址。	

Option 145	表示为DHCP客户端分配的非配置文件信息，支持指定文件路径，指定的路径和文件名不能超过69字符。例如：系统软件信息、版本号信息、补丁文件信息、Web文件信息和模块文件信息。格式为：
	`vrpfile=VRPFILENAME;vrpver=VRPVERSION;patchfile=PATCHFILENAME;webfile=WEBFILE;modulefile=MODFILENAME;`
	例如：
	`vrpfile=easy_V200R022C00SPC100.cc;vrpver=V200R022C00SPC100;patchfile=easy_V200R022C00.pat;webfile=easy_V200R022C00.web.7z;modulefile=easy_V200R022C00.mod;`
		Option方式实现零配置部署：可选
		中间文件方式实现零配置部署：无需配置

Option编号	描述	说明
Option 146	表示用户指定动作的操作信息，包括存储空间不足时删除文件的策略和文件延迟生效时间，字段及含义为： ● opervalue=0：表示空间不足时，不删除文件系统中系统软件。opervalue=1：表示空间不足时，删除文件系统中系统软件。缺省情况下，opervalue=0。 ● delaytime：表示EasyDeploy下载文件成功后，文件延时生效时间，单位为秒。缺省情况下，delaytime=0。 ● netfile：表示设置的中间文件名称，文件名称最长为64字节，文件名支持字符0～9、a～z、A～Z、-、_，配置的文件名必须是“cfg”后缀。文件名非法时，默认文件为lswnet.cfg。 ● intime：表示文件生效的指定时间，指定的范围是“00:00～23:59”。 ● actmode：表示文件激活的方式。 actmode=0表示采用默认的方式激活文件。 – 如果下载的文件是配置文件和补丁文件，则不需要复位设备，文件即可自动激活。 – 如果下载的文件中包含版本文件，则需要复位设备来激活文件。 actmode=1表示下载的文件都必须采用复位设备的方式来激活。 缺省情况下，actmode=0。 **说明** ● 配置的延时重启生效时间最大为一天，即86400秒。如果配置的时间大于一天，则按一天计算。 ● 如果delaytime和intime同时配置了，则以delaytime的配置生效。	Option方式实现零配置部署：可选 中间文件方式实现零配置部署：必选。通过中间文件获取下载文件信息时，必须配置Option 146中“netfile”的值，指定中间文件名称，从而通过中间文件实现文件的自动加载。
Option 147	表示认证信息。可以不配置，如果配置，必须配置为AutoConfig，区分大小写。	Option方式实现零配置部署：可选 中间文件方式实现零配置部署：可选

在设备零配置部署场景下，不同开局方式优先级从高到低如下：

1. NETCONF Option148方式（*ascii-string*的格式为**agilemode**=**agile-cloud**;**agilemanage-mode**=**ip**;**agilemanage-domain**=*ip-address*;**agilemanage-port**=*port-number*;**agilemanage-backup-address**=*ip-address*:*port-number*;**sitecode**=*sitecode-value*;）

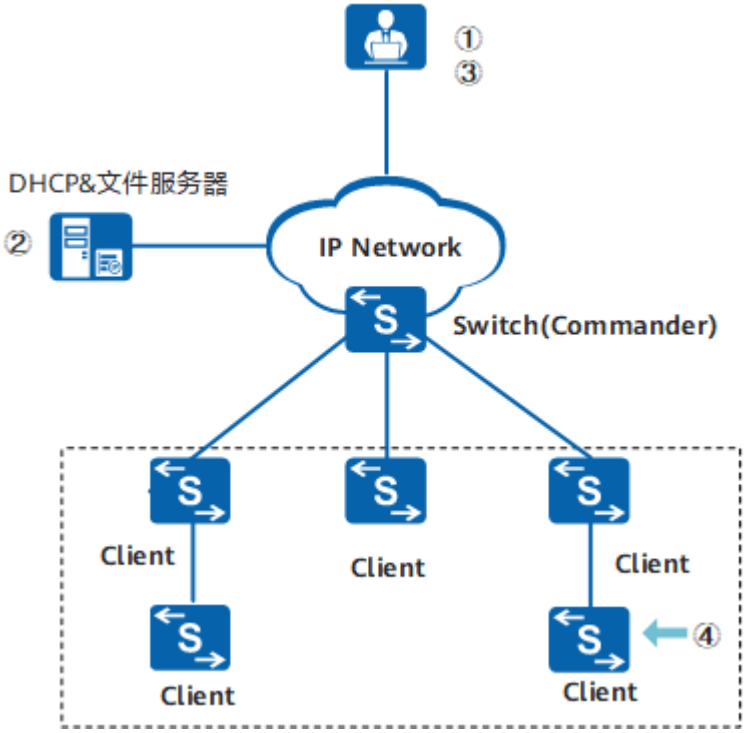
2. EasyDeploy Option148方式（*ascii-string*的格式为**ipaddr**=*ip-address*;**port**=*udp-port*;）
3. EasyDeploy Option66方式
4. 注册中心开局方式

3.2.3 通过 Commander 实现零配置设备部署

通过Commander实现零配置设备部署时，零配置设备获取文件信息的方式是从Commander上获取文件信息。

如图3-7所示，Client为新加入的零配置设备。下面以其中一台Client为例，说明通过Commander实现零配置设备部署的配置及实现流程。

图 3-7 零配置设备部署组网示意图



1. 网络管理员进行网络规划，包括选定一台正常工作的设备作为Commander；规划Client的物理位置、管理IP、管理VLAN以及网络业务配置参数等，生成各Client的离线配置文件。

   说明

   在配置文件中加入Commander的IP地址，便于对零配置部署完成之后的Client管理和维护。

2. 部署文件服务器和DHCP服务器（必须指定Option 148参数，其他无需指定），并将Client上需要加载的文件保存至文件服务器工作目录下。

   如果Client与DHCP服务器不在同一网段，还需要部署DHCP中继。

注意

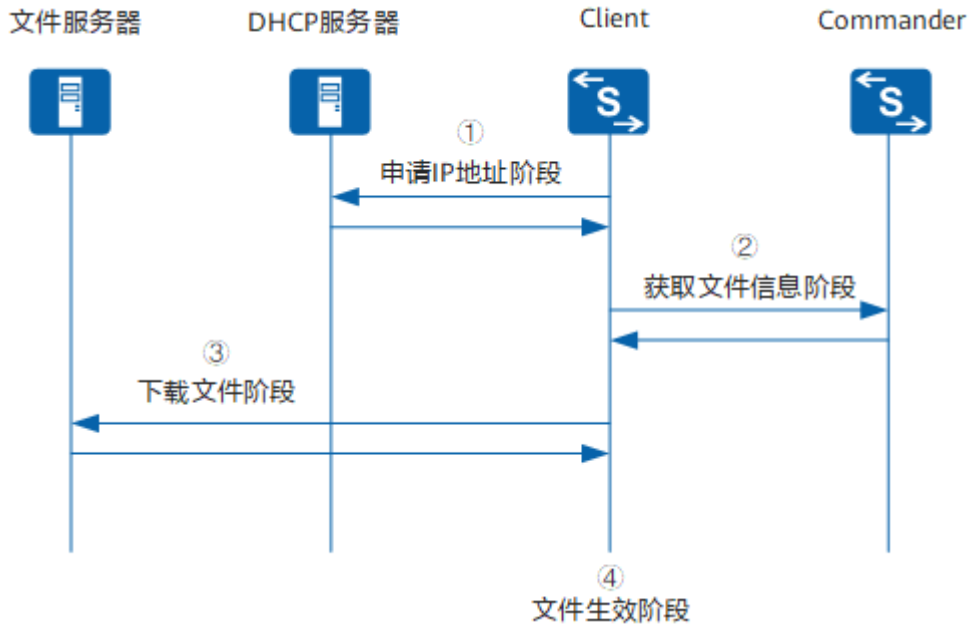
- DHCP服务器不支持认证，存在被仿冒的风险，建议用户在安全组网环境中使用信任的DHCP服务器进行开局。

3. 在选定作为Commander的设备上配置文件服务器地址及用户名和密码、根据设备安装工程师上报Client的MAC地址或ESN号，配置Client上需要下载的文件信息等。

   如果Commander支持网络拓扑收集功能，则可根据Commander收集到的拓扑信息，配置Client的下载文件信息，不需要设备安装工程师上报Client的MAC地址或ESN号。
4. 配置完成以后，Client启动零配置设备部署流程。

零配置设备部署流程启动后，内部实现流程如图3-8所示。

图 3-8 零配置设备部署内部实现流程



零配置设备部署内部实现流程分为以下4个阶段：

1. 申请IP地址阶段：Client发送DHCP请求，DHCP服务器响应请求，并携带Commander的地址信息。
2. 获取文件信息阶段：Client与Commander建立通信，并从Commander获取文件信息。
3. 下载文件阶段：根据获取到的信息从文件服务器下载相应文件。

   Client下载文件的顺序：

   a. 系统软件
   b. 补丁文件
   c. Web网页文件
   d. 配置文件

e. 用户自定义文件（零配置部署场景不支持下载License文件）

4. 文件生效阶段：下载文件完成后，根据文件激活策略激活文件。

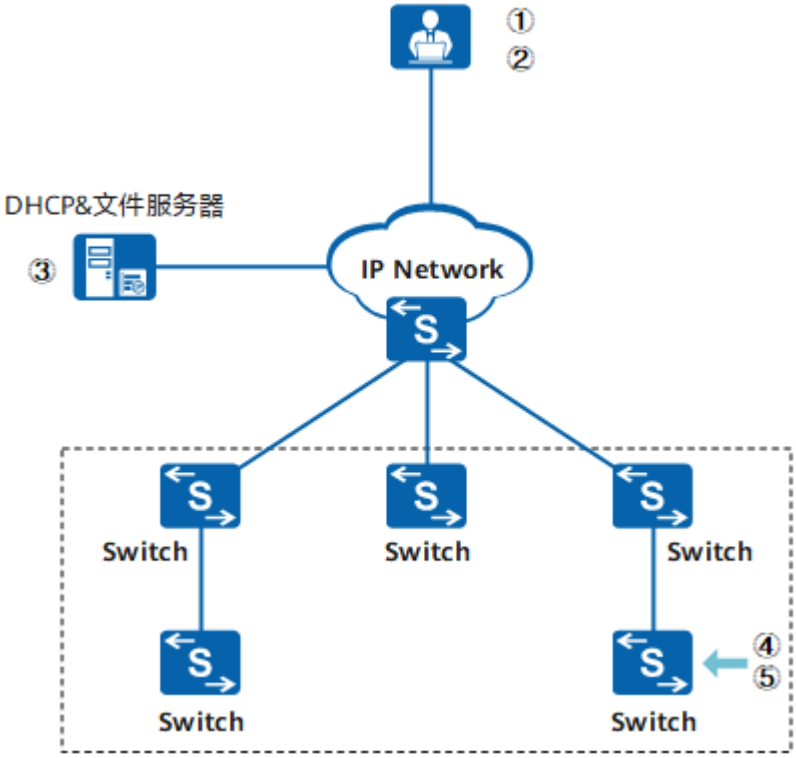
   如果Client为堆叠环境，在到达激活时间后，下载的文件会从主交换机拷贝到从交换机。文件同步完成后，开始激活文件，此后Client进入正常运行状态。

在零配置部署流程中，如果申请IP地址阶段设备无法获取到IP地址，则设备会停留在该阶段定时发送请求获取IP地址，直到获取成功或者人工干预。在成功获取到IP地址后，如果出现错误（例如文件服务器信息错误等），则会切换至初始化状态重新开始，出错后再次切换至初始化状态，并且一直循环，直到人工干预。其中在文件下载过程中，如果第一次下载失败，则间隔1分钟再次尝试下载，共计尝试5次，如果仍失败，则Client会在延迟5分钟之后切换为初始化状态，重新开始DHCP流程，获取下载文件信息和下载文件。

3.2.4 通过中间文件实现带配置部署

如图3-9所示，黑色框内的Switch为新加入的带配置设备。下面以其中一台Switch为例，说明通过中间文件实现带配置设备部署的配置及实现流程。

图 3-9 带配置设备部署组网示意图



1. 网络管理员进行网络规划：包括待配置设备的物理位置、管理IP、管理VLAN以及其他网络和基本业务配置参数，生成待配置设备的离线配置文件。
2. 通过中间文件获取SNMP主机的地址、下载文件信息，待配置设备需要下载的文件信息都在中间文件上指定，中间文件需要离线创建完成。
3. 部署DHCP服务器及文件服务器。将中间文件、生成的待配置设备的配置文件及其他需要加载的文件保存至文件服务器中。

   如果待配置设备与DHCP服务器不在同一网段，还需要部署DHCP中继。

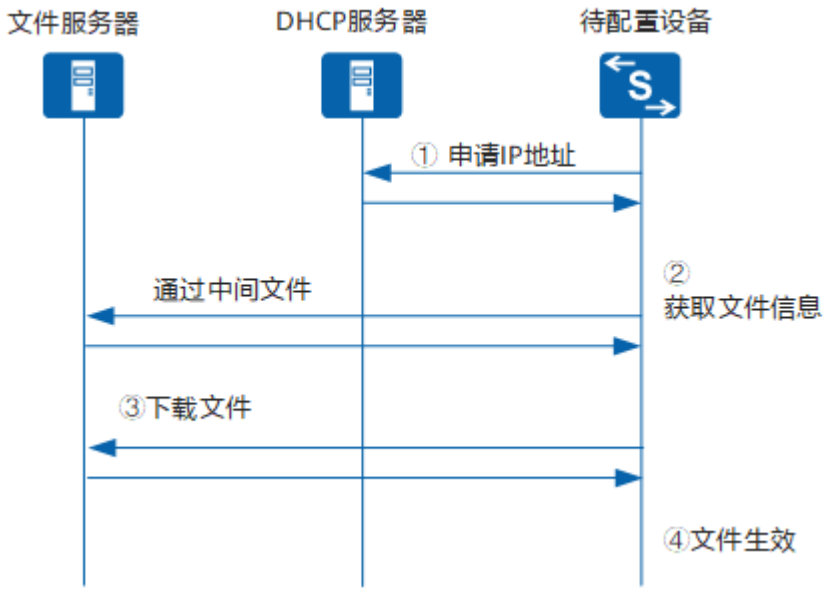
注意

- DHCP服务器不支持认证，存在被仿冒的风险，建议用户在安全组网环境中使用信任的DHCP服务器进行开局。

4. 设备出厂时已经自带相关配置。包括文件服务器地址、开局使用的中间文件名、设备与SNMP主机的共享密钥等。
5. 启动带配置部署流程。

带配置部署流程启动后，内部实现流程如图3-10所示。

图 3-10 带配置部署内部实现流程



带配置部署内部实现流程分为以下4个阶段：

1. 申请IP地址阶段：待配置设备发送DHCP请求，DHCP服务器回应。
2. 获取文件信息阶段：设备上已经通过命令指定了设备需要获取的中间文件。
3. 下载文件阶段：根据中间文件中的信息从文件服务器分别下载相应文件。

   待配置设备下载文件的顺序：

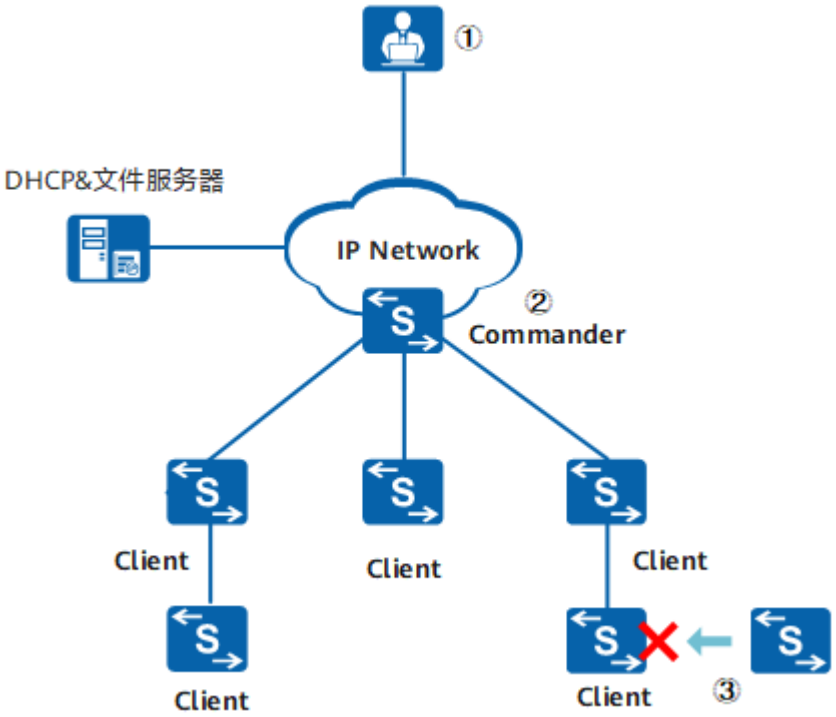
   a. 系统文件
   b. 补丁文件
   c. Web网页文件
   d. 配置文件
4. 配置文件生效：复位设备来激活文件。

如果待配置设备为堆叠环境，下载的系统软件、补丁文件及Web网页文件会从主交换机拷贝到从交换机。文件同步完成后，开始激活文件，此后待配置设备进入正常运行状态。

3.2.5 故障设备替换

如图3-11所示，在运行EasyDeploy功能的网络中，以其中一台Client因硬件故障无法正常启动为例，说明故障设备替换的配置及实现的流程。

图 3-11 故障设备替换组网示意图



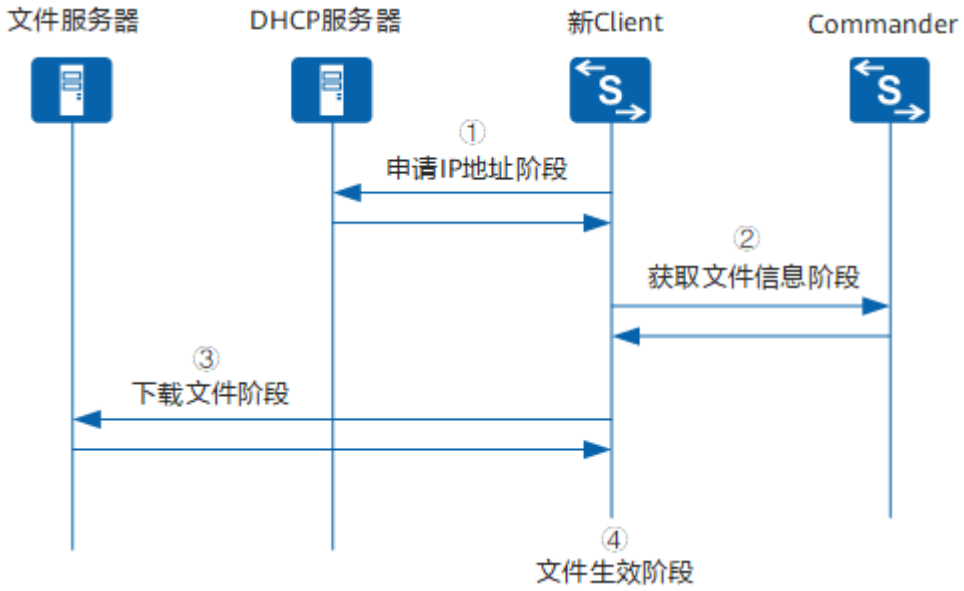
1. 网络管理员发现有Client出现故障。设备安装工程师使用新的设备替换故障的设备，并且将新设备的MAC地址或ESN序列号上报给网络管理员。
2. 根据新Client的MAC地址或ESN序列号，在Commander上配置新Client与故障Client的对应关系。

   如果整网使能了拓扑收集功能，在只需要恢复配置文件的情况下，则不需要任何配置，通过拓扑匹配就可以发现新Client与故障Client的对应关系。

   如果新Client还需要加载除配置文件以外的文件，则需要将这些文件保存至文件服务器，并且在Commander上指定新Client下载的文件名称。
3. 配置完成后，新Client将会自动启动故障设备替换流程，将备份在文件服务器上故障Client的配置文件下载到新Client上，恢复原来的配置。

故障设备替换流程启动后，内部实现流程如图3-12所示。

图 3-12 故障设备替换内部实现流程



故障设备替换内部实现流程分为以下4个阶段：

1. 申请IP地址阶段：新Client发送DHCP请求，DHCP服务器回应，并携带Commander的地址信息。
2. 获取文件信息阶段：新Client与Commander建立通信，根据新Client与故障Client的替换信息从Commander获取非配置文件的信息以及备份配置文件的记录。
3. 下载文件阶段：根据获取到的信息先从文件服务器下载非配置文件，下载成功后再下载备份的配置文件。

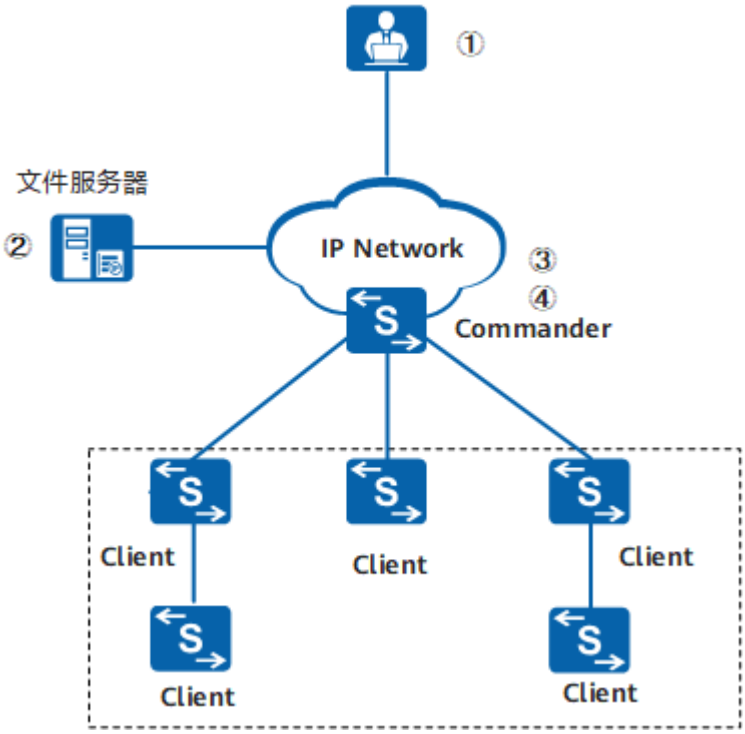
   Client下载文件的顺序：系统软件->补丁文件->Web网页文件->用户自定义文件->备份的配置文件（故障替换场景不支持下载License文件）。
4. 文件生效阶段：下载文件完成后，根据文件激活策略激活文件，新Client进入正常运行状态。

故障替换流程中，如果申请IP地址阶段设备无法获取到IP地址，则设备会停留在该阶段定时发送请求获取IP地址，直到获取成功或者人工干预。在成功获取到IP地址后，如果出现错误（例如文件服务器信息错误等），则会切换至初始化状态重新开始，出错后再次切换至初始化状态，并且一直循环，直到人工干预。其中在文件下载过程中，如果第一次下载失败后，间隔1分钟再次尝试下载，共计尝试5次，如果仍失败，则Client会在延迟5分钟之后切换为初始化状态，重新开始DHCP流程，获取下载文件信息和下载文件。

3.2.6 批量升级

如图3-13所示，在运行EasyDeploy功能的网络中，Client为待升级设备。以待升级的Client为例，说明批量升级的配置及实现的流程。

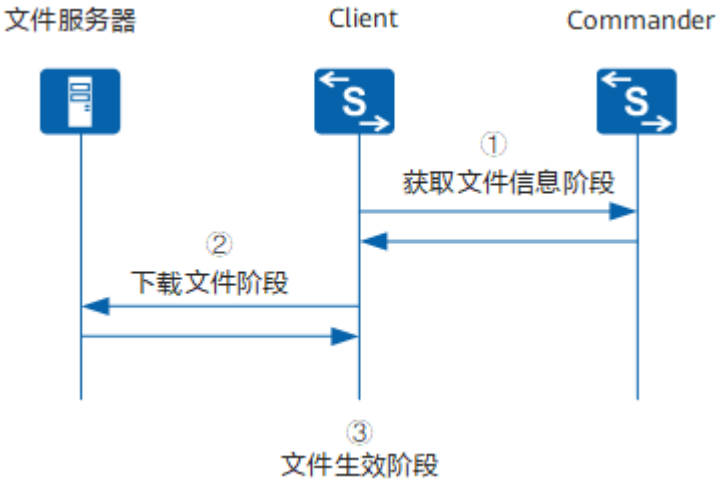
图 3-13 批量升级组网示意图



1. 网络工程师进行升级规划，确定升级的设备、升级的文件及升级策略。
2. 将Client需要升级的文件保存至文件服务器中。
3. 在Commander上进行升级相关的配置，包括文件服务器地址及用户名和密码、Client上需要下载的文件信息等。
4. Commander按照升级策略的要求，向Client下发升级指令，Client启动升级流程。

批量升级流程启动后，内部实现流程如图3-14所示。

图 3-14 批量升级内部实现流程



批量升级内部实现流程分为以下3个阶段：

1. 获取文件信息阶段：Client与Commander建立通信，Client从Commander获取文件信息。
2. 下载文件阶段：根据获取到的信息从文件服务器下载相应文件。

   Client下载文件的顺序：

   a. 系统软件
   b. 补丁文件
   c. License文件
   d. Web网页文件
   e. 配置文件
   f. 用户自定义文件
3. 文件生效阶段：下载文件完成后，根据文件激活策略激活文件。

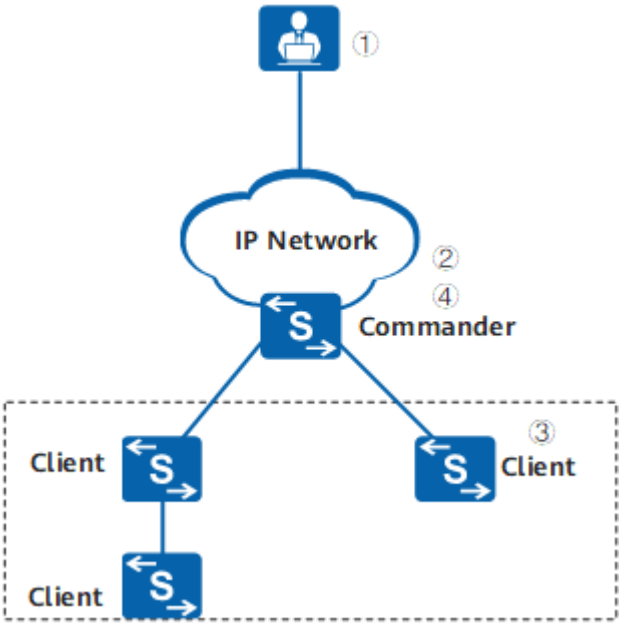
   如果Client为堆叠环境，在到达激活时间后，下载的文件会从主交换机拷贝到从交换机。文件同步完成后，开始激活文件，此后Client进入正常运行状态。

在批量升级流程中，如果出现错误（例如文件服务器信息错误、指定文件不存在等），Client会退出批量升级流程，切换至原来的正常运行状态，已经下载的文件不会自动清除。其中，在文件下载过程中，如果第一次下载失败后，间隔1分钟再次尝试下载，共计尝试5次，如果仍失败，则Client退出批量升级流程。

3.2.7 批量配置

如图3-15所示，在运行EasyDeploy功能的网络中，以所有的Client需要配置相同的命令行为例，说明批量配置的实现流程。

图 3-15 批量配置组网示意图

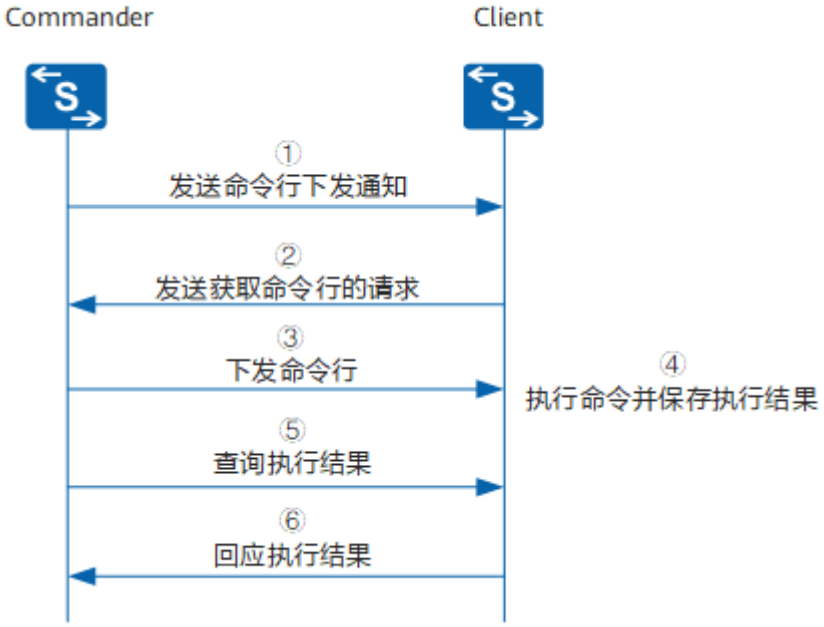


1. 网络管理员离线制作命令行脚本并上传到Commander上或者在Commander上在线编辑命令行脚本。
2. 在Commander上指定需要下发命令的Client或者Group，下发命令行。
3. Client接收到Commander下发的命令后，执行并保存执行结果。

4. 在Commander上查询各个Client执行命令的结果。

命令行下发启动后，内部实现流程如图3-16所示。

图 3-16 批量配置内部实现流程



1. Commander向Client发送命令行下发通知。
2. Client收到通知后，向Commander发送请求获取命令行。
3. Commander收到请求后，将命令行下发给Client。
4. Client执行命令，并保存执行的结果。
5. Commander向Client发送查询执行结果请求。
6. Client回应请求，将保存的执行结果回应给Commander。

3.3 EasyDeploy 配置注意事项

涉及网元

EasyDeploy组网需要以下角色配合：

- DHCP服务器
- 文件服务器
- Commander和Client

License 支持

本特性是交换机的基本特性，无需获得License许可即可应用此功能。

V200R022C00 版本特性支持情况

除S5731-L和S5731S-L外，S2700, S5700, S6700系列交换机中所有款型均支持EasyDeploy。

说明

如需了解交换机软件配套详细信息，请点击**硬件中心**，并选择产品型号进行查询。

S5731-L和S5731S-L属于远端模块，不支持Web管理、YANG和命令行，仅支持通过中心交换机对其下发配置，相关操作请参见《S300, S500, S2700, S5700, S6700 V200R022C00 配置指南-设备管理》中的“智能极简园区网络配置（小行星方案）”。

特性依赖和限制

- EasyDeploy功能不支持IPv6场景和VPN网络场景。
- EasyDeploy功能与SVF、U盘开局、WEB初始化模式功能互斥。
- 在零配置设备部署和故障设备替换场景中，如果通过Console口登录到待配置设备，则此设备会停止EasyDeploy流程，切换至正常运行状态。
- 设备上的Ethernet0/0/0和MEth0/0/1管理口不支持EasyDeploy功能，只有加入缺省VLAN的业务口才支持，使用业务口开局存在三面隔离风险，建议用户在安全组网环境中使用。
- 在零配置设备部署场景中，用户可以根据需要选择是否指定配置文件。如果没有指定配置文件但是指定了升级的系统软件，则需要同时指定升级的版本号。
- 在零配置设备部署场景中，如果用户指定配置文件，配置文件第一行需要指定版本号。
- EasyDeploy配置文件中必须配置Console接口的登录密码，否则会导致设备部署失败，失败原因可查看“EZOP/3/UPGRADE_FAIL”日志信息。
- EasyDeploy配置文件中vty用户登录界面验证方式请勿设置为**authentication-mode none**，否则会导致EasyDeploy配置失败。
- 通过Option或中间文件方式只适用于零配置设备部署场景，且对网络设备没有后期维护的功能，建议配置通过Commander的方式来实现。
- Commander在网络中的位置没有特殊的限定，但需要保证Commander与获取IP地址后的Client路由可达。
- EasyDeploy支持堆叠系统做Client，此时，Client的MAC地址为堆叠系统MAC，Client的ESN为堆叠主设备的ESN。
- 堆叠系统是先做堆叠再去EasyDeploy，由于组件堆叠的配置并不是在配置文件里，所以还是会被认为是空配置。
- 当使能EasyDeploy拓扑收集功能时，如果NTDP需要拓扑收集的设备节点规模数较大（一般大于200），发起拓扑收集的Commander设备会收到大量的协议报文。为防止报文规模超过NTDP默认CAR值导致报文被丢弃影响拓扑收集，用户可执行car（防攻击策略视图）命令，适当放大针对NTDP报文的CPCAR值。
- **DTLS加密**
  - 在有配置的设备上，EasyDeploy支持DTLS加密，DTLS加密默认开启。零配置设备部署场景，不受DTLS加密的限制，可以正常部署。
  - 在DTLS加密开启的情况下，如果Commander或者Client发生了主备倒换，Client需要重新上线。如果DTLS加密没有开启，主备倒换对Client的在线管理不会有影响。
  - 对于V200R010C00之前版本的Client，如果需要加入V200R010C00及之后版本的Commander进行管理，若Commander使能了DTLS加密功能，则必须升级Client到V200R010C00及之后版本。否则Client无法加入到现有的网络。
  - 对于V200R010C00及之后版本的Client，如果需要加入V200R010C00之前版本的Commander进行管理，需要在Client上配置**easy-operation dtls disable**命令关闭DTLS加密功能。

- **规格**

  EasyDeploy的规格如表3-2所示。

  表 3-2 EasyDeploy 的规格

实现方案	角色	支持的形态	支持的版本	支持管理Client的数量	说明
通过配置Commander方式实现EasyDeploy	Commander	S12700	V200R005C00版本及以后版本	255	• 如果Client是框式交换机，则只支持批量升级、批量配置场景，不支持零配置部署和故障替换场景。 • 如果Client是盒式交换机，则批量升级、批量配置，零配置部署和故障替换四种场景全部支持。
		S12700E	V200R019C00版本及以后版本	255	
		S7700	V200R003C00版本及以后版本	255	
		S7900	V200R011C10版本至V200R013C00版本	255	
		S9700	V200R003C00版本至V200R013C00版本	255	
		S5700-HI	V200R003C00版本至V200R005C00版本	128	
		S5710-HI	V200R003C00版本至V200R005C00版本	128	
		S6700-EI	V200R003C00版本至V200R005C00版本	64	
		S5700-EI	V200R003C00版本至V200R005C00版本	64	
		S5710-EI	V200R003C00版本至V200R005C00版本	64	

实现方案	角色	支持的形态	支持的版本	支持管理Client的数量	说明
		S5720-HI	V200R006C00版本至V200R019C10版本	128	
		S5720-EI	V200R007C00版本至V200R019C10版本	128	
		S5730-HI	V200R012C00版本至V200R019C10版本	128	
		S5731-H	V200R013C02版本及以后版本	128	
		S5731-H-K	V200R019C10版本及以后版本	128	
		S5731-S	V200R019C00版本及以后版本	128	
		S5731S-S	V200R019C00版本及以后版本	128	
		S5731S-H	V200R019C00版本及以后版本	128	
		S5732-H	V200R019C00版本及以后版本	128	
		S5732-H-K	V200R019C10版本及以后版本	128	
		S6720-EI	V200R008C00版本及以后版本	128	
		S6720S-EI	V200R009C00版本及以后版本	128	
		S6720-HI	V200R012C00版本至V200R019C10版本	128	
		S6730-H	V200R013C02版本及以后版本	128	
		S6730-H-K	V200R019C10版本及以后版本	128	

实现方案	角色	支持的形态	支持的版本	支持管理Client的数量	说明
		S6730S-H	V200R019C10版本及以后版本	128	
		S6730-S	V200R019C00版本及以后版本	128	
		S6730S-S	V200R019C00版本及以后版本	128	
		S6735-S	V200R021C00SPC600版本及以后版本	128	
	Client	• 盒式交换机全形态支持（S5731-L和S5731S-L除外） • 框式交换机全形态支持	V200R003C00版本及以后版本	-	
通过Option或中间文件方式实现EasyDeploy	待配置的设备可以是所有的盒式交换机（S5731-L和S5731S-L除外）				

- EasyDeploy支持的文件类型如表3-3所示。

表 3-3 EasyDeploy 支持的文件类型

使用场景	文件类型
零配置部署	系统软件、补丁文件、Web网页文件、配置文件和用户自定义文件
故障替换	系统软件、补丁文件、Web网页文件、配置文件（自动备份）和用户自定义文件
批量升级	系统软件、补丁文件、Web网页文件、配置文件、License文件（Client是框式交换机时支持）和用户自定义文件
批量配置	命令行脚本

交换机支持最多3个自定义文件（例如批处理文件、登录标题文件等）的下载，其中通过Option或中间文件方式实现零配置部署不支持加载用户自定义文件。

3.4 EasyDeploy 缺省配置

表 3-4 EasyDeploy 的缺省配置

参数	缺省值
设备Commander功能	未使能
设备Client功能	设备默认情况下为Client角色

3.5 通过 Option 参数实现零配置设备部署

前置任务

通过Option参数实现EasyDeploy功能之前，需完成以下任务：

- 文件服务器、DHCP服务器与待配置设备（获取IP地址后）之间路由可达。
- 设备安装工程师上报待配置设备的MAC地址或ESN序列号。获取方法：设备表面贴的标签上可以查看设备的系统MAC地址和ESN序列号。

配置流程

请按照以下配置顺序完成配置。

3.5.1 配置文件服务器

背景信息

文件服务器用于存放待配置设备需要下载的版本文件，可以将网络中其他交换机或者服务器配置为文件服务器。EasyDeploy支持的文件服务器类型有FTP、TFTP和SFTP，建议使用SFTP服务器。

说明

此处给出的是交换机作为SFTP服务器的配置。如果使用的是第三方服务器，配置的具体方法请参见第三方服务器的操作指导。

操作步骤

步骤1 使能SFTP功能。具体操作步骤请参见“**8.3.3 通过SFTP进行文件操作**”中的“**配置SFTP服务器功能及参数**”。

步骤2 配置SSH用户的用户登录界面、用户名、认证方式、服务方式、SFTP服务授权目录等。具体操作步骤请参见“**8.3.3 通过SFTP进行文件操作**”中的“**配置SSH用户登录的用户界面**”和“**配置SSH用户**”。

----结束

后续处理

配置完文件服务器后，将待配置设备需要下载的文件上传至文件服务器的工作目录下。

说明

- 上传文件时，要保证存放目录下有足够的存储空间。
- 如果待配置设备数量较多，可以将文件服务器的并发访问数设置大一些，否则部分待配置设备会由于等待连接文件服务器而将整个部署时间延长。
- 为充分保证文件服务器的安全，建议配置的文件服务器用户名唯一。EasyDeploy过程结束后，请关闭相应的文件服务器功能。

3.5.2 配置 DHCP

背景信息

在配置通过Option实现EasyDeploy功能之前，必须先部署DHCP服务器，保证待配置设备能通过Option参数的配置获取到文件服务器信息和下载文件信息。

如果待配置设备与DHCP服务器在同一网段，则配置DHCP服务器即可。如果待配置设备与DHCP服务器在不同网段，除了需要配置DHCP服务器外，还需要配置DHCP中继。

下面操作步骤以交换机为例配置DHCP服务器。如果使用的是第三方设备，配置的具体方法请参见第三方设备的操作指导。

DHCP服务器必须支持配置相关的Option参数。此处给出DHCP服务器的基本配置，如果需要灵活部署DHCP功能，请参见《S300, S500, S2700, S5700, S6700 V200R022C00 配置指南-IP业务》DHCP配置。

注意

- DHCP服务器不支持认证，存在被仿冒的风险，建议用户在安全组网环境中使用信任的DHCP服务器进行开局。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**dhcp enable**，使能DHCP服务。

步骤3 执行命令**interface** *interface-type interface-number*，进入接口视图。

步骤4 （可选）对于以太网接口，执行命令**undo portswitch**，配置接口切换到三层模式。

缺省情况下，以太网接口处于二层模式。

说明

仅S5731-H、S5731-S、S5731S-H、S5731-H-K、S5731S-S、S5732-H、S5732-H-K、S6720-EI、S6735-S、S6720S-EI、S6730-H、S6730S-H、S6730-H-K、S6730-S和S6730S-S支持二层模式与三层模式切换。

步骤5 执行命令**dhcp select global**，配置接口工作在全局地址池模式。

步骤6 执行命令**quit**，返回到系统视图。

步骤7 执行命令**ip pool** *ip-pool-name*，创建全局地址池并进入全局地址池视图。

步骤8 执行命令**network** *ip-address* [**mask** { *mask* | *mask-length* }]，配置全局地址池可动态分配的IP地址范围。

- 配置的IP地址范围应该避免使用待配置设备需要加载的配置文件里面已经配置的IP地址，以防止地址冲突。
- 保证DHCP服务器上有可用的IP地址提供给待配置设备。

步骤9 执行命令**gateway-list** *ip-address* &<1-8>，配置DHCP客户端的出口网关地址。

步骤10 执行命令**option** *code* { **ascii** *ascii-string* | **hex** *hex-string* | **cipher** *cipher-string* | **ip-address** *ip-address* &<1-8> }，配置DHCP服务器的Option参数选项。

- 如果通过Option获取下载文件信息，则需要先配置**Option 67**参数。
- 至少配置一种文件服务器。指定文件服务器信息的Option参数请参见“**3.2.2 通过Option参数或中间文件实现零配置设备部署**”中的“**表3-1**”，其他可配的Option参数也请参考此处。

⚠ 注意

- DHCP协议是非加密传输，通过Option开局或升级时，
  - 如果待开局或升级设备是V200R020C10及之后版本，SFTP/FTP服务器的用户名密码通过Option66传输，安全性存在一定的风险，建议用户在安全组网环境中使用。
  - 如果待开局或升级设备是V200R020C10之前版本，SFTP/FTP服务器的用户名密码通过Option141、Option142传输，安全性存在一定的风险，建议用户在安全组网环境中使用。
- Option参数中，Option 66只用于V200R020C10及之后版本的设备，Option 141、Option 142、Option 143、Option 149只用于V200R020C10之前版本的设备。

  如果待配置设备中既有V200R020C10版本之前的设备，也有V200R020C10版本之后的设备，则待配置设备的配置文件中可以同时配置Option 66、Option 141、Option 142、Option 143、Option 149，V200R020C10之前版本的设备，通过Option 141、Option 142、Option 143、Option 149解析到正确的FTP信息，V200R020C10及之后版本的设备，通过Option 66解析到正确的FTP信息。

----结束

在使用EasyDeploy进行零配置开局时，如果Commander与Client通信时，不使用默认的VLAN1，此时Commander需要执行以下步骤把修改后的VLAN ID通知给Client设备。

1. 执行命令**pnp startup-vlan** *vlan-id*，配置有线PnP VLAN ID。

   缺省情况下，交换机未配置有线PnP VLAN ID。

2. 执行命令**pnp startup-vlan send enable**，使能向下游设备发送的LLDP报文中携带PnP VLAN信息的功能。

   缺省情况下，换机未使能向下游设备传递PnP VLAN的功能。
3. 执行命令**interface** *interface-type interface-number*，进入以太接口视图。
4. 执行命令**lldp tlv-enable legacy-tlv pnp startup-vlan**，使能向下游设备发送的LLDP报文中携带PnP VLAN信息的功能。

   缺省情况下，交换机已使能向下游设备发送的LLDP报文中携带PnP VLAN信息的功能。
5. 执行命令**quit**，退出以太网接口视图。
6. （可选）当交换机之间是通过Eth-Trunk接口相连时，还需要执行如下步骤：

   a. 执行命令**interface eth-trunk** *trunk-id*，进入Eth-Trunk接口视图。

   b. 执行命令**pnp startup-link-aggregation enable**，使能向下游设备传递需要建立Eth-Trunk链路的功能。

      缺省情况下，交换机未使能向下游设备传递需要建立Eth-Trunk链路的功能。

3.6 通过中间文件实现零配置设备部署

前置任务

通过中间文件实现EasyDeploy功能之前，需完成以下任务：

- 文件服务器、DHCP服务器与待配置设备（获取IP地址后）之间路由可达。
- 设备安装工程师上报待配置设备的MAC地址或ESN序列号。获取方法：设备表面贴的标签上可以查看设备的系统MAC地址和ESN序列号。

配置流程

请按照以下配置顺序完成配置。

3.6.1 配置文件服务器

背景信息

文件服务器用于存放待配置设备需要下载的版本文件，可以将网络中其他交换机或者服务器配置为文件服务器。EasyDeploy支持的文件服务器类型有FTP、TFTP和SFTP，建议使用SFTP服务器。

说明

此处给出的是交换机作为SFTP服务器的配置。如果使用的是第三方服务器，配置的具体方法请参见第三方服务器的操作指导。

操作步骤

步骤1 使能SFTP功能。具体操作步骤请参见“**8.3.3 通过SFTP进行文件操作**”中的“**配置SFTP服务器功能及参数**”。

步骤2 配置SSH用户的用户登录界面、用户名、认证方式、服务方式、SFTP服务授权目录等。具体操作步骤请参见“**8.3.3 通过SFTP进行文件操作**”中的“**配置SSH用户登录的用户界面**”和“**配置SSH用户**”。

----结束

后续处理

配置完文件服务器后，将待配置设备需要下载的文件上传至文件服务器的工作目录下。

说明

- 上传文件时，要保证存放目录下有足够的存储空间。
- 如果待配置设备数量较多，可以将文件服务器的并发访问数设置大一些，否则部分待配置设备会由于等待连接文件服务器而将整个部署时间延长。
- 为充分保证文件服务器的安全，建议配置的文件服务器用户名唯一。EasyDeploy过程结束后，请关闭相应的文件服务器功能。

3.6.2 编辑中间文件

背景信息

如果配置DHCP服务器时既没有配置Option 148参数，也没有配置Option 67参数（配置文件信息），EasyDeploy功能需要通过中间文件来实现文件的自动加载。

中间文件存放在文件服务器上，文件内容为下载文件信息，格式为设备MAC地址、ESN序列号或设备型号Model与待下载文件的对应关系。当设备获得文件服务器的IP地址后，就从文件服务器上下载中间文件进行解析，查询到与本设备MAC地址、ESN序列号或设备型号Model匹配的系统软件名称，系统软件的版本号，补丁文件名称，Web网页文件名称和配置文件名称，然后根据名称从文件服务器下载文件。

操作步骤

根据设备的MAC地址、ESN序列号或设备型号Model与所需的系统软件、补丁文件、Web网页文件和配置文件名称，编辑中间文件，具体步骤如下：

1. 新建一个文件名为lswnet.cfg的文本文档。
2. 编辑中间文件。

   假设一台待配置设备的MAC地址为xxxx-xxxx-xxxx，设备序列号ESN为93000701xxxxxxxx，设备型号Model为S5731-H24T4XC，对应这台设备应下载的版本文件名为auto_V200R022C00SPC200.cc，版本号信息为V200R022C00SPC200，补丁文件为auto_V200R022C00.pat，配置文件为auto_V200R022C00.cfg，Web网页文件为auto_V200R022C00.web.7z。则中间文件lswnet.cfg内容如下（中间文件中各配置项名称必须为小写）：

   ```
   mac=xxxx-xxxx-xxxx;vrpfile=auto_V200R022C00SPC200.cc;vrpver=V200R022C00SPC200;patchfile=auto_V200R022C00.pat;cfgfile=auto_V200R022C00.cfg;webfile=auto_V200R022C00.web.7z;
   ```

说明

- 当有多台设备需要配置时，中间文件的每行对应一台设备的配置信息。中间文件的大小不能超过1M。
- 中间文件的配置项中，MAC地址、设备序列号ESN和设备型号Model必选其一，三者的优先级从高到低分别为MAC地址、设备序列号ESN、设备型号Model；配置文件为必选项，系统软件、Web网页文件和补丁文件为可选项，三者间没有顺序限制。
- 如果中间文件中包含版本号信息，则必须要包含系统软件名称，并且要求系统软件的版本号与中间文件中的版本号信息一致。
- 中间文件中可以指定系统软件、补丁文件、Web文件和配置文件的路径，如：

  ```
  mac=xxxx-xxxx- xxxx;vrpfile=auto/
  auto_V200R022C00SPC200.cc;vrpver=V200R022C00SPC200;patchfile=auto/
  auto_V200R022C00.pat;cfgfile=auto/auto_V200R022C00.cfg;webfile=auto/
  auto_V200R022C00.web.7z;
  ```

  其中auto为指定文件所在文件服务器的文件夹。
- 中间文件中指定的系统软件、补丁文件、Web网页文件和配置文件路径不能超过48字符。

3.6.3 配置 DHCP

背景信息

在配置通过中间文件实现EasyDeploy功能之前，必须先部署DHCP服务器，保证待配置设备能通过DHCP服务器获取到IP地址、文件服务器信息和中间文件名称。

如果待配置设备与DHCP服务器在同一网段，则配置DHCP服务器即可。如果待配置设备与DHCP服务器在不同网段，除了需要配置DHCP服务器外，还需要配置DHCP中继。

下面操作步骤中以交换机为例配置DHCP服务器。如果使用的是第三方设备，配置的具体方法请参见第三方设备的操作指导。

DHCP服务器必须支持配置相关的Option参数。此处给出DHCP服务器的基本配置，如果需要灵活部署DHCP功能，请参见《S300, S500, S2700, S5700, S6700 V200R022C00 配置指南-IP业务》DHCP配置。

注意

- DHCP服务器不支持认证，存在被仿冒的风险，建议用户在安全组网环境中使用信任的DHCP服务器进行开局。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**dhcp enable**，使能DHCP服务。

步骤3 执行命令**interface** *interface-type interface-number*，进入接口视图。

步骤4 （可选）对于以太网接口，执行命令**undo portswitch**，配置接口切换到三层模式。

缺省情况下，以太网接口处于二层模式。

说明

仅S5731-H、S5731-S、S5731S-H、S5731-H-K、S5731S-S、S5732-H、S5732-H-K、S6720-EI、S6735-S、S6720S-EI、S6730-H、S6730S-H、S6730-H-K、S6730-S和S6730S-S支持二层模式与三层模式切换。

步骤5 执行命令**dhcp select global**，配置接口工作在全局地址池模式。

步骤6 执行命令**quit**，返回到系统视图。

步骤7 执行命令**ip pool** *ip-pool-name*，创建全局地址池并进入全局地址池视图。

步骤8 执行命令**network** *ip-address* [**mask** { *mask* | *mask-length* }]，配置全局地址池可动态分配的IP地址范围。

- 配置的IP地址范围应该避免使用待配置设备需要加载的配置文件里面已经配置的IP地址，以防止地址冲突。
- 保证DHCP服务器上有可用的IP地址提供给待配置设备。

步骤9 执行命令**gateway-list** *ip-address* &<1-8>，配置DHCP客户端的出口网关地址。

步骤10 执行命令**option** *code* { **ascii** *ascii-string* | **hex** *hex-string* | **cipher** *cipher-string* | **ip-address** *ip-address* &<1-8> }，配置DHCP服务器的Option参数选项。

- 如果通过中间文件获取下载文件信息，则不能配置**Option 67**参数，但需要配置**Option 146**中“netfile”的值，指定中间文件名称，从而通过中间文件实现文件的自动加载。
- 至少配置一种文件服务器。指定文件服务器信息的Option参数请参见“**3.2.2 通过Option参数或中间文件实现零配置设备部署**”中的“**表3-1**”，其他可配的Option参数也请参考此处。

----结束

在使用EasyDeploy进行零配置开局时，如果Commander与Client通信时，不使用默认的VLAN1，此时Commander需要执行以下步骤把修改后的VLAN ID通知给Client设备。

1. 执行命令**pnp startup-vlan** *vlan-id*，配置有线PnP VLAN ID。
   缺省情况下，交换机未配置有线PnP VLAN ID。
2. 执行命令**pnp startup-vlan send enable**，使能向下游设备发送的LLDP报文中携带PnP VLAN信息的功能。
   缺省情况下，换机未使能向下游设备传递PnP VLAN的功能。
3. 执行命令**interface** *interface-type interface-number*，进入以太接口视图。
4. 执行命令**lldp tlv-enable legacy-tlv pnp startup-vlan**，使能向下游设备发送的LLDP报文中携带PnP VLAN信息的功能。
   缺省情况下，交换机已使能向下游设备发送的LLDP报文中携带PnP VLAN信息的功能。
5. 执行命令**quit**，退出以太网接口视图。
6. （可选）当交换机之间是通过Eth-Trunk接口相连时，还需要执行如下步骤：
   a. 执行命令**interface eth-trunk** *trunk-id*，进入Eth-Trunk接口视图。
   b. 执行命令**pnp startup-link-aggregation enable**，使能向下游设备传递需要建立Eth-Trunk链路的功能。
      缺省情况下，交换机未使能向下游设备传递需要建立Eth-Trunk链路的功能。

3.7 通过中间文件实现带配置设备部署

说明

带配置是指设备上出厂时已有包含带配置部署相关命令的配置文件，此配置文件用户可根据需求定制。设备正常运行情况下，用户不可以通过执行命令行进行自主配置。

设备正常运行情况下，用户如果要启动带配置部署流程，可以通过重新设置下次启动使用的配置文件并重启设备的方式来实现。设备下次启动使用的配置文件中必须包含带配置部署相关命令行。

前置任务

通过中间文件实现EasyDeploy功能之前，需完成以下任务：

- 文件服务器、DHCP服务器与待配置设备（获取IP地址后）之间路由可达。
- 设备安装工程师上报待配置设备的MAC地址或ESN序列号。获取方法：设备表面贴的标签上可以查看设备的系统MAC地址和ESN序列号。

配置流程

请按照以下配置顺序完成配置。

3.7.1 配置文件服务器

背景信息

文件服务器用于存放待配置设备需要下载的版本文件，可以将网络中其他交换机或者服务器配置为文件服务器。EasyDeploy支持的文件服务器类型有FTP、TFTP和SFTP，建议使用SFTP服务器。

说明

此处给出的是交换机作为SFTP服务器的配置。如果使用的是第三方服务器，配置的具体方法请参见第三方服务器的操作指导。

操作步骤

步骤1 使能SFTP功能。具体操作步骤请参见“**8.3.3 通过SFTP进行文件操作**”中的“**配置SFTP服务器功能及参数**”。

步骤2 配置SSH用户的用户登录界面、用户名、认证方式、服务方式、SFTP服务授权目录等。具体操作步骤请参见“**8.3.3 通过SFTP进行文件操作**”中的“**配置SSH用户登录的用户界面**”和“**配置SSH用户**”。

----结束

后续处理

配置完文件服务器后，将待配置设备需要下载的文件上传至文件服务器的工作目录下。

说明

- 上传文件时，要保证存放目录下有足够的存储空间。
- 如果待配置设备数量较多，可以将文件服务器的并发访问数设置大一些，否则部分待配置设备会由于等待连接文件服务器而将整个部署时间延长。
- 为充分保证文件服务器的安全，建议配置的文件服务器用户名唯一。EasyDeploy过程结束后，请关闭相应的文件服务器功能。

3.7.2 编辑中间文件

背景信息

中间文件存放在文件服务器上，文件内容为SNMP主机的IP地址、设备MAC地址、ESN序列号、设备型号Model、待下载文件的信息等。当设备获得文件服务器的IP地址后，就从文件服务器上下载中间文件进行解析，查询到与本设备MAC地址、ESN序列号或设备型号Model匹配的系统软件名称，系统软件的版本号，补丁文件名称，Web网页文件名称和配置文件名称，然后根据名称从文件服务器下载文件。带配置部署流程中，设备产生的告警可以发送到指定地址的SNMP主机上。

操作步骤

根据SNMP主机的IP地址、设备的MAC地址、ESN序列号或设备型号Model与所需的系统软件、补丁文件、Web网页文件和配置文件名称，编辑中间文件，具体步骤如下：

1. 新建一个后缀名为.cfg的文本文档。
2. 编辑中间文件。

   假设一台待配置设备的MAC地址为xxxx-xxxx-xxxx，设备序列号ESN为93000701xxxxxxxx，设备型号Model为S5731-H24T4XC，对应这台设备应下载的版本文件名为auto_V200R022C00SPC200.cc，版本号信息为V200R022C00SPC200，补丁文件为auto_V200R022C00.pat，配置文件为auto_V200R022C00.cfg，Web网页文件为auto_V200R022C00.web.7z，SNMP主机的IP地址为192.168.1.1，接收Trap报文的端口号为1000（可以不指定，如果不指定，则使用默认端口号162），则中间文件lswnet.cfg内容如下（中间文件中各配置项名称必须为小写）：

   ```
   snmphostv4=192.168.1.1;snmphostport=1000;
   mac=xxxx-xxxx-
   xxxx;vrpfile=auto_V200R022C00SPC200.cc;vrpver=V200R022C00SPC200;patchfile=auto_V200R022C00.pat;cfgfile=auto_V200R022C00.cfg;webfile=auto_V200R022C00.web.7z;
   ```


说明

- 当有多台设备需要配置时，中间文件的每行对应一台设备的配置信息。中间文件的大小不能超过1M。
- 中间文件的配置项中，MAC地址、设备序列号ESN和设备型号Model必选其一，三者的优先级从高到低分别为MAC地址、设备序列号ESN、设备型号Model；配置文件为必选项，系统软件、Web网页文件和补丁文件为可选项，三者间没有顺序限制。
- 如果中间文件中包含版本号信息，则必须要包含系统软件名称，并且要求系统软件的版本号与中间文件中的版本号信息一致。
- 中间文件中可以指定接收Trap报文的端口号，系统软件、补丁文件、Web文件和配置文件的路径，如：

  ```
  snmphostv4=192.168.1.1;snmphostport=1000;
  mac=xxxx-xxxx-
  xxxx;vrpfile=auto_V200R022C00SPC200.cc;vrpver=V200R022C00SPC200;patchfile=auto_V200R022C00.pat;cfgfile=auto_V200R022C00.cfg;webfile=auto_V200R022C00.web.7z;
  ```

  其中auto为指定文件所在文件服务器的文件夹。
- 中间文件中指定的系统软件、补丁文件、Web网页文件和配置文件路径不能超过48字符。

3.7.3 配置 DHCP

背景信息

在配置通过中间文件实现EasyDeploy功能之前，必须先部署DHCP服务器，保证待配置设备能通过DHCP服务器获取到IP地址。

如果待配置设备与DHCP服务器在同一网段，则配置DHCP服务器即可。如果待配置设备与DHCP服务器在不同网段，除了需要配置DHCP服务器外，还需要配置DHCP中继。

下面操作步骤中以交换机为例配置DHCP服务器。如果使用的是第三方设备，配置的具体方法请参见第三方设备的操作指导。

此处给出DHCP服务器的基本配置，如果需要灵活部署DHCP功能，请参见《S300, S500, S2700, S5700, S6700 V200R022C00 配置指南-IP业务》DHCP配置。

注意

- DHCP服务器不支持认证，存在被仿冒的风险，建议用户在安全组网环境中使用信任的DHCP服务器进行开局。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**dhcp enable**，使能DHCP服务。

步骤3 执行命令**interface** *interface-type interface-number*，进入接口视图。

步骤4 （可选）对于以太网接口，执行命令**undo portswitch**，配置接口切换到三层模式。

缺省情况下，以太网接口处于二层模式。

说明

仅S5731-H、S5731-S、S5731S-H、S5731-H-K、S5731S-S、S5732-H、S5732-H-K、S6720-EI、S6735-S、S6720S-EI、S6730-H、S6730S-H、S6730-H-K、S6730-S和S6730S-S支持二层模式与三层模式切换。

步骤5 执行命令**dhcp select global**，配置接口工作在全局地址池模式。

步骤6 执行命令**quit**，返回到系统视图。

步骤7 执行命令**ip pool** *ip-pool-name*，创建全局地址池并进入全局地址池视图。

步骤8 执行命令**network** *ip-address* [**mask** { *mask* | *mask-length* }]，配置全局地址池可动态分配的IP地址范围。

- 配置的IP地址范围应该避免使用待配置设备需要加载的配置文件里面已经配置的IP地址，以防止地址冲突。
- 保证DHCP服务器上有可用的IP地址提供给待配置设备。

步骤9 执行命令**gateway-list** *ip-address* &<1-8>，配置DHCP客户端的出口网关地址。

----结束

3.7.4 带配置设备部署

背景信息

在某些特定场景下，设备出厂时可以自带定制化的配置文件，配置文件中包含了带配置部署相关的命令行，用以指定文件服务器地址、开局使用的中间文件名、设备与SNMP主机的共享密钥等。用户仅需简单地配置设备上线，设备就可以自动获取并加载正确的配置，减少用户的操作成本。

说明

带配置部署流程中，设备处于Busy状态，不允许用户执行其他配置命令，只能执行查询操作。

带配置部署相关命令包含于设备出厂自带的配置文件中，设备正常运行情况下，用户不可以自主手动执行。

设备正常运行情况下，用户如果要启动带配置部署流程，可以通过重新设置下次启动使用的配置文件并重启设备的方式来实现。设备下次启动使用的配置文件中必须包含带配置部署相关命令行。

如果用户不希望使用带配置部署功能，为了避免设备出厂自带的配置对其他功能产生影响，可以手动执行对应的undo命令将配置取消掉。

相关命令

设备自带的配置文件中包含的命令行如表3-5所示。

表 3-5 带配置部署相关的命令行

功能	命令	备注
使能设备的带配置部署功能	**easy-operation client ztp-with-cfg enable**	缺省情况下，设备没有使能带配置部署功能。

功能	命令	备注
（可选）指定带配置部署流程中所使用的中间文件	**easy-operation client netfile** *filename*	缺省情况下，设备使用的中间文件为lswnet.cfg。
（可选）指定带配置部署流程中所用的VLAN	**easy-operation client vlan** *vlanid*	缺省情况下，设备使用的VLAN为VLAN 1。
配置文件服务器的相关信息	通过IP地址方式指定： • **easy-operation client ftp-server** *ipaddress* &<1-4> [**username** *username* [**password** *password*]] • **easy-operation client sftp-server** *ipaddress* &<1-4> [**username** *username* [**password** *password*]] • **easy-operation client tftp-server ip-address** *ipaddress* &<1-4>	• 只能指定一种文件服务器类型。 • 用户在指定文件服务器的地址时，可以通过IP地址的方式指定，也可以通过URL地址的方式指定，二者只能选其一。 • 如果使用的是SFTP或FTP服务器，用户名及密码是否需要指定取决于服务器端是否设置了用户名及密码。 • 使用FTP或TFTP协议存在安全风险，推荐使用SFTP服务器。

功能	命令	备注
	通过URL地址方式指定： • **easy-operation client ftp-server-url** *ipaddress* [**username** *username* [**password** *password*]] • **easy-operation client sftp-server-url** *ipaddress* [**username** *username* [**password** *password*]] • **easy-operation client tftp-server-url ip-address** *ipaddress*	
配置设备与SNMP主机的共享密钥	**easy-operation client snmp securityname cipher** *password*	-

配置文件实例

假设某地需要通过带配置部署的方式配置一批华为交换机，设备所需的中间文件及版本文件等都已上传到文件服务器上，SFTP文件服务器的IP地址为10.1.1.1，用户名和密码分别为test和easyoperation，设备与SNMP主机的共享密钥为YsHsjx_202206，中间文件名称为ztpwithcfg.cfg，使用的VLAN为VLAN 100。此时设备出厂时自带的配置文件应当包含如下配置：

```
#
easy-operation client ztp-with-cfg enable
easy-operation client netfile ztpwithcfg.cfg
easy-operation client vlan 100
easy-operation client sftp-server ip-address 10.1.1.1 username test password easyoperation
easy-operation client snmp securityname cipher YsHsjx_202206
#
return
```

3.8 通过 Commander 实现零配置设备部署

可通过两种方式实现零配置设备部署，区别是Commander上是否使能了网络拓扑收集功能。通过使能网络拓扑收集方式，无需用户手动收集设备MAC地址或ESN序列号等信息，零配置设备上电启动完成后，Commander可自动收集到这些信息并为设备分配Client ID，完成设备信息与设备的绑定，即收集到网络拓扑信息，并根据网络拓扑信息来配置下载文件信息，实现零配置设备部署。如果不使能网络拓扑收集功能，则需要手动收集设备MAC地址或ESN序列号等信息，并手动配置Client与设备的对应关系。

前置任务

配置通过Commander实现零配置部署功能之前，需完成以下任务：

- 不使能网络拓扑收集功能方式
  - DHCP服务器、文件服务器、Commander与Client（获取IP地址后）之间路由可达。
  - 设备安装工程师上报待配置设备的MAC地址或ESN序列号。获取方法：设备表面贴的标签上可以查看设备的系统MAC地址和ESN序列号。
- 使能网络拓扑收集功能方式
  - DHCP服务器、文件服务器、Commander与Client（获取IP地址后）之间路由可达。
  - Client已上电启动完成。

配置流程

请按照以下配置顺序完成配置。

3.8.1 配置文件服务器

背景信息

文件服务器是用于存放Client需要下载的文件的设备。用户也可以将Commander设备配置为文件服务器，但由于文件服务器需要占用设备的存储资源，因此在使用Commander作为文件服务器时，需要考虑存储空间的问题。所以在EasyDeploy网络中，一般需要部署第三方服务器。

EasyDeploy支持的文件服务器类型有FTP、TFTP和SFTP，建议使用SFTP服务器。

说明

此处给出的是交换机作为SFTP服务器的配置。如果使用的是第三方服务器，配置的具体方法请参见第三方服务器的操作指导。

操作步骤

步骤1 使能SFTP功能。具体操作步骤请参见“**8.3.3 通过SFTP进行文件操作**”中的“**配置SFTP服务器功能及参数**”。

步骤2 配置SSH用户的用户登录界面、用户名、认证方式、服务方式、SFTP服务授权目录等。具体操作步骤请参见“**8.3.3 通过SFTP进行文件操作**”中的“**配置SSH用户登录的用户界面**”和“**配置SSH用户**”。

----结束

后续处理

配置完文件服务器后，将Client需要下载的文件保存至文件服务器的工作目录下。

说明

- 上传文件时，要保证存放目录下有足够的存储空间。
- 如果Client数量较多，那么同时部署时，部分Client会由于等待连接文件服务器而将整个部署时间延长。这种情况下，如果文件服务器支持配置并发访问数，可以将并发访问数设置大一些。
- 为充分保证文件服务器的安全，建议配置的文件服务器用户名唯一。EasyDeploy过程结束后，请关闭相应的文件服务器功能。

3.8.2 配置 DHCP

背景信息

在实现零配置部署功能之前，必须部署DHCP，确保作为DHCP客户端的Client可以从DHCP服务器获取自身IP地址及Commander的IP地址，从而实现通过Commander获取需要下载的文件的信息。

如果Client与DHCP服务器在同一网段，则配置DHCP服务器即可。如果Client与DHCP服务器在不同网段，除了需要配置DHCP服务器外，还需要配置DHCP中继。

可以将Commander设备配置为DHCP服务器或者是DHCP中继，DHCP服务器也可以是网络中其他交换机或另外部署第三方设备。下面操作步骤以网络中其他交换机为例配置DHCP服务器。如果使用的是第三方设备，配置的具体方法请参见第三方设备的操作指导。

DHCP服务器必须支持配置相关的Option参数。此处给出DHCP服务器的基本配置，如果需要灵活部署DHCP功能，请参见《S300, S500, S2700, S5700, S6700 V200R022C00 配置指南-IP业务》DHCP配置。

注意

- DHCP服务器不支持认证，存在被仿冒的风险，建议用户在安全组网环境中使用信任的DHCP服务器进行开局。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**dhcp enable**，使能DHCP服务。

步骤3 执行命令**interface** *interface-type interface-number*，进入接口视图。

步骤4 （可选）对于以太网接口，执行命令**undo portswitch**，配置接口切换到三层模式。

缺省情况下，以太网接口处于二层模式。

说明

仅S5731-H、S5731-S、S5731S-H、S5731-H-K、S5731S-S、S5732-H、S5732-H-K、S6720-EI、S6735-S、S6720S-EI、S6730-H、S6730S-H、S6730-H-K、S6730-S和S6730S-S支持二层模式与三层模式切换。

步骤5 执行命令**dhcp select global**，配置接口工作在全局地址池模式。

步骤6 执行命令**quit**，返回到系统视图。

步骤7 执行命令**ip pool** *ip-pool-name*，创建全局地址池并进入全局地址池视图。

步骤8 执行命令**network** *ip-address* [**mask** { *mask* | *mask-length* }]，配置全局地址池可动态分配的IP地址范围。

- 配置的IP地址范围应该避免使用零配置Client需要加载的配置文件里面已经配置的IP地址，以防止地址冲突。
- 保证DHCP服务器上有可用的IP地址提供给待配置设备。

步骤9 执行命令**gateway-list** *ip-address* &<1-8>，配置DHCP客户端的出口网关地址。

步骤10 执行命令**option 148 ascii** *ascii-string*，配置DHCP服务器的Option参数。

- 此处必须配置**option 148**，表示Commander的IP地址及端口号，即通过Commander实现EasyDeploy功能。
- *ascii-string*的格式为“ipaddr=*ip-address*;port=*udp-port*;”。例如：Commander的IP地址为10.10.10.1，端口号为60000，则*ascii-string*可以表示为：**ipaddr=10.10.10.1;port=60000;**或者**ipaddr=10.10.10.1;**，端口号60000是缺省值可以省略。

----结束

在使用EasyDeploy进行零配置开局时，如果Commander与Client通信时，不使用默认的VLAN1，此时Commander需要执行以下步骤把修改后的VLAN ID通知给Client设备。

1. 执行命令**pnp startup-vlan** *vlan-id*，配置有线PnP VLAN ID。

   缺省情况下，交换机未配置有线PnP VLAN ID。
2. 执行命令**pnp startup-vlan send enable**，使能向下游设备发送的LLDP报文中携带PnP VLAN信息的功能。

   缺省情况下，换机未使能向下游设备传递PnP VLAN的功能。
3. 执行命令**interface** *interface-type interface-number*，进入以太接口视图。
4. 执行命令**lldp tlv-enable legacy-tlv pnp startup-vlan**，使能向下游设备发送的LLDP报文中携带PnP VLAN信息的功能。

   缺省情况下，交换机已使能向下游设备发送的LLDP报文中携带PnP VLAN信息的功能。
5. 执行命令**quit**，退出以太网接口视图。

6. （可选）当交换机之间是通过Eth-Trunk接口相连时，还需要执行如下步骤：
   a. 执行命令**interface eth-trunk** *trunk-id*，进入Eth-Trunk接口视图。
   b. 执行命令**pnp startup-link-aggregation enable**，使能向下游设备传递需要建立Eth-Trunk链路的功能。

      缺省情况下，交换机未使能向下游设备传递需要建立Eth-Trunk链路的功能。

3.8.3 配置 Commander

3.8.3.1 配置 Commander 基本功能

背景信息

通过Commander实现EasyDeploy功能，最重要的步骤之一就是在网络中指定一台合适的设备，并在该设备上配置Commander使能。

说明

为了方便设备统一管理，建议在同一个运行EasyDeploy功能的网络中，只指定其中一台设备作为Commander。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**easy-operation commander ip-address** *ip-address* [**udp-port** *udp-port*]，配置Commander的IP地址。

配置的IP地址必须是Commander设备中存在的IP地址。

步骤3 执行命令**easy-operation commander enable**，使能设备的Commander功能，成为网络中的Commander设备。

缺省情况下，Commander功能不使能。

----结束

3.8.3.2 配置文件服务器信息

背景信息

文件服务器信息是指Client需要获取的文件服务器IP地址、用户名和密码等信息。

Client需要下载的文件都保存在文件服务器中，当Client从Commander获取文件信息后，就会根据这些信息从Commander上配置的文件服务器中下载指定文件。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**easy-operation**，进入Easy-Operation视图。

步骤3 根据文件服务器类型选择以下配置：

- 执行命令**tftp-server** *ip-address*，配置TFTP服务器的IP地址。

- 执行命令**ftp-server** *ip-address* [**username** *username* [**password** *password*]]，配置FTP服务器的IP地址，用户名及密码。
- 执行命令**sftp-server** *ip-address* [**username** *username* [**password** *password*]]，配置SFTP服务器的地址，用户名及密码。

  如果使用的是SFTP或FTP服务器，用户名及密码是否需要指定取决于服务器端是否设置了用户名及密码。

  只可在Commander上配置一种文件服务器信息，以最后一次的配置为准。

  说明

  使用FTP、TFTP协议存在安全风险，推荐使用SFTP服务器。

----结束

3.8.3.3 （可选）配置网络拓扑收集功能

背景信息

网络拓扑收集功能是基于**NDP**和**NTDP**协议的，由Commander作为网络拓扑收集设备。通过网络拓扑收集功能实现零配置设备部署，无需用户手动收集设备MAC地址或ESN序列号等信息，零配置设备上电启动完成后，Commander可自动收集到这些信息并为设备分配Client ID，完成设备信息与设备的绑定，即收集到网络拓扑信息，并根据网络拓扑信息来配置下载文件信息。

操作步骤

1. 配置NDP
   a. 执行命令**system-view**，进入系统视图。
   b. 执行命令**ndp enable**，全局使能NDP。

      缺省情况下，全局NDP功能处于使能状态。
   c. （可选）执行命令**ndp enable interface** { *interface-type interface-number* [**to** *interface-type interface-number*] }&<1-10>，使能接口NDP功能。

      缺省情况下，接口NDP功能处于使能状态。
   d. （可选）执行命令**ndp timer aging** *aging-time*，配置NDP信息的老化时间。

      缺省情况下，NDP信息的老化时间为180秒。NDP信息的老化时间必须比NDP报文发送的时间间隔长。
   e. （可选）执行命令**ndp timer hello** *interval*，配置NDP报文发送的时间间隔。

      缺省情况下，NDP报文发送时间间隔为60秒。NDP报文发送的时间间隔必须比NDP信息的老化时间短。
   f. （可选）执行命令**ndp trunk-member enable**，使能基于Trunk成员口的NDP功能。

      缺省情况下，基于Trunk成员口的NDP功能处于去使能状态。

      进行NTDP拓扑收集时，如果设备间的链路使用Trunk口连接，缺省情况下系统将基于Trunk逻辑口进行邻居发现及拓扑呈现。如果用户希望呈现Trunk成员口的连接信息，可以执行本命令，使能基于Trunk成员口的NDP功能进行邻居发现，并通过网管得到实际的物理口拓扑信息。

2. 配置NTDP
   a. 执行命令**ntdp enable**，全局使能NTDP。
      缺省情况下，全局NTDP功能处于使能状态。
   b. （可选）使能接口的NTDP功能。
      i. 执行命令**interface range** { *interface-type interface-number1* [**to** *interface-type interface-number2*] } &<1-10>，进入端口组视图。
      ii. 执行命令**ntdp enable**，使能接口的NTDP功能。
      缺省情况下，接口NTDP功能处于使能状态。
      iii. 执行命令**quit**，返回系统视图。
   c. （可选）执行命令**ntdp hop** *max-hop-value*，配置拓扑收集范围。
      缺省情况下，通过NTDP进行拓扑收集的最大跳数是8。拓扑收集范围越大，占用拓扑收集设备的内存越多。
   d. （可选）执行命令**ntdp timer hop-delay** *hop-delay-time*，配置转发NTDP报文的跳数延迟时间。
      缺省情况下，设备在转发NTDP拓扑请求报文时的跳数延迟时间是200毫秒。
   e. （可选）执行命令**ntdp timer port-delay** *port-delay-time*，配置转发NTDP报文的接口延迟时间。
      缺省情况下，NTDP的接口延迟时间为20ms。
   f. 执行命令**ntdp timer** *interval*，配置定时拓扑收集的时间间隔。
      缺省情况下，定时拓扑收集的时间间隔为0分钟，即不进行定时拓扑收集。

      说明

      由于Commander的网络拓扑收集周期为5分钟，建议将NTDP拓扑收集时间间隔设置小于5分钟。

   g. （可选）用户视图下执行命令**ntdp explore**，手动收集拓扑信息。
      用户可以通过此命令随时收集网络拓扑。
3. 配置集群管理VLAN
   a. 执行命令**system-view**，进入系统视图。
   b. 执行命令**cluster enable**，使能网络集群功能。
      缺省情况下，集群功能处于禁止状态。
   c. 执行命令**cluster**，进入集群视图。
   d. 执行命令**mngvlanid** *vlanid*，配置集群管理VLAN。
      缺省情况下，集群管理VLAN是VLAN 1，但是不建议用户使用缺省的VLAN 1作为集群管理VLAN，建议通过命令修改为其他VLAN。

      说明

      集群管理VLAN要同Commander上与Client相连的端口所加入的VLAN保持一致。
4. 配置Commander拓扑收集
   a. 执行命令**system-view**，进入系统视图。
   b. 执行命令**easy-operation**，进入Easy-Operation视图。
   c. 执行命令**topology enable**，使能Commander的网络拓扑收集功能。
      缺省情况下，未使能Commander的网络拓扑收集功能。

d. (可选)执行命令**topology save**，保存当前收集到的网络拓扑信息。

e. (可选)执行命令**client auto-join enable**，使能Client自动加入功能。

缺省情况下，Client自动加入功能不使能。

使能Client自动加入功能后，Commander将自动学习Client的信息，并自动分配一个当前最小且未被分配的ID。不使能自动加入功能，则不会给Client自动分配ID，需要通过**client** [*client-id*] { **mac-address** *mac-address* | **esn** *esn* }确定Client与ID的对应关系。

任务示例

执行命令**display easy-operation topology**，查看已使能Client自动加入功能的Commander收集到的网络拓扑信息。

```
<HUAWEI> display easy-operation topology
<-->:normal device        <??>:lost device
Total topology node number: 3
------------------------------------------------------------------------------
[HUAWEI: xxxx-xxxx-xxxx](Commander)
|-(GE0/0/8)<-->(GE0/0/38)[HUAWEI: xxxx-xxxx-xxxx](Client 1)
| |-(GE0/0/16)<-->(GE0/0/16)[HUAWEI: xxxx-xxxx-xxxx](Client 2)
```

如上显示信息所示，网络拓扑发现的Client已分配ID。如果不使能Client自动加入功能，则不会显示Client的ID。

3.8.3.4 配置下载文件信息

背景信息

下载文件信息是指Client需要下载的文件的信息，包括系统软件名及版本号、补丁文件名、配置文件名等。网络管理员可以根据需要任意指定需要下载的文件类型。

在零配置部署场景中，可以为每台设备单独指定下载文件信息，也可以将具有相同属性的设备划分Group，配置相同的下载文件信息。设备优先匹配单台Client规则，如果未匹配上，则匹配Group规则。如果未匹配到任何规则，或者匹配到了规则但是规则下没有配置下载文件信息，则会使用默认的下载文件信息。

操作步骤

根据网络规划选择以下配置。

配置单台Client的下载文件信息

1. 执行命令**system-view**，进入系统视图。
2. 执行命令**easy-operation**，进入Easy-Operation视图。
3. 以下两种情况下需要手工进行设备信息与设备的绑定，其他情况可直接执行下一步骤：
   - 如果不是通过网络拓扑收集功能进行零配置设备部署

     执行命令**client** [*client-id*] { **mac-address** *mac-address* | **esn** *esn* }，配置Client的匹配规则，即根据MAC地址或ESN号匹配Client，用来唯一标识一台Client。

     如果未指定*client-id*，则会自动分配一个当前最小且未被分配的ID。
   - 如果是通过网络拓扑收集功能进行零配置设备部署，但是未使能Client自动加入功能

执行命令**client** [*client-id*] **mac-address** *mac-address*，配置Client的匹配规则，即通过MAC地址匹配Client。

4. 执行命令**client** *client-id* { **system-software** *file-name* [*version*] | **patch** *file-name* | **configuration-file** *file-name* | **web-file** *file-name* | { **custom-file** *file-name* } &<1-3> }*，配置Client需要下载的文件的信息。

配置Group的下载文件信息

1. 执行命令**system-view**，进入系统视图。
2. 执行命令**easy-operation**，进入Easy-Operation视图。
3. 根据配置的Group类型，选择配置
   - 配置内置Group匹配规则
     i. 执行命令**group build-in** *device-type*，创建内置Group，通过*device-type*指定匹配的设备类型,并进入内置Group视图。
   - 配置自定义Group匹配规则
     i. 执行命令**group custom** { **mac-address** | **esn** | **ip-address** | **model** | **device-type** } *group-name*，创建自定义Group，并进入自定义Group视图。
     ii. 执行命令**match** { **mac-address** *mac-address* [*mac-mask* | *mac-mask-length*] | **esn** *esn* | **ip-address** *ip-address* [*ip-mask* | *ip-mask-length*] | **model** *model* | **device-type** *device-type* }，配置自定义Group的匹配规则。

   说明

   - 在Commander上最多可以配置256个Group，所有Group的规则总数不能超过256条。自定义Group中，对于MAC地址、IP地址和ESN序列号类型的Group，可配置多条匹配规则，设备类型和型号类型的Group只能配置一条匹配规则。
   - 如果配置了多个类型的Group，则各个类型的Group匹配优先级如下：MAC地址 > ESN序列号 > IP地址 > 设备型号 > 自定义的设备类型 > 内置的设备类型。
   - 如果同一类型不同名称的多个Group匹配同一设备时，按Group名称的字典序排序来判断优先级。
4. 根据需要下载的文件选择配置。
   - 执行命令**system-software** *file-name* [*version*]，配置需要下载的系统软件名称和版本号。
   - 执行命令**patch** *file-name*，配置需要下载的补丁文件名称。
   - 执行命令**configuration-file** *file-name*，配置需要下载的配置文件名称。
   - 执行命令**web-file** *file-name*，配置需要下载的Web网页文件名称。
   - 执行命令{ **custom-file** *file-name* } &<1-3>，配置需要下载的用户自定义文件名称，目前支持配置3个自定义文件。

配置默认的下载文件信息

1. 执行命令**system-view**，进入系统视图。
2. 执行命令**easy-operation**，进入Easy-Operation视图。
3. 根据需要下载的文件选择配置。
   - 执行命令**system-software** *file-name* [*version*]，配置需要下载的系统软件名称和版本号。
   - 执行命令**patch** *file-name*，配置需要下载的补丁文件名称。

- 执行命令**configuration-file** *file-name*，配置需要下载的配置文件名称。
- 执行命令**web-file** *file-name*，配置需要下载的Web网页文件名称。
- 执行命令{ **custom-file** *file-name* } &<1-3>，配置需要下载的用户自定义文件名称，目前支持配置3个自定义文件。

3.8.3.5 配置下载后文件的激活策略

背景信息

下载后文件的激活策略包括：

- 文件激活的时间
  - 指定时间激活：指定在某个时间点开始激活文件。
  - 延时激活：在文件下载完成后延迟一定的时间开始激活文件，最长可以延迟24小时。
- 文件激活的方式
  - 不复位：缺省情况下，系统使用不复位激活策略。但是，如果下载文件中包含了系统软件（*.cc），则无论是否配置了复位激活方式，系统都会复位。如果不包含系统软件，则系统默认不会复位，这种策略下：
    - 补丁文件将自动激活。
    - 配置文件将被反译后逐行输入设备，实现配置，同时Client会将此配置文件作为下次启动项。但是如果配置恢复过程中有配置执行失败，则系统会通过复位方式激活配置文件。
    - Web网页文件需要手动进行激活。
  - 复位：系统软件、补丁文件和配置文件将会作为Client的下次启动项；Web网页文件需要复位后手动进行激活。
    - 如果补丁为热补丁，则可以采用默认不复位方式激活；如果为冷补丁，则需要配置复位方式激活。
    - 如果加载了配置文件且采用不复位方式进行激活，当配置文件中有命令恢复失败时，Client会自动通过复位的方式激活配置文件。
    - 如果网络中的Client有串联组网（Client下挂Client）的方式，建议在Commander全局下配置延时激活时间。以免上级Client因为获取文件后立即激活重启或配置变更，使下挂的Client与Commander或者文件服务器发生中断，从而导致下挂的Client零配置部署流程失败。需要根据下挂Client所下载的文件大小设置合理的延时时间，以确保所有下挂的Client在这个延时时间内完成文件下载。

根据下载文件信息的配置，选择下载后文件的激活策略：

- 如果在下载文件信息步骤中配置了Group来匹配Client，则以Group中配置的激活方式和时间生效。如果Group中没有配置激活方式和时间，则以Commander全局配置的生效。如果Commander全局也没有配置激活方式和时间，则采用缺省的激活方式和时间。
- 如果在下载文件信息步骤中配置的是指定Client或默认的下载文件信息，则以Commander全局配置的激活方式和时间生效。如果Commander全局没有配置激活方式和时间，则采用缺省的激活方式和时间。

操作步骤

配置Group的文件激活策略

1. 执行命令**system-view**，进入系统视图。
2. 执行命令**easy-operation**，进入Easy-Operation视图。
3. 执行命令**group build-in** *device-type*，进入内置Group视图。

   或者

   执行命令**group custom** { **mac-address** | **esn** | **ip-address** | **model** | **device-type** } *group-name*，进入自定义Group视图。
4. 执行命令**activate-file** { **reload** | { **in** *time* | **delay** *delay-time* } }*，配置匹配相应Group的文件激活策略。

配置全局的文件激活策略

1. 执行命令**system-view**，进入系统视图。
2. 执行命令**easy-operation**，进入Easy-Operation视图。
3. 执行命令**activate-file** { **reload** | { **in** *time* | **delay** *delay-time* } }*，配置全局的文件激活策略。

3.8.3.6 （可选）使能自动清理存储空间功能

背景信息

Client在下载系统软件时，可能因为存储器空间不足，而导致无法下载成功。如果使能自动清理存储空间功能，则会删除Client上的非启动系统软件。

说明

启动系统软件包括当前正在运行使用的系统软件以及配置的下次启动系统软件。Client清理存储空间时，不能删除启动系统软件。

Client在执行自动清理存储器空间时，依赖文件服务器的类型。如果从TFTP服务器下载文件，由于无法获取到文件大小，因此无法执行自动清理存储器空间的动作。在使用FTP或者SFTP服务器时，如果服务器不支持返回文件大小的功能，则Client也不能执行自动清理存储器空间的动作。使用S交换机作FTP或TFTP文件服务器时，不支持返回文件大小的功能。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**easy-operation**，进入Easy-Operation视图。

步骤3 执行命令**client auto-clear enable**，使能自动清理存储器空间的功能。

缺省情况下，自动清理存储器空间功能不使能。

----结束

3.8.3.7 （可选）配置自动备份配置文件功能

背景信息

配置自动备份配置文件功能后，Client的配置文件会自动备份至文件服务器，可用于故障替换场景。当新Client替换了故障Client后，新Client必须要获取到原故障Client的实时配置文件，将故障带来的影响降至最小。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**easy-operation**，进入Easy-Operation视图。

步骤3 执行命令**backup configuration interval** *interval* [**duplicate**]，配置自动备份配置文件的时间间隔和模式。

缺省情况下，自动备份配置文件功能不使能。

----结束

3.8.4 检查配置结果

操作步骤

- 执行命令**display ip pool** { **interface** *interface-pool-name* | **name** *ip-pool-name* } **used**，DHCP服务器上查看为Client分配的IP地址信息。
- 执行命令**display easy-operation configuration**，查看Commander的配置信息。
- 执行命令**display easy-operation client** [*client-id* | **mac-address** *mac-address* | **esn** *esn* | **verbose**]，查看Commander上的Client的信息。
- 执行命令**display easy-operation group** [**build-in** [*device-type* [**vendor** *vendorname*]] | **custom** [*groupname*]]，查看Commander上配置的Group信息。
- 执行命令**display easy-operation download-status** [**client** *client-id* | **verbose**]，查看Client的下载状态信息。
- （通过网络拓扑收集功能部署）执行命令**display ndp**，查看系统NDP配置信息。
- （通过网络拓扑收集功能部署）执行命令**display ndp interface** { *interface-type interface-number1* [**to** *interface-type interface-number2*] }&<1-10>，查看指定接口NDP发现的邻居信息。
- （通过网络拓扑收集功能部署）执行命令**display ntdp**，查看全局NTDP信息。
- （通过网络拓扑收集功能部署）执行命令**display ntdp device-list** [**verbose**]，查看NTDP收集到的设备信息。
- （通过网络拓扑收集功能部署）执行命令**display easy-operation topology**，查看Commander收集到的网络拓扑信息。

----结束

3.9 通过 Commander 实现手动替换故障设备

背景信息

故障替换功能的实现必须是基于已部署EasyDeploy功能的网络，且要确保Commander上已通过**backup configuration interval** *interval* [**duplicate**]命令配置了自动备份配置文件功能。如果新Client没有获取到备份配置文件信息，即执行零配置部署流程，会获取Client信息库中的配置文件信息。如果也没有获取到，则会使用默认的配置文件信息。但此时无法保证与原故障Client中的配置文件一致。

前置任务

通过Commander实现手动替换故障设备之前，需完成以下任务：

- 文件服务器、DHCP服务器、Commander与新Client（获取IP地址后）之间路由可达。
- 已配置**文件服务器**、**DHCP**和**Commander**。
- 确保新Client为零配置设备。
- 设备安装工程师上报待配置设备的MAC地址或ESN序列号。获取方法：设备表面贴的标签上可以查看设备的系统MAC地址和ESN序列号。
- 如果要升级或下载其他文件，需要将文件上传至文件服务器的工作目录下。

操作步骤

配置替换信息

1. 执行命令**system-view**，进入系统视图。
2. 执行命令**easy-operation**，进入Easy-Operation视图。
3. 根据实际情况选择：
   - 如果只需要新Client恢复原来的配置，则执行命令**client** *client-id* **replace** { **mac-address** *mac-address* | **esn** *esn* }，配置*client-id*与新MAC地址或新ESN号的替换信息即可。
   - 如果还需要升级或下载其他文件，则执行命令**client** *client-id* **replace** { { **mac-address** *mac-address* | **esn** *esn* } | **system-software** *file-name* [*version*] | **patch** *file-name* | **web-file** *file-name* | **license** *file-name* | { **custom-file** *file-name* } &<1-3> }*，配置替换信息，可以通过此命令一次配置完成，也可通过此命令多次分别配置完成。故障设备的*client-id*与新MAC地址或新ESN号的替换信息必须要配置。

配置下载后文件的激活策略

1. 执行命令**system-view**，进入系统视图。
2. 执行命令**easy-operation**，进入Easy-Operation视图。
3. 执行命令**activate-file** { **reload** | { **in** *time* | **delay** *delay-time* } }*，配置下载后文件的激活策略。

替换故障设备

拆除故障设备，连接新设备。

检查配置结果

- 执行命令**display easy-operation client replace** [**verbose**]或**display easy-operation client** *client-id* **replace**，查看Commander上的替换信息库的信息。

3.10 通过 Commander 实现自动替换故障设备

背景信息

故障替换功能的实现必须是基于已部署EasyDeploy功能的网络，且要确保Commander上已通过**backup configuration interval** *interval* [**duplicate**]命令配置了自动备份配置文件功能。如果新Client没有获取到备份配置文件信息，即执行零配置部署流程，会获取Client信息库中的配置文件信息。如果也没有获取到，则会使用默认的配置文件信息。但此时无法保证与原故障Client中的配置文件一致。

前置任务

通过Commander实现自动替换故障设备之前，需完成以下任务：

- 文件服务器、DHCP服务器、Commander与新Client（获取IP地址后）之间路由可达。
- 已配置**文件服务器**、**DHCP**和**Commander**。
- 确保新Client为零配置设备。
- 如果要升级或下载其他文件，需要将文件上传至文件服务器的工作目录下。

操作步骤

如果需要升级或下载除配置文件之外的其他文件，则进行以下配置

1. 执行命令**system-view**，进入系统视图。
2. 执行命令**easy-operation**，进入Easy-Operation视图。
3. 执行命令**client** *client-id* **replace** { { **mac-address** *mac-address* | **esn** *esn* } | **system-software** *file-name* [*version*] | **patch** *file-name* | **web-file** *file-name* | **license** *file-name* | { **custom-file** *file-name* } &<1-3> }*，配置替换信息，可以通过此命令一次配置完成，也可通过此命令多次分别配置完成。可以不用指定新Client的MAC地址或ESN号。

说明

如果替换故障设备的新设备只是需要获取原设备的配置文件，那么只要能确保新设备与Commander的连接位置与原故障设备与Commander的连接位置相同，新设备即可自动实现故障替换，而不需要进行上述的配置。

配置下载后文件的激活策略

1. 执行命令**system-view**，进入系统视图。
2. 执行命令**easy-operation**，进入Easy-Operation视图。
3. 执行命令**activate-file** { **reload** | { **in** *time* | **delay** *delay-time* } }*，配置下载后文件的激活策略。

替换故障设备

拆除故障设备，连接新设备。

检查配置结果

- 执行命令**display easy-operation client replace** [**verbose**]或**display easy-operation client** *client-id* **replace**，查看Commander上的替换信息库的信息。

3.11 通过 Commander 批量升级设备

背景信息

常见的设备升级主要是对系统软件或者补丁文件的升级，建议Group按如下规则创建：

- 如果待升级的Client设备型号（module）相同，并且升级文件相同，建议配置内置Group进行升级。
- 如果设备型号不同，但是设备类型（device-type）相同并且升级文件相同，建议配置内置Group进行升级。
- 如果升级文件不同，并且待升级的设备型号也不同时，建议根据Client的IP地址规划，配置自定义Group进行升级。

如果未匹配到任何规则或者匹配到了规则，但是规则下没有配置下载文件信息，则会使用默认的下载文件信息。

前置任务

配置通过Commander实现批量升级功能之前，需完成以下任务：

- 文件服务器和Commander与Client之间路由可达。
- 确保已配置**文件服务器**、**Commander基本功能**和**文件服务器信息**。
- 确保已**将有配置设备加入Commander管理**。
- 确保Client处于正常运行状态。
- 将升级文件上传至文件服务器的工作目录下。

  说明

  为了增强Commander和Client之间通信的安全性，防止有仿冒的Commander获取Client的控制权，可以分别在Commander和Client的系统视图下通过**easy-operation shared-key**命令配置相同的共享密钥。

操作步骤

1. 配置下载文件信息
   - 配置Group的下载文件信息
     i. 执行命令**system-view**，进入系统视图。
     ii. 执行命令**easy-operation**，进入Easy-Operation视图。
     iii. 根据Group类型选择配置
     - 配置内置Group的匹配规则

       执行命令**group build-in** *device-type*，创建内置Group，通过*device-type*指定匹配的设备类型,并进入内置Group视图。
     - 配置自定义Group的匹配规则

执行命令**group custom** { **mac-address** | **esn** | **ip-address** | **model** | **device-type** } *group-name*，创建自定义Group，并进入自定义Group视图。

执行命令**match** { **mac-address** *mac-address* [*mac-mask* | *mac-mask-length*] | **esn** *esn* | **ip-address** *ip-address* [*ip-mask* | *ip-mask-length*] | **model** *model* | **device-type** *device-type* }，配置自定义Group的匹配规则。

说明

- 在Commander上最多可以配置256个Group，所有Group的规则总数不能超过256条。自定义Group中，对于MAC地址、IP地址和ESN序列号类型的Group，可配置多条匹配规则，设备类型和型号类型的Group只能配置一条匹配规则。
- 如果配置了多个类型的Group，则各个类型的Group匹配优先级如下：MAC地址 > ESN序列号 > IP地址 > 设备型号 > 自定义的设备类型 > 内置的设备类型。
- 如果同一类型不同名称的多个Group匹配同一设备时，按Group名称的字典序排序来判断优先级。

iv. 根据需要下载的文件选择配置。

- 执行命令**system-software** *file-name* [*version*]，配置需要下载的系统软件名称和版本号。
- 执行命令**patch** *file-name*，配置需要下载的补丁文件名称。
- 执行命令**configuration-file** *file-name*，配置需要下载的配置文件名称。
- 执行命令**web-file** *file-name*，配置需要下载的Web网页文件名称。
- 执行命令**license** *file-name*，配置需要下载的License文件名称。
- 执行命令{ **custom-file** *file-name* } &<1-3>，配置需要下载的用户自定义文件名称，目前支持配置3个自定义文件。

– 配置默认的下载文件信息

i. 执行命令**system-view**，进入系统视图。

ii. 执行命令**easy-operation**，进入Easy-Operation视图。

iii. 根据需要下载的文件选择配置。

- 执行命令**system-software** *file-name* [*version*]，配置需要下载的系统软件名称和版本号。
- 执行命令**patch** *file-name*，配置需要下载的补丁文件名称。
- 执行命令**configuration-file** *file-name*，配置需要下载的配置文件名称。
- 执行命令**web-file** *file-name*，配置需要下载的Web网页文件名称。
- 执行命令**license** *file-name*，配置需要下载的License文件名称。
- 执行命令{ **custom-file** *file-name* } &<1-3>，配置需要下载的用户自定义文件名称，目前支持配置3个自定义文件。

2. 配置下载后文件的激活策略

如果Group中没有配置激活方式和时间，则以Commander全局配置的生效。如果Commander全局也没有配置激活方式和时间，则采用缺省的激活方式和时间。

缺省情况下，如果下载的文件中包括系统软件或者配置文件，则采用复位设备的方式立即激活文件，否则采用不复位设备的方式激活。

- 配置Group的文件激活策略
  i. 执行命令**system-view**，进入系统视图。
  ii. 执行命令**easy-operation**，进入Easy-Operation视图。
  iii. 执行命令**group build-in** *device-type*，进入内置Group视图。
  或者
  执行命令**group custom** { **mac-address** | **esn** | **ip-address** | **model** | **device-type** } *group-name*，进入自定义Group视图。
  iv. 执行命令**activate-file** { **reload** | { **in** *time* | **delay** *delay-time* } }*，配置匹配相应Group的文件激活策略。
- 配置全局的文件激活策略
  i. 执行命令**system-view**，进入系统视图。
  ii. 执行命令**easy-operation**，进入Easy-Operation视图。
  iii. 执行命令**activate-file** { **reload** | { **in** *time* | **delay** *delay-time* } }*，配置全局的文件激活策略。

3. 启动批量升级
   a. 执行命令**system-view**，进入系统视图。
   b. 执行命令**easy-operation**，进入Easy-Operation视图。
   c. 执行命令**upgrade group** [*group-name*] &<1-15>，启动批量升级流程。

检查配置结果

- 执行命令**display easy-operation group** [**build-in** [*device-type* [**vendor** *vendorname*]] | **custom** [*groupname*]]，查看Commander上配置的Group信息库的信息。
- 执行命令**display easy-operation download-status** [**client** *client-id* | **verbose**]，查看Client的下载状态。

3.12 通过 Commander 批量配置设备

背景信息

制作命令行脚本有以下两种方式：

- 在线制作命令行脚本：使用**batch-cmd begin**命令开始在线编辑命令行脚本。命令录入完成后，使用系统快捷键Ctrl+C退出编辑。退出编辑以后，如果再次执行此命令开始在线编辑命令行脚本，原有已录入的命令行将被清除。

  说明

  在线制作的命令行脚本保存在Commander的内存中，如果Commander重启，在线录入的命令行将清除。

- 离线制作命令行脚本：将需要配置的命令行逐条写入批处理文件。批处理文件可以由文本文档进行编辑，每一条需执行的命令占据一行。脚本名称可以为“*.txt”或者“*.bat”。

从用户视图开始，依次执行脚本命令。由于命令行执行的结果保存在Client的内存中，所以命令行脚本中如果有清除Client内存的命令行，如**reboot**等，则命令下发后无法通过**display easy-operation batch-cmd result**查看批量配置的执行结果。

前置任务

配置通过Commander实现批量配置设备功能之前，需完成以下任务：

- Commander和Client之间路由可达。
- 确保已配置**Commander基本功能**。
- 确保已**将有配置设备加入Commander管理**。
- 确保Client处于正常运行状态。

说明

为了增强Commander和Client之间通信的安全性，防止有仿冒的Commander获取Client的控制权，可以分别在Commander和Client的系统视图下通过**easy-operation shared-key**命令配置相同的共享密钥。

操作步骤

步骤1 如果要下发命令行到Group，先创建Group

1. 执行命令**system-view**，进入系统视图。
2. 执行命令**easy-operation**，进入Easy-Operation视图。
3. 配置Group的匹配规则
   - 配置内置Group的匹配规则
     i. 执行命令**group build-in** *device-type*，创建内置Group，通过*device-type*指定匹配的设备类型,并进入内置Group视图。
   - 配置自定义Group的匹配规则
     i. 执行命令**group custom** { **mac-address** | **esn** | **ip-address** | **model** | **device-type** } *group-name*，创建自定义Group，并进入自定义Group视图。
     ii. 执行命令**match** { **mac-address** *mac-address* [*mac-mask* | *mac-mask-length*] | **esn** *esn* | **ip-address** *ip-address* [*ip-mask* | *ip-mask-length*] | **model** *model* | **device-type** *device-type* }，配置自定义Group的匹配规则。

步骤2 制作命令行脚本

- 在线制作命令行脚本
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**easy-operation**，进入Easy-Operation视图。
  c. 执行命令**batch-cmd begin**，进入命令行脚本编辑模式。
     - 同一时间，只允许一名网络管理员在线编辑命令行脚本。
     - 命令行脚本编辑模式下，30秒未操作则自动退出编辑模式返回到Easy-Operation视图，脚本中保留已经编辑完成的命令行。
  d. 编辑命令行脚本。

- 输入单条命令的最大长度为510个字符，包括使用不完整格式的情况。超过510个字符将无法输入。
- 脚本的命令行数量最大为200条。
- 录入命令时，按回车键确认输入。确认输入后，光标不能回退，即不能修改已确认输入的命令行。

e. 使用快捷键Ctrl+C退出命令行脚本编辑模式。

- 离线制作命令行脚本

  离线制作格式为“*.txt”或“*.bat”的命令脚本文件，然后将脚本文件上传至Commander的根目录下保存。离线命令行脚本中内容的格式要求与制作在线命令行脚本一致。

说明

- 命令行脚本中不支持中文字符。
- 离线制作的命令行脚本中，建议不要包含密码类的信息，否则安全得不到保证。
- 如果需要配置的命令比较多，建议使用离线制作命令行脚本的方式。如果一定要采用在线制作的方式，请保证输入的正确性，因为在线输入后，不能修改，不能查看，所以一旦输入错误，只能退出并再次进入编辑模式从第一条命令开始重新输入。

步骤3 下发命令行，根据不同的应用场景选择

- 下发命令行到指定的Client，执行命令**execute** [*script-file*] **to client** { *client-id1* [**to** *client-id2*] }&<1-10>。
- 下发命令行到所有Client，执行命令**execute** [*script-file*] **to client all**。
- 下发命令行到指定的Group，执行命令**execute** [*script-file*] **to group** { **name** *group-name* }&<1-10>。
- 下发命令行到所有Group，执行命令**execute** [*script-file*] **to group all**。

如果未指定*script-file*，则代表下发在线制作的命令行脚本；如果指定*script-file*，则代表下发指定的离线制作的命令行脚本。

----结束

检查配置结果

- 执行命令**display easy-operation batch-cmd result**，查看批量配置的执行结果。

3.13 将有配置设备加入 Commander 管理

背景信息

在运行EasyDeploy功能的网络中，将有配置设备加入Commander管理之后，Commander会学习到加入设备的基本信息，包括MAC地址、ESN号、IP地址、设备类型、设备型号、加载的系统软件等。

将有配置设备加入Commander管理之后，可以实现对有配置设备的故障替换、批量升级和批量配置功能。

前置任务

配置将有配置设备加入Commander管理之前，需完成以下任务：

- 确保有配置设备处于正常运行状态。
- 有配置设备与Commander之间路由可达。
- 如果需要从DHCP服务器获取信息，需确保有配置设备与DHCP服务器之间路由可达同时正确配置DHCP服务器。DHCP服务器配置与零配置部署中DHCP服务器配置相同，请参见“**3.8.2 配置DHCP**”。

  说明

  为了增强Commander和Client之间通信的安全性，防止有仿冒的Commander获取Client的控制权，可以分别在Commander和Client的系统视图下通过**easy-operation shared-key**命令配置相同的共享密钥。

操作步骤

步骤1 在Client上配置Commander的IP地址，可通过以下两种方式实现

- 命令行配置
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**easy-operation commander ip-address** *ip-address* [**udp-port** *udp-port*]，配置Commander的IP地址。
- 从DHCP服务器获取

  Client上使能DHCP客户端，配置设备从DHCP服务器获取设备IP地址。配置流程请参见《S300, S500, S2700, S5700, S6700 V200R022C00 配置指南-IP业务》DHCP配置 中的“开启DHCP Client功能”。

  只有设备配置了从DHCP服务器获取设备IP地址的功能，才会从DHCP服务器获取Commander的IP地址。Commander的IP地址通过DHCP服务器返回消息中携带的Option 148字段信息获取，因此需要在DHCP服务器上配置Option 148信息。

说明

- 由于设备是有配置的，如果配置文件中已经有上述配置，则无需再配置。
- 如果两种方式都可以获取到Commander的IP地址，则优先使用命令行配置；取消命令行配置后，使用DHCP服务器上的配置；如果通过DHCP服务器获取方式取得多个Commander的IP地址，则使用第一个能够正确解析的地址。

步骤2 在Commander上进行以下配置

- 手动配置
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**easy-operation**，进入Easy-Operation视图。
  c. 执行命令**client** [*client-id*] { **mac-address** *mac-address* | **esn** *esn* }，配置Client的匹配规则，即根据MAC地址或ESN号匹配Client。
- 自动加入
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**easy-operation**，进入Easy-Operation视图。
  c. 执行命令**client auto-join enable**，使能Client自动加入功能。

  使能此功能后，Commander会自动学习到Client的基本信息。

缺省情况下，未使能Client自动加入功能。

----结束

检查配置结果

- 执行命令**display easy-operation client** [*client-id* | **mac-address** *mac-address* | **esn** *esn* | **verbose**]，查看Commander上的Client信息库的信息。

3.14 维护 EasyDeploy

3.14.1 维护 Client 信息

背景信息

Commander上保存了Client的相关信息，包括Client信息、Group信息、全局信息等，Commander根据这些信息决定给Client加载哪些文件，同时Commander还根据这些信息实时跟踪各个Client的状态。

Commander支持管理的Client数量受规格限制，当Client的数量超过Commander的上限时，无法再增加新的Client信息。为了防止长时间处于丢失状态的Client占用信息库资源，可以配置老化丢失状态Client的功能，当老化时间超时之后，删除丢失状态Client。如果已经出现长时间处于丢失状态Client占用信息库资源的情况，可以清除丢失状态Client。

操作步骤

老化丢失状态的Client

1. 执行命令**system-view**，进入系统视图。
2. 执行命令**easy-operation**，进入Easy-Operation视图。
3. 执行命令**client aging-time** *aging-time*，配置老化丢失状态的Client功能，并指定老化时间。

   缺省情况下，未配置老化丢失状态的Client功能。
   - 自动加入的Client，老化时间超时之后，删除丢失状态Client。
   - 手动配置的Client，老化时间超时之后，Client不会被删除，状态变为未知。

清除丢失状态的Client

在用户视图下执行命令**reset easy-operation client-offline**，清除丢失状态的Client。

- 自动加入的Client，删除丢失状态Client。
- 手动配置的Client，Client不会被删除，状态变为未知。

清空Client信息库

须知

清空Client信息库会导致已配置的Client信息丢失，执行前请务必仔细确认。

在用户视图下执行命令**reset easy-operation client-database**，清空Client信息库。

清空Client信息库会同时删除手动配置的Client信息和自动学习的Client信息。如果此时Commander的自动加入功能是使能的，则Commander仍会自动学习到Client信息保存至Client信息库。

3.14.2 查看能耗信息

背景信息

用户可以在不同角色上查看不同设备的能耗数据，以便掌握整网的能耗状态。

操作步骤

步骤1 执行命令**display easy-operation power** [**client** *client-id* | **commander**]，查看Commander和Client的能耗信息。

在不同角色设备上命令功能有所不同：

- 在Commander上
  - 若不选择参数，则查看Commander和所有处于初始化状态、升级状态和正常运行状态的Client的能耗信息。
  - 若选择**client** *client-id*参数，则查看指定Client的能耗信息。
  - 若选择**commander**参数，则查看Commander的能耗信息。
- 在Client上

  不支持选择**client** *client-id*和**commander**参数，只用来查看当前Client的能耗信息。

----结束

3.15 EasyDeploy 配置举例

3.15.1 通过 Option 参数实现零配置设备部署示例

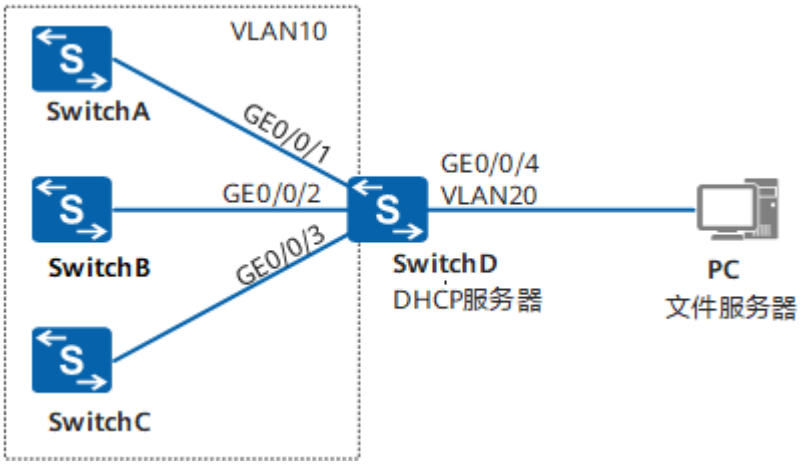
组网需求

如图3-17所示，在小区接入组网环境下的部署场景中，汇聚设备SwitchD连接着整个小区各个楼层的新出厂设备（如SwitchA、SwitchB和SwitchC）。

用户希望为小区内的各楼层的新设备加载相同的系统软件、补丁文件和配置文件；并且由于待配置的新设备较多，为了降低人工成本、节省部署的时间，用户希望各楼层设备能实现统一自动的配置。

实现零配置设备部署前，需要确保文件服务器、DHCP服务器与待配置设备（获取IP地址后）之间路由可达。

图 3-17 配置通过 Option 实现零配置部署组网图



配置思路

采用以下思路配置设备：

1. 用户PC与SwitchD直接相连，在PC上配置文件服务器。将需要加载的配置文件、系统软件和补丁文件放至文件服务器的工作目录下，保证SwitchA、SwitchB和SwitchC能够获取到需要加载的文件。
2. 在SwitchD上配置DHCP服务器，为SwitchA、SwitchB和SwitchC提供网络配置信息。由于待配置设备需加载相同的系统软件、补丁文件和配置文件，所以在配置DHCP服务器时，通过Option67和Option145提供需加载文件的信息。
3. SwitchA、SwitchB和SwitchC上电，实现通过EasyDeploy功能自动加载配置文件、系统软件和补丁文件。

操作步骤

步骤1 配置文件服务器

请根据文件服务器的操作指导进行配置。

配置完成后，将待配置设备需要加载的文件保存至文件服务器中。

步骤2 配置DHCP服务器

```
<HUAWEI> system-view
[HUAWEI] sysname DHCP_Server
[DHCP_Server] dhcp enable
[DHCP_Server] vlan batch 10 20
[DHCP_Server] interface gigabitethernet 0/0/1
[DHCP_Server-GigabitEthernet0/0/1] port link-type hybrid
[DHCP_Server-GigabitEthernet0/0/1] port hybrid pvid vlan 10
[DHCP_Server-GigabitEthernet0/0/1] port hybrid untagged vlan 10
[DHCP_Server-GigabitEthernet0/0/1] quit
[DHCP_Server] interface gigabitethernet 0/0/2
[DHCP_Server-GigabitEthernet0/0/2] port link-type hybrid
[DHCP_Server-GigabitEthernet0/0/2] port hybrid pvid vlan 10
[DHCP_Server-GigabitEthernet0/0/2] port hybrid untagged vlan 10
[DHCP_Server-GigabitEthernet0/0/2] quit
[DHCP_Server] interface gigabitethernet 0/0/3
[DHCP_Server-GigabitEthernet0/0/3] port link-type hybrid
[DHCP_Server-GigabitEthernet0/0/3] port hybrid pvid vlan 10
[DHCP_Server-GigabitEthernet0/0/3] port hybrid untagged vlan 10
```

```
[DHCP_Server-GigabitEthernet0/0/3] quit
[DHCP_Server] interface gigabitethernet 0/0/4
[DHCP_Server-GigabitEthernet0/0/4] port link-type hybrid
[DHCP_Server-GigabitEthernet0/0/4] port hybrid pvid vlan 20
[DHCP_Server-GigabitEthernet0/0/4] port hybrid untagged vlan 20
[DHCP_Server-GigabitEthernet0/0/4] quit
[DHCP_Server] interface vlanif 10
[DHCP_Server-Vlanif10] ip address 192.168.2.6 255.255.255.0
[DHCP_Server-Vlanif10] dhcp select global
[DHCP_Server-Vlanif10] quit
[DHCP_Server] interface vlanif 20
[DHCP_Server-Vlanif20] ip address 192.168.1.1 255.255.255.0
[DHCP_Server-Vlanif20] quit
[DHCP_Server] ip pool auto-config
[DHCP_Server-ip-pool-auto-config] network 192.168.2.0 mask 255.255.255.0
[DHCP_Server-ip-pool-auto-config] gateway-list 192.168.2.6
[DHCP_Server-ip-pool-auto-config] option 66 ascii sftp://user:YsHsjx_202206@192.168.1.16
[DHCP_Server-ip-pool-auto-config] option 67 ascii s_V200R022C00.cfg
[DHCP_Server-ip-pool-auto-config] option 145 ascii
vrpfile=s_V200R022C00.cc;vrpver=V200R022C00SPC200;patchfile=s_V200R022C00.pat;
[DHCP_Server-ip-pool-auto-config] quit
```

步骤3 待配置设备SwitchA、SwitchB和SwitchC上电启动，EasyDeploy流程开始运行

步骤4 验证配置结果

EasyDeploy流程结束后，登录到待配置设备执行命令**display startup**查看设备当前的启动系统软件，启动配置文件和启动补丁文件。以SwitchA为例：

```
<HUAWEI> display startup
MainBoard:
  Configured startup system software:        flash:/s_V200R022C00.cc
  Startup system software:                   flash:/s_V200R022C00.cc
  Next startup system software:              flash:/s_V200R022C00.cc
  Startup saved-configuration file:          flash:/s_V200R022C00.cfg
  Next startup saved-configuration file:     flash:/s_V200R022C00.cfg
  Startup paf file:                          NULL
  Next startup paf file:                     NULL
  Startup license file:                      NULL
  Next startup license file:                 NULL
  Startup patch package:                     flash:/s_V200R022C00.pat
  Next startup patch package:                flash:/s_V200R022C00.pat
```

----结束

配置文件

DHCP_Server的配置文件

```
#
sysname DHCP_Server
#
vlan batch 10 20
#
dhcp enable
#
ip pool auto-config
 gateway-list 192.168.2.6
 network 192.168.2.0 mask 255.255.255.0
 option 66 ascii sftp://user:YsHsjx_202206@192.168.1.16:10020
 option 67 ascii s_V200R022C00.cfg
 option 145 ascii vrpfile=s_V200R022C00.cc;vrpver=V200R022C00SPC200;patchfile=s_V200R022C00.pat;
#
interface Vlanif10
 ip address 192.168.2.6 255.255.255.0
 dhcp select global
#
interface Vlanif20
 ip address 192.168.1.1 255.255.255.0
```



```
#
interface GigabitEthernet0/0/1
 port link-type hybrid
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface GigabitEthernet0/0/2
 port link-type hybrid
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface GigabitEthernet0/0/3
 port link-type hybrid
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface GigabitEthernet0/0/4
 port link-type hybrid
 port hybrid pvid vlan 20
 port hybrid untagged vlan 20
#
return
```

3.15.2 通过中间文件实现零配置设备部署示例

组网需求

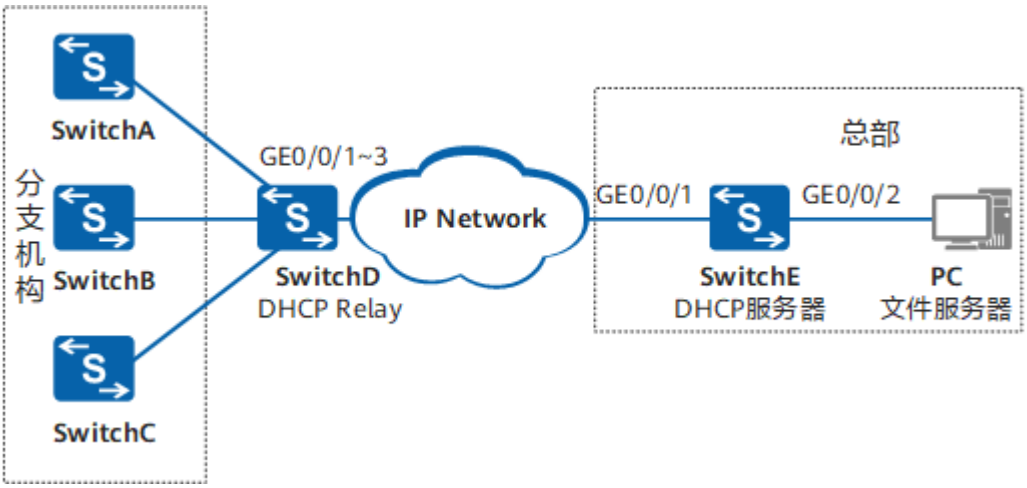
如图3-18所示，在某公司分支机构的部署场景中，新出厂设备SwitchA、SwitchB和SwitchC分别连接到设备SwitchD的GE0/0/1、GE0/0/2和GE0/0/3接口上。SwitchD作为分支机构出口的网关，跨越三层网络与总部相连。

SwitchA、SwitchB和SwitchC因为设备类型不同，所以需要加载不同的系统软件、补丁文件和配置文件。同时，为了降低现场配置的人力成本，用户希望能对这些设备实现远程自动的配置。

SwitchA、SwitchB和SwitchC的设备信息及待加载的文件信息如下：

- SwitchA：MAC地址为xxxx-xxxx-xxxx，需加载的系统软件名为s57li_easy_V200R022C00.cc，版本号信息为V200R022C00SPC100，补丁文件为s57li_easy_V200R022C00.pat，配置文件为s57li_easy_V200R022C00.cfg
- SwitchB：MAC地址为xxxx-xxxx-xxxx，需加载的系统软件名为s5720ei_easy_V200R022C00.cc，版本号信息为V200R022C00SPC100，补丁文件为s5720ei_easy_V200R022C00.pat，配置文件为s5720ei_easy_V200R022C00.cfg
- SwitchC：MAC地址为xxxx-xxxx-xxxx，需加载的系统软件名为s57li_easy_V200R022C00.cc，版本号信息为V200R022C00SPC100，补丁文件为s57li_easy_V200R022C00.pat，配置文件为s57li_easy_V200R022C00.cfg

图 3-18 配置通过中间文件实现零配置跨网段部署组网图



配置思路

采用以下思路配置设备：

1. 用户PC与SwitchE直接相连，在PC上配置文件服务器。
2. 编辑中间文件，实现待配置设备SwitchA、SwitchB和SwitchC通过中间文件获取配置文件、系统软件和补丁文件。
3. 将中间文件、系统软件、补丁文件和配置文件放至文件服务器的工作目录下，保证待配置设备能够获取到需要加载的文件。
4. 在分支机构网关设备SwitchD上配置DHCP中继；在位于总部的设备SwitchE上配置DHCP服务器。实现DHCP服务器跨网段为待配置设备提供网络配置信息。
5. SwitchA、SwitchB和SwitchC上电，实现自动加载配置文件、系统软件和补丁文件。

操作步骤

步骤1 编辑中间文件lswnet.cfg

新建一个文本文件，命名为“lswnet.cfg”。中间文件的内容与格式如下：

```
mac=xxxx-xxxx-
xxxx;vrpfile=s57li_easy_V200R022C00.cc;vrpver=V200R022C00SPC100;patchfile=s57li_easy_V200R022C00.pat;
cfgfile=s57li_easy_V200R022C00.cfg;
mac=xxxx-xxxx-
xxxx;vrpfile=s5720ei_easy_V200R022C00.cc;vrpver=V200R022C00SPC100;patchfile=s5720ei_easy_V200R022C
00.pat;cfgfile=s5720ei_easy_V200R022C00.cfg;
mac=xxxx-xxxx-
xxxx;vrpfile=s57li_easy_V200R022C00.cc;vrpver=V200R022C00SPC100;patchfile=s57li_easy_V200R022C00.pat;
cfgfile=s57li_easy_V200R022C00.cfg;
```

步骤2 配置文件服务器

请根据文件服务器的操作指导进行配置。

配置完成后，将中间文件、待配置设备需要加载的文件保存至文件服务器中。

步骤3 配置SwitchD

配置SwitchD的DHCP中继功能。

```
<HUAWEI> system-view
[HUAWEI] sysname DHCP_Relay
[DHCP_Relay] dhcp enable
[DHCP_Relay] vlan 10
[DHCP_Relay-vlan10] quit
[DHCP_Relay] interface gigabitethernet 0/0/1
[DHCP_Relay-GigabitEthernet0/0/1] port link-type hybrid
[DHCP_Relay-GigabitEthernet0/0/1] port hybrid pvid vlan 10
[DHCP_Relay-GigabitEthernet0/0/1] port hybrid untagged vlan 10
[DHCP_Relay-GigabitEthernet0/0/1] quit
[DHCP_Relay] interface gigabitethernet 0/0/2
[DHCP_Relay-GigabitEthernet0/0/2] port link-type hybrid
[DHCP_Relay-GigabitEthernet0/0/2] port hybrid pvid vlan 10
[DHCP_Relay-GigabitEthernet0/0/2] port hybrid untagged vlan 10
[DHCP_Relay-GigabitEthernet0/0/2] quit
[DHCP_Relay] interface gigabitethernet 0/0/3
[DHCP_Relay-GigabitEthernet0/0/3] port link-type hybrid
[DHCP_Relay-GigabitEthernet0/0/3] port hybrid pvid vlan 10
[DHCP_Relay-GigabitEthernet0/0/3] port hybrid untagged vlan 10
[DHCP_Relay-GigabitEthernet0/0/3] quit
[DHCP_Relay] interface vlanif 10
[DHCP_Relay-Vlanif10] ip address 192.168.1.6 255.255.255.0
[DHCP_Relay-Vlanif10] dhcp select relay
[DHCP_Relay-Vlanif10] dhcp relay server-ip 192.168.2.6
[DHCP_Relay-Vlanif10] quit
```

在SwitchD上配置一条静态路由：路由的目的地址为PC的IP地址，下一跳为与SwitchD直连的位于三层网络的设备接口的IP地址。

步骤4 配置SwitchE

配置SwitchE的DHCP服务器功能。

```
<HUAWEI> system-view
[HUAWEI] sysname DHCP_Server
[DHCP_Server] dhcp enable
[DHCP_Server] vlan batch 20 30
[DHCP_Server] interface gigabitethernet 0/0/1
[DHCP_Server-GigabitEthernet0/0/1] port link-type trunk
[DHCP_Server-GigabitEthernet0/0/1] port trunk allow-pass vlan 20
[DHCP_Server-GigabitEthernet0/0/1] quit
[DHCP_Server] interface gigabitethernet 0/0/2
[DHCP_Server-GigabitEthernet0/0/2] port link-type hybrid
[DHCP_Server-GigabitEthernet0/0/2] port hybrid pvid vlan 30
[DHCP_Server-GigabitEthernet0/0/2] port hybrid untagged vlan 30
[DHCP_Server-GigabitEthernet0/0/2] quit
[DHCP_Server] interface vlanif 20
[DHCP_Server-Vlanif20] ip address 192.168.2.6 255.255.255.0
[DHCP_Server-Vlanif20] dhcp select global
[DHCP_Server-Vlanif20] quit
[DHCP_Server] interface vlanif 30
[DHCP_Server-Vlanif30] ip address 192.168.4.1 255.255.255.0
[DHCP_Server-Vlanif30] quit
[DHCP_Server] ip pool easy-operation
[DHCP_Server-ip-pool-easy-operation] network 192.168.1.0 mask 255.255.255.0
[DHCP_Server-ip-pool-easy-operation] gateway-list 192.168.1.6
[DHCP_Server-ip-pool-auto-config] option 66 ascii sftp://user:YsHsjx_202206@192.168.1.16:10020
[DHCP_Server-ip-pool-easy-operation] option 146 ascii opervalue=1;delaytime=0;netfile=lswnet.cfg;
[DHCP_Server-ip-pool-easy-operation] quit
```

在SwitchE上配置一条静态路由：路由的目的地址为IP地址池网段，下一跳为与SwitchE直连的位于三层网络的设备接口的IP地址。

步骤5 待配置设备SwitchA、SwitchB和SwitchC上电启动，EasyDeploy流程开始运行

步骤6 验证配置结果

EasyDeploy流程结束后，登录到待配置设备执行命令**display startup**查看设备当前的启动系统软件，启动配置文件和启动补丁文件。以SwitchB为例：

```
<HUAWEI> display startup
MainBoard:
  Configured startup system software:        flash:/s5720ei_easy_V200R022C00.cc
  Startup system software:                   flash:/s5720ei_easy_V200R022C00.cc
  Next startup system software:              flash:/s5720ei_easy_V200R022C00.cc
  Startup saved-configuration file:          flash:/s5720ei_easy_V200R022C00.cfg
  Next startup saved-configuration file:     flash:/s5720ei_easy_V200R022C00.cfg
  Startup paf file:                          NULL
  Next startup paf file:                     NULL
  Startup license file:                      NULL
  Next startup license file:                 NULL
  Startup patch package:                     flash:/s5720ei_easy_V200R022C00.pat
  Next startup patch package:                flash:/s5720ei_easy_V200R022C00.pat
```

----结束

配置文件

- DHCP_Relay的配置文件

```
#
sysname DHCP_Relay
#
vlan batch 10
#
dhcp enable
#
interface Vlanif10
 ip address 192.168.1.6 255.255.255.0
 dhcp select relay
 dhcp relay server-ip 192.168.2.6
#
interface GigabitEthernet0/0/1
 port link-type hybrid
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface GigabitEthernet0/0/2
 port link-type hybrid
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface GigabitEthernet0/0/3
 port link-type hybrid
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
return
```

- DHCP_Server的配置文件

```
#
sysname DHCP_Server
#
vlan batch 20 30
#
dhcp enable
#
ip pool easy-operation
 gateway-list 192.168.1.6
 network 192.168.1.0 mask 255.255.255.0
 option 66 ascii sftp://user:YsHsjx_202206@192.168.1.16:10020
 option 146 ascii opervalue=1;delaytime=0;netfile=lswnet.cfg;
#
interface Vlanif20
 ip address 192.168.2.6 255.255.255.0
 dhcp select global
#
```



```
interface Vlanif30
 ip address 192.168.4.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 20
#
interface GigabitEthernet0/0/2
 port link-type hybrid
 port hybrid pvid vlan 30
 port hybrid untagged vlan 30
#
return
```

3.15.3 通过 Commander 实现零配置设备部署（不使能网络拓扑收集功能）示例

组网需求

如图3-19所示，在某企业网络中，文件服务器和DHCP服务器与SwitchA之间路由可达。现在需要将企业新建楼宇中的设备Client1、Client2、Client3加入到网络中。新加入的Client与DHCP服务器不在同一网段。为了降低人工成本、节省部署的时间，用户希望为新部署的设备实现统一自动的配置和后续的维护功能。

其中SwitchA上接口VLANIF20的地址为192.168.4.2/24，对端地址为192.168.4.1/24。

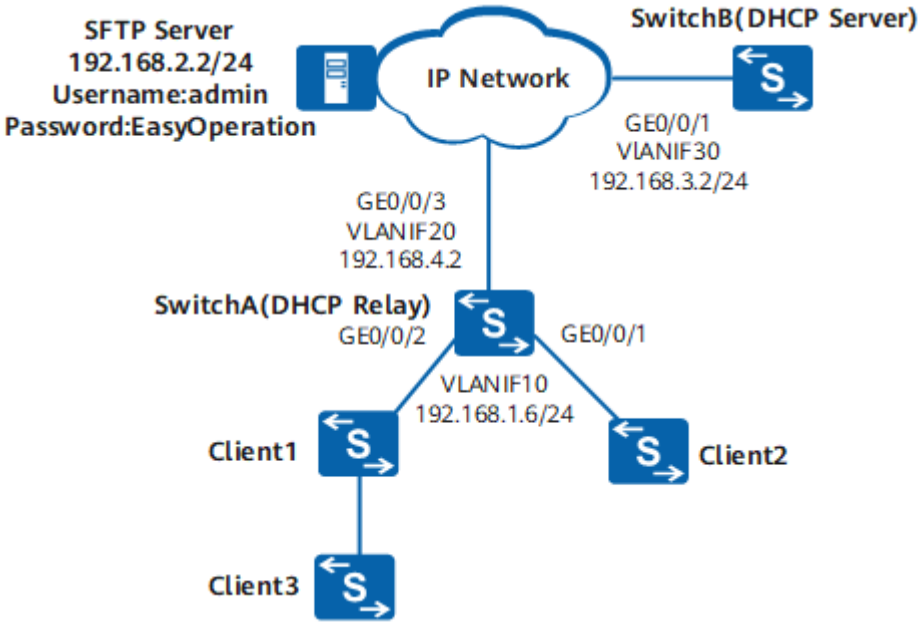
SwitchB上接口VLANIF30的地址为192.168.3.2/24，对端地址为192.168.3.1/24。

新加入的设备情况如表3-6所示。

表 3-6 设备情况说明

新加入的设备	设备型号	需要加载的文件
Client1	S5700-HI	s5700-hi.cfg 自定义文件header1.txt
Client2	S5700-HI	s5700-hi.cfg 自定义文件header1.txt
Client3	S5700-X-LIS5736-S	s5700-hi.cfg 自定义文件header2.txt

图 3-19 通过 Commander 实现零配置设备部署组网图



配置思路

采用以下思路进行配置：

1. 配置文件服务器，将Client需要加载的文件保存至文件服务器。
2. 在SwitchB上配置基于全局地址池的DHCP服务器，在SwitchA上配置DHCP中继功能，实现新加入的Client自动获取IP地址及Commander的IP地址。
3. 在SwitchA上配置Commander功能，以实现通过Commander进行零配置部署。
   - 为了后期的维护，需要在Commander上配置自动备份配置文件功能，便于后续进行故障替换。
   - Client1和Client2由于是同类型设备且需要加载配置文件相同，所以可以配置内置Group。Client3与Client1、Client2加载的配置文件不同，所以可以直接指定此Client的下载信息。
   - 由于Client3与Client1是串联组网，所以需要在Commander全局下配置延时时间，以确保Client3能够下载文件成功。

操作步骤

步骤1 配置文件服务器

请根据文件服务器的操作指导进行配置。

配置完成后，将Client需要加载的文件保存至文件服务器。

步骤2 配置DHCP

在SwitchB上配置基于全局地址池的DHCP服务器。

```
<HUAWEI> system-view
[HUAWEI] sysname SwitchB
[SwitchB] dhcp enable
```

```
[SwitchB] vlan batch 30
[SwitchB] interface vlanif 30
[SwitchB-Vlanif30] ip address 192.168.3.2 24
[SwitchB-Vlanif30] dhcp select global
[SwitchB-Vlanif30] quit
[SwitchB] interface gigabitethernet 0/0/1
[SwitchB-GigabitEthernet0/0/1] port link-type hybrid
[SwitchB-GigabitEthernet0/0/1] port hybrid pvid vlan 30
[SwitchB-GigabitEthernet0/0/1] port hybrid untagged vlan 30
[SwitchB-GigabitEthernet0/0/1] quit
[SwitchB] ip pool easy-operation
[SwitchB-ip-pool-easy-operation] network 192.168.1.0 mask 255.255.255.0
[SwitchB-ip-pool-easy-operation] gateway-list 192.168.1.6
[SwitchB-ip-pool-easy-operation] option 148 ascii ipaddr=192.168.1.6;
[SwitchB-ip-pool-easy-operation] quit
```

在SwitchB上配置缺省路由。

```
[SwitchB] ip route-static 0.0.0.0 0.0.0.0 192.168.3.1
```

在SwitchA（Commander）上配置DHCP中继。

```
<HUAWEI> system-view
[HUAWEI] sysname SwitchA
[SwitchA] vlan batch 10 20
[SwitchA] dhcp enable
[SwitchA] interface vlanif 10
[SwitchA-Vlanif10] ip address 192.168.1.6 24
[SwitchA-Vlanif10] quit
[SwitchA] interface vlanif 20
[SwitchA-Vlanif20] ip address 192.168.4.2 24
[SwitchA-Vlanif20] quit
[SwitchA] interface gigabitethernet 0/0/1
[SwitchA-GigabitEthernet0/0/1] port link-type hybrid
[SwitchA-GigabitEthernet0/0/1] port hybrid pvid vlan 10
[SwitchA-GigabitEthernet0/0/1] port hybrid untagged vlan 10
[SwitchA-GigabitEthernet0/0/1] quit
[SwitchA] interface gigabitethernet 0/0/2
[SwitchA-GigabitEthernet0/0/2] port link-type hybrid
[SwitchA-GigabitEthernet0/0/2] port hybrid pvid vlan 10
[SwitchA-GigabitEthernet0/0/2] port hybrid untagged vlan 10
[SwitchA-GigabitEthernet0/0/2] quit
[SwitchA] interface gigabitethernet 0/0/3
[SwitchA-GigabitEthernet0/0/3] port link-type hybrid
[SwitchA-GigabitEthernet0/0/3] port hybrid pvid vlan 20
[SwitchA-GigabitEthernet0/0/3] port hybrid untagged vlan 20
[SwitchA-GigabitEthernet0/0/3] quit
[SwitchA] interface vlanif 10
[SwitchA-Vlanif10] dhcp select relay
[SwitchA-Vlanif10] dhcp relay server-ip 192.168.3.2
[SwitchA-Vlanif10] quit
```

在SwitchA上配置缺省路由。

```
[SwitchA] ip route-static 0.0.0.0 0.0.0.0 192.168.4.1
```

步骤3 配置Commander的基本功能

```
[SwitchA] easy-operation commander ip-address 192.168.1.6
Warning: The pre-shared key can be modified to improve security. Continue? [Y/N]:y
Enter the pre-shared key:******
Confirm the pre-shared key:******
[SwitchA] easy-operation commander enable
```

步骤4 配置文件服务器信息

```
[SwitchA] easy-operation
[SwitchA-easyoperation] sftp-server 192.168.2.2 username admin password EasyOperation
[SwitchA-easyoperation] backup configuration interval 2
```

步骤5 配置下载文件信息

为Client1和Client2配置根据设备类型匹配的内置Group，并指定需要加载的文件信息。

```
[SwitchA-easyoperation] group build-in S5700-HIS5736-S
[SwitchA-easyoperation-group-build-in-S5700-HIs5736-s] configuration-file s5700-his5736-s.cfg
[SwitchA-easyoperation-group-build-in-S5700-HIs5736-s] custom-file header1.txt
[SwitchA-easyoperation-group-build-in-S5700-HIs5736-s] quit
[SwitchA-easyoperation] client auto-join enable
Warning: The commander will create the client information in database automatica
lly when received message from unknown client. Continue? [Y/N]: y
[SwitchA-easyoperation]
```

为Client3指定下载文件信息。

```
[SwitchA-easyoperation] client 3 mac-address xxxx-xxxx-xxxx
[SwitchA-easyoperation] client 3 configuration-file s5700-hi.cfg custom-file header2.txt
```

在全局Commander下配置延时激活时间。根据Client3下载文件的大小，将延时时间配置为15分钟（900秒）。

```
[SwitchA-easyoperation] activate-file delay 900
[SwitchA-easyoperation] quit
```

步骤6 检查配置结果

查看Commander上的全局配置信息。

```
[SwitchA] display easy-operation configuration
------------------------------------------------------------------------------
 Role                          : Commander
 Commander IP address          : 192.168.1.6
 Commander UDP port            : 60000
 IP address of file server     : 192.168.2.2
 Type of file server           : SFTP
 Username of file server       : admin
 Default system-software file  : -
 Default system-software version : -
 Default configuration file    : -
 Default patch file            : -
 Default WEB file              : -
 Default license file          : -
 Default custom file 1         : -
 Default custom file 2         : -
 Default custom file 3         : -
 Auto clear up                 : Disable
 Auto join in                  : Disable
 Topology collection           : Disable
 Activating file time          : Delay 900s
 Activating file method        : Default
 Aging time of lost client(hours): -
 Backup configuration file mode  : Default
 Backup configuration file interval(hours): 2
------------------------------------------------------------------------------
```

零配置部署流程开始后，查看各Client的下载状态。

```
[SwitchA] display easy-operation download-status
The total number of client in downloading files is :
3
------------------------------------------------------------------------------
  ID    Mac address    IP address      Method      Phase        Status
------------------------------------------------------------------------------
  1     xxxx-xxxx-xxxx 192.168.1.254   Zero-touch  Config-file  Upgrading
  2     xxxx-xxxx-xxxx 192.168.1.253   Zero-touch  Config-file  Upgrading
  3     xxxx-xxxx-xxxx 192.168.1.252   Zero-touch  Config-file  Upgrading
```

----结束

配置文件

SwitchA的配置文件

```
#
sysname SwitchA
#
vlan batch 10 20
#
dhcp enable
#
interface Vlanif10
 ip address 192.168.1.6 255.255.255.0
 dhcp select relay
 dhcp relay server-ip 192.168.3.2
#
interface Vlanif20
 ip address 192.168.4.2 255.255.255.0
#
interface GigabitEthernet0/0/1
 port link-type hybrid
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface GigabitEthernet0/0/2
 port link-type hybrid
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface GigabitEthernet0/0/3
 port link-type hybrid
 port hybrid pvid vlan 20
 port hybrid untagged vlan 20
#
ip route-static 0.0.0.0 0.0.0.0 192.168.4.1
#
easy-operation commander ip-address 192.168.1.6
easy-operation commander enable
#
easy-operation
 sftp-server 192.168.2.2 username admin password %^%#=.X8C_TN##%&9P>3RK503O@w-=Fr
%>naT#E3P4{0%^%#
 backup configuration interval 2
 activate-file delay 900
 client 3 mac-address xxxx-xxxx-xxxx
 client 3 configuration-file s5700-x-li.cfg
 client 3 custom-file header2.txt
 group build-in S5700-HI
  configuration-file s5700-hi.cfg
  custom-file header1.txt
#
return
```

SwitchB的配置文件

```
#
sysname SwitchB
#
vlan batch 30
#
dhcp enable
#
ip pool easy-operation
 gateway-list 192.168.1.6
 network 192.168.1.0 mask 255.255.255.0
 option 148 ascii ipaddr=192.168.1.6;
#
interface Vlanif30
 ip address 192.168.3.2 255.255.255.0
```



```
 dhcp select global
#
interface GigabitEthernet0/0/1
 port link-type hybrid
 port hybrid pvid vlan 30
 port hybrid untagged vlan 30
#
ip route-static 0.0.0.0 0.0.0.0 192.168.3.1
#
return
```

3.15.4 通过 Commander 实现零配置设备部署（使能网络拓扑收集功能）示例

组网需求

如图3-20所示，在某企业网络中，文件服务器和DHCP服务器与SwitchA之间路由可达。现在需要将企业新建楼宇中的设备SwitchC、SwitchD、SwitchE加入到网络中。新加入的Switch与DHCP服务器不在同一网段。为了降低人工成本、节省部署的时间，用户希望为新部署的设备实现统一自动的配置和后续的维护功能。由于设备安装工程师未上报Client对应的MAC地址和ESN号，所以配置网络拓扑收集功能。

其中SwitchA上接口VLANIF20的地址为192.168.4.2/24，对端地址为192.168.4.1/24。

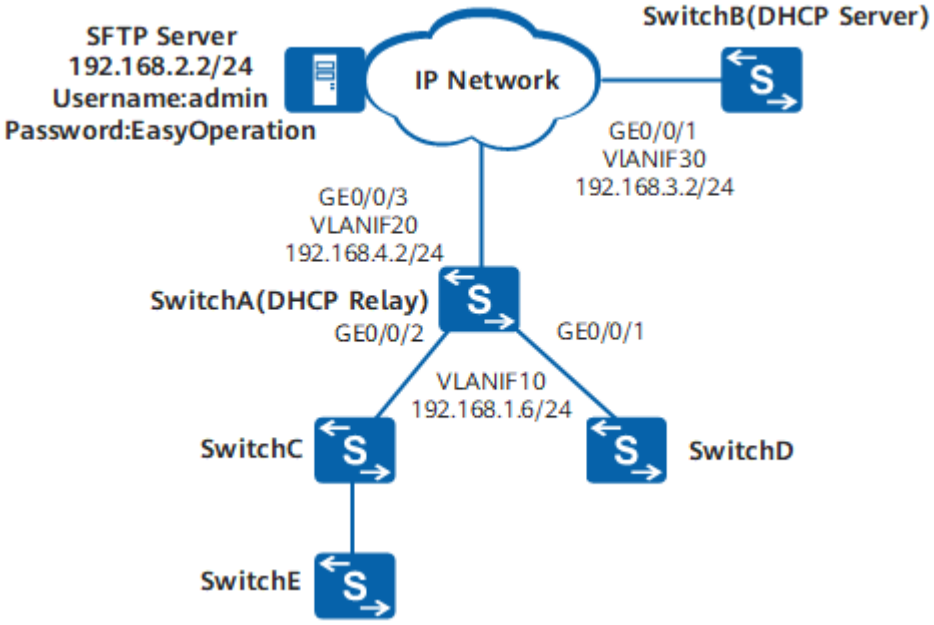
SwitchB上接口VLANIF30的地址为192.168.3.2/24，对端地址为192.168.3.1/24。

新加入的设备情况如表3-7所示。

表 3-7 设备情况说明

新加入的设备	设备型号	需要加载的文件
SwitchC	S5700-HI	s5700-hi.cfg 自定义文件header1.txt
SwitchD	S5700-HI	s5700-hi.cfg 自定义文件header1.txt
SwitchE	S5700-X-LI	s5700-x-li.cfg 自定义文件header2.txt

图 3-20 通过 Commander 实现零配置设备部署组网图



配置思路

采用以下思路进行配置：

1. 配置文件服务器，将Client需要加载的文件保存至文件服务器。
2. SwitchB上配置基于全局地址池的DHCP服务器和Commander的IP地址，在SwitchA上配置DHCP中继功能，实现新加入的Client自动获取IP地址及Commander的IP地址。
3. 在SwitchA上配置Commander功能，以实现通过Commander进行零配置部署。
   - 为了后期的维护，需要在Commander上配置自动备份配置文件功能，便于后续进行故障替换。
   - 根据网络拓扑，配置Client的下载文件信息。
   - 由于SwitchE与SwitchC是串联组网，所以需要在Commander全局下配置延时时间，以确保SwitchE能够下载文件成功。

操作步骤

步骤1 配置文件服务器

请根据文件服务器的操作指导进行配置。

配置完成后，将Client需要加载的文件保存至文件服务器。

步骤2 配置DHCP

在SwitchB上配置基于全局地址池的DHCP服务器。

```
<HUAWEI> system-view
[HUAWEI] sysname SwitchB
[SwitchB] dhcp enable
[SwitchB] vlan batch 30
```

```
[SwitchB] interface vlanif 30
[SwitchB-Vlanif30] ip address 192.168.3.2 24
[SwitchB-Vlanif30] dhcp select global
[SwitchB-Vlanif30] quit
[SwitchB] interface gigabitethernet 0/0/1
[SwitchB-GigabitEthernet0/0/1] port link-type hybrid
[SwitchB-GigabitEthernet0/0/1] port hybrid pvid vlan 30
[SwitchB-GigabitEthernet0/0/1] port hybrid untagged vlan 30
[SwitchB-GigabitEthernet0/0/1] quit
[SwitchB] ip pool easy-operation
[SwitchB-ip-pool-easy-operation] network 192.168.1.0 mask 255.255.255.0
[SwitchB-ip-pool-easy-operation] gateway-list 192.168.1.6
[SwitchB-ip-pool-easy-operation] option 148 ascii ipaddr=192.168.1.6;
[SwitchB-ip-pool-easy-operation] quit
```

在SwitchB上配置缺省路由。

```
[SwitchB] ip route-static 0.0.0.0 0.0.0.0 192.168.3.1
```

在SwitchA（Commander）上配置DHCP中继。

```
<HUAWEI> system-view
[HUAWEI] sysname SwitchA
[SwitchA] vlan batch 10 20
[SwitchA] dhcp enable
[SwitchA] interface vlanif 10
[SwitchA-Vlanif10] ip address 192.168.1.6 24
[SwitchA-Vlanif10] quit
[SwitchA] interface vlanif 20
[SwitchA-Vlanif20] ip address 192.168.4.2 24
[SwitchA-Vlanif20] quit
[SwitchA] interface gigabitethernet 0/0/1
[SwitchA-GigabitEthernet0/0/1] port link-type hybrid
[SwitchA-GigabitEthernet0/0/1] port hybrid pvid vlan 10
[SwitchA-GigabitEthernet0/0/1] port hybrid untagged vlan 10
[SwitchA-GigabitEthernet0/0/1] quit
[SwitchA] interface gigabitethernet 0/0/2
[SwitchA-GigabitEthernet0/0/2] port link-type hybrid
[SwitchA-GigabitEthernet0/0/2] port hybrid pvid vlan 10
[SwitchA-GigabitEthernet0/0/2] port hybrid untagged vlan 10
[SwitchA-GigabitEthernet0/0/2] quit
[SwitchA] interface gigabitethernet 0/0/3
[SwitchA-GigabitEthernet0/0/3] port link-type hybrid
[SwitchA-GigabitEthernet0/0/3] port hybrid pvid vlan 20
[SwitchA-GigabitEthernet0/0/3] port hybrid untagged vlan 20
[SwitchA-GigabitEthernet0/0/3] quit
[SwitchA] interface vlanif 10
[SwitchA-Vlanif10] dhcp select relay
[SwitchA-Vlanif10] dhcp relay server-ip 192.168.3.2
[SwitchA-Vlanif10] quit
```

在SwitchA上配置缺省路由。

```
[SwitchA] ip route-static 0.0.0.0 0.0.0.0 192.168.4.1
```

步骤3 配置Commander的基本功能

```
[SwitchA] easy-operation commander ip-address 192.168.1.6
Warning: The pre-shared key can be modified to improve security. Continue? [Y/N]:y
Enter the pre-shared key:******
Confirm the pre-shared key:******
[SwitchA] easy-operation commander enable
```

步骤4 配置文件服务器信息

```
[SwitchA] easy-operation
[SwitchA-easyoperation] sftp-server 192.168.2.2 username admin password EasyOperation
[SwitchA-easyoperation] quit
```

步骤5 配置网络拓扑收集功能

```
[SwitchA] ndp enable
[SwitchA] ntdp enable
[SwitchA] ntdp timer 5
[SwitchA] easy-operation
[SwitchA-easyoperation] topology enable
[SwitchA-easyoperation] client auto-join enable
[SwitchA-easyoperation] quit
```

步骤6 配置集群和集群管理VLAN

```
[SwitchA] cluster enable
[SwitchA] cluster
[SwitchA-cluster] mngvlanid 10
[SwitchA-cluster] quit
```

步骤7 配置下载文件信息

查看Commander收集到的网络拓扑信息。

```
[SwitchA] display easy-operation topology
<-->:normal device          <??>:lost device
Total topology node number: 3
------------------------------------------------------------------------------
[SwitchA: 00E0-FC8F-0447](Commander)
|-(GE0/0/1)<-->(GE0/0/1)[HUAWEI: 00E0-FC34-3190](Client 1)
|-(GE0/0/2)<-->(GE0/0/1)[HUAWEI: 00E0-FC12-A34B](Client 2)
| |-(GE0/0/2)<-->(GE0/0/1)[HUAWEI: 00E0-FC75-EDFF] (Client 3)
```

根据网络规划和网络拓扑信息，知道**Client1**对应**SwitchD**，**Client2**对应**SwitchC**，**Client3**对应**SwitchE**。

为Client1指定下载文件信息。

```
[SwitchA] easy-operation
[SwitchA-easyoperation] client 1 configuration-file s5700-hi.cfg custom-file header1.txt
```

为Client2指定下载文件信息。

```
[SwitchA-easyoperation] client 2 configuration-file s5700-hi.cfg custom-file header1.txt
```

为Client3指定下载文件信息。

```
[SwitchA-easyoperation] client 3 configuration-file s5700-x-li.cfg custom-file header2.txt
```

在全局Commander下配置延时激活时间。根据Client3下载文件的大小，将延时时间配置为15分钟（900秒）。

```
[SwitchA-easyoperation] activate-file delay 900
```

步骤8 配置自动备份配置文件

```
[SwitchA-easyoperation] backup configuration interval 2
[SwitchA-easyoperation] quit
```

步骤9 检查配置结果

查看Commander上的全局配置信息。

```
[SwitchA] display easy-operation configuration
------------------------------------------------------------------------------
 Role                          : Commander
 Commander IP address          : 192.168.1.6
 Commander UDP port            : 60000
 IP address of file server     : 192.168.2.2
 Type of file server           : SFTP
 Username of file server       : admin
 Default system-software file  : -
 Default system-software version : -
 Default configuration file    : -
 Default patch file            : -
```



```
 Default WEB file               : -
 Default license file           : -
 Default custom file 1          : -
 Default custom file 2          : -
 Default custom file 3          : -
 Auto clear up                  : Disable
 Auto join in                   : Enable
 Topology collection            : Enable
 Activating file time           : Delay 900s
 Activating file method         : Default
 Aging time of lost client(hours): -
 Backup configuration file mode  : Default
 Backup configuration file interval(hours): 2
------------------------------------------------------------------------------
```

零配置部署流程开始后，查看各Client的下载状态。

```
[SwitchA] display easy-operation download-status
The total number of client in downloading files is : 3

------------------------------------------------------------------------------
  ID    Mac address    IP address      Method      Phase         Status
------------------------------------------------------------------------------
  1     00E0-FC12-A34B 192.168.1.254   Zero-touch  Config-file  Upgrading
  2     00E0-FC34-3190 192.168.1.253   Zero-touch  Config-file  Upgrading
  3     00E0-FC34-EDFF 192.168.1.252   Zero-touch  Config-file  Upgrading
```

----结束

配置文件

SwitchA的配置文件

```
#
sysname SwitchA
#
vlan batch 10 20
#
cluster enable
#
ntdp timer 5
#
dhcp enable
#
interface Vlanif10
 ip address 192.168.1.6 255.255.255.0
 dhcp select relay
 dhcp relay server-ip 192.168.3.2
#
interface Vlanif20
 ip address 192.168.4.2 255.255.255.0
#
interface GigabitEthernet0/0/1
 port link-type hybrid
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface GigabitEthernet0/0/2
 port link-type hybrid
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface GigabitEthernet0/0/3
 port link-type hybrid
 port hybrid pvid vlan 20
 port hybrid untagged vlan 20
#
cluster
 mngvlanid 10
```



```
#
ip route-static 0.0.0.0 0.0.0.0 192.168.4.1
#
easy-operation commander ip-address 192.168.1.6
easy-operation commander enable
#
easy-operation
 client auto-join enable
 topology enable
 sftp-server 192.168.2.2 username admin password %^%#=.X8C_TN##%&9P>3RK503O@w-=Fr
%>naT#E3P4{0%^%#
 backup configuration interval 2
 activate-file delay 900
 client 1 configuration-file s5700-hi.cfg
 client 1 custom-file header1.txt
 client 2 configuration-file s5700-hi.cfg
 client 2 custom-file header1.txt
 client 3 configuration-file s5700-x-li.cfg
 client 3 custom-file header2.txt
#
return
```

SwitchB的配置文件

```
#
sysname SwitchB
#
vlan batch 30
#
dhcp enable
#
ip pool easy-operation
 gateway-list 192.168.1.6
 network 192.168.1.0 mask 255.255.255.0
 option 148 ascii ipaddr=192.168.1.6;
#
interface Vlanif30
 ip address 192.168.3.2 255.255.255.0
 dhcp select global
#
interface GigabitEthernet0/0/1
 port link-type hybrid
 port hybrid pvid vlan 30
 port hybrid untagged vlan 30
#
ip route-static 0.0.0.0 0.0.0.0 192.168.3.1
#
return
```

3.15.5 通过 Commander 实现手动替换故障设备示例

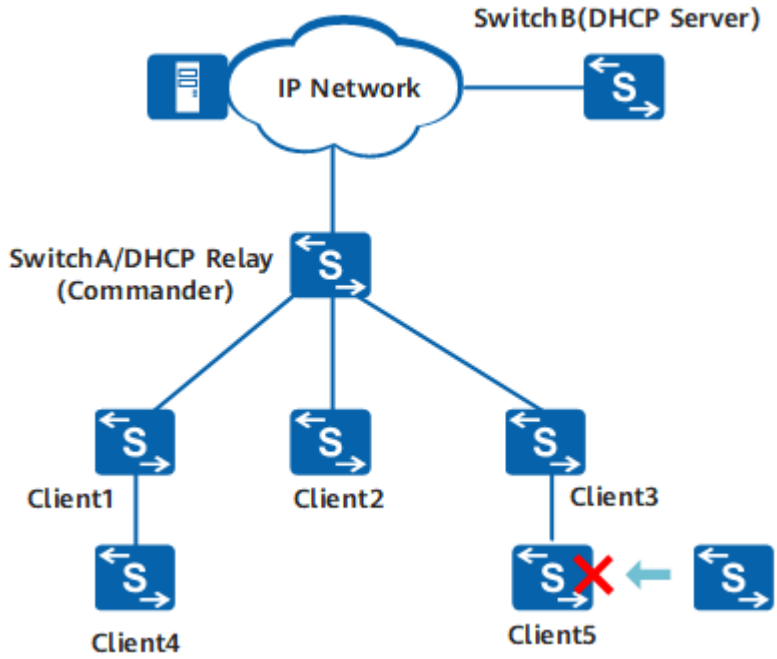
组网需求

如图3-21所示，在运行EasyDeploy功能的某企业网络中，SwitchA为Commander及DHCP中继，DHCP服务器和文件服务器与SwitchA之间路由可达。

现在网络中有一台设备Client5故障导致其下行业务中断。此时需要用新设备来替换Client5，并快速实现原来Client5的业务功能，将故障影响降至最小。

新Client的MAC地址是00e0-fc12-3456，在替换过程中还需要下载web_1.web.7z的网页文件。

图 3-21 通过 Commander 实现手动替换故障设备组网图



配置思路

采用以下思路配置设备：

1. 将web_1.web.7z文件保存至文件服务器。
2. 在SwitchA上配置故障替换信息，使得新Client能够获取到原故障Client的备份配置文件。

说明

故障替换功能的实现基于已部署EasyDeploy功能的网络，进行故障替换配置前已完成文件服务器、DHCP以及Commander的配置部署。

操作步骤

步骤1 使用故障替换功能，应提前配置自动备份配置文件的功能，以确保新Client能获取到原故障设备的配置文件

```
<HUAWEI> system-view
[HUAWEI] sysname SwitchA
[SwitchA] easy-operation
[SwitchA-easyoperation] backup configuration interval 72
```

步骤2 在SwitchA上配置故障替换信息

```
[SwitchA-easyoperation] client 5 replace mac-address 00e0-fc12-3456
[SwitchA-easyoperation] client 5 replace web-file web_1.web.7z
```

步骤3 检查配置结果

查看Client替换信息库的信息。

```
[SwitchA-easyoperation] display easy-operation client replace
The total number of replacement information is : 1
```

```
-------------------------------------------------------------
 ID      Replaced Mac       Replaced Esn
-------------------------------------------------------------
 5       00e0-fc12-3456   -
-------------------------------------------------------------
```

在故障设备替换流程开始后，可以执行命令**display easy-operation client 5**查看新Client的状态。

```
[SwitchA-easyoperation] display easy-operation client 5
-------------------------------------------------------------------------------
 Client ID                   : 5
 Host name                     : HUAWEI
 Mac address                   : 00e0-fc12-3456
 ESN                         : 210235182810xxxxxxxx
 IP address                    : 192.168.1.254
 Model                       : S5701-28X-LI-AC
 Device Type                   : S5700-X-LI
 System-software file          : flash:/S5700XLI.cc
 System-software version       : V200R005C00
 Configuration file            : -
 Patch file                  : -
 WEB file                    : -
 License file                : -
 System CPU usage              : 55%
 System Memory usage           : 44%
 Backup configuration file     : vrpcfg.zip
 Backup result               : Successful
 Last operation result         : -
 Last operation time           : 0000-00-00  00:00:00
 State                       : UPGRADING
 Aging time left (hours)       : -
-------------------------------------------------------------------------------
```

还可以执行命令**display easy-operation download-status**查看新Client的下载状态。

```
[SwitchA-easyoperation] display easy-operation download-status
The total number of client in downloading files is : 1

-------------------------------------------------------------------------------
 ID  Mac address      IP address          Method       Phase       Status
-------------------------------------------------------------------------------
 5   00e0-fc12-3456   192.168.1.254       Zero-touch   Web-file    Upgrading
```

----结束

配置文件

SwitchA的配置文件

```
#
sysname SwitchA
#
vlan batch 10 20
#
dhcp enable
#
interface Vlanif10
 ip address 192.168.1.6 255.255.255.0
 dhcp select relay
 dhcp relay server-ip 192.168.3.2
#
interface Vlanif20
 ip address 192.168.4.2 255.255.255.0
#
interface GigabitEthernet0/0/1
 port link-type hybrid
```



```
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface GigabitEthernet0/0/2
 port link-type hybrid
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface GigabitEthernet0/0/3
 port link-type hybrid
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface GigabitEthernet0/0/4
 port link-type hybrid
 port hybrid pvid vlan 20
 port hybrid untagged vlan 20
#
ip route-static 0.0.0.0 0.0.0.0 192.168.4.1
#
easy-operation commander ip-address 192.168.1.6
easy-operation commander enable
#
easy-operation
 sftp-server 192.168.2.2 username admin password %^%#=.X8C_TN##%&9P>3RK503O@w-=Fr
%>naT#E3P4{0%^%#
 backup configuration interval 72
 client 5 mac-address 00e0-fc12-3456
#
return
```

SwitchB的配置文件

```
#
sysname SwitchB
#
vlan batch 30
#
dhcp enable
#
ip pool easy-operation
 gateway-list 192.168.1.6
 network 192.168.1.0 mask 255.255.255.0
 option 148 ascii ipaddr=192.168.1.6;
#
interface Vlanif30
 ip address 192.168.3.2 255.255.255.0
 dhcp select global
#
interface GigabitEthernet0/0/1
 port link-type hybrid
 port hybrid pvid vlan 30
 port hybrid untagged vlan 30
#
ip route-static 0.0.0.0 0.0.0.0 192.168.3.1
#
return
```

3.15.6 通过 Commander 实现批量升级设备示例

组网需求

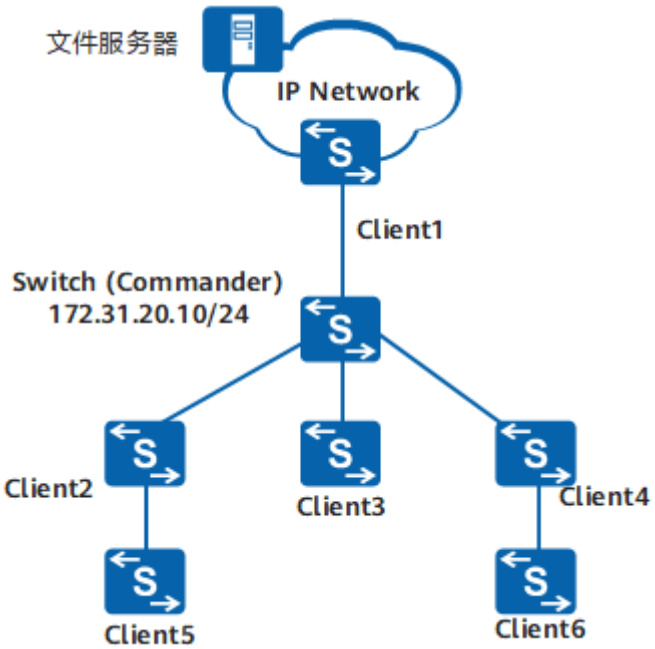
如图3-22所示，在企业网络中，Client1～Client6是某企业内部各楼宇中的设备，与Switch及文件服务器间的路由可达，Switch的IP地址是172.31.20.10/24，文件服务器的IP地址是172.31.1.90。为了降低人工成本也便于后续的升级维护操作，用户希望各个Client能够自动获取所需要文件，实现批量升级。

Client1～Client6的设备信息及需要加载的文件，如表3-8所示。

表 3-8 Client1～Client6 的设备信息及需要加载的文件

Client	设备类型	MAC地址	IP地址	需要加载的文件
Client1	S7700	-	172.31.20.100/24	s7700.cc license.dat header1.txt
Client2	S5700-HI	-	-	s5700-hi.cc
Client3	S5700-HI	-	-	s5700-hi.cc
Client4	S5700-X-LI	-	172.31.10.10/24	s5700-x-li.cc
Client5	S5700-HI	-	-	s5700-hi.cc
Client6	S5700-SI	xxxx-xxxx-xxxx	-	web_1.web.7z header.txt

图 3-22 配置通过 Commander 实现批量升级组网图



配置思路

采用以下思路配置设备：

1. 配置文件服务器，将用户需要加载的文件保存至文件服务器。
2. 在各Client上配置Switch（Commander）的IP地址。
3. 在Switch上配置Commander功能，以实现通过Commander进行批量升级。
   - 配置Commander的基本功能。
   - 根据需要待升级Client的设备类型及需要加载的文件，配置相应的Group进行匹配。
   - 为了后期的维护，需要在Commander上配置自动备份配置文件功能，便于后续进行故障替换。
   - 由于有Client串联组网，为了确保Client5和Client6能够下载文件成功，所以需要配置延时激活时间，同时为了减少升级带来的业务影响，所以选择在凌晨2点激活文件。
4. 启动批量升级流程。

操作步骤

步骤1 配置文件服务器

请根据文件服务器的操作指导进行配置。

配置完成后，将所有待升级Client需要加载的文件保存至文件服务器中。

步骤2 在各Client上配置Commander的IP地址

在Client1上配置Commander的IP地址。

```
<HUAWEI> system-view
[HUAWEI] easy-operation commander ip-address 172.31.20.10
Warning: The pre-shared key can be modified to improve security. Continue? [Y/N]:y
Enter the pre-shared key:******
Confirm the pre-shared key:******
```

在Client2～Client6进行同样的配置。

步骤3 配置Commander的基本功能。

```
<HUAWEI> system-view
[HUAWEI] sysname Commander
[Commander] easy-operation commander ip-address 172.31.20.10
Warning: The pre-shared key can be modified to improve security. Continue? [Y/N]:y
Enter the pre-shared key:******
Confirm the pre-shared key:******
[Commander] easy-operation commander enable
[Commander] easy-operation
[Commander-easyoperation] sftp-server 172.31.1.90 username admin password EasyOperation
[Commander-easyoperation] backup configuration interval 2
```

步骤4 配置Client加入Commander的管理

```
[Commander-easyoperation] client auto-join enable
```

使能自动加入功能后，可以在Commander上学习到Client1～Client6的设备信息及当前加载的文件信息。可通过**display easy-operation client**进行查询。

步骤5 配置下载文件信息及文件生效方式

为Client1配置根据IP地址匹配的Group，并指定需要加载的文件信息。

```
[Commander-easyoperation] group custom ip-address g1
[Commander-easyoperation-group-custom-g1] match ip-address 172.31.20.100 24
[Commander-easyoperation-group-custom-g1] system-software s7700.cc
[Commander-easyoperation-group-custom-g1] license license.dat
```



```
[Commander-easyoperation-group-custom-g1] custom-file header1.txt
[Commander-easyoperation-group-custom-g1] quit
```

为Client2、Client3、Client5配置根据设备类型匹配的内置Group，并指定需要加载的文件信息。

```
[Commander-easyoperation] group build-in s5700-hi
[Commander-easyoperation-group-build-in-S5700-HI] system-software s5700-hi.cc
[Commander-easyoperation-group-build-in-S5700-HI] quit
```

为Client4配置根据IP地址匹配的Group，并指定需要加载的文件信息。

```
[Commander-easyoperation] group custom ip-address g2
[Commander-easyoperation-group-custom-g2] match ip-address 172.31.10.10 24
[Commander-easyoperation-group-custom-g2] system-software s5700-x-li.cc
[Commander-easyoperation-group-custom-g2] quit
```

为Client6配置根据MAC地址匹配的Group，并指定需要加载的文件信息。

```
[Commander-easyoperation] group custom mac-address g3
[Commander-easyoperation-group-custom-g3] match mac-address xxxx-xxxx-xxxx
[Commander-easyoperation-group-custom-g3] web-file web_1.web.7z
[Commander-easyoperation-group-custom-g3] custom-file header.txt
[Commander-easyoperation-group-custom-g3] quit
```

在全局Commander下配置激活时间及方式。

```
[Commander-easyoperation] activate-file in 2:00 reload
[Commander-easyoperation] quit
```

步骤6 检查配置结果

查看Commander上的全局配置信息。

```
[Commander] display easy-operation configuration
-------------------------------------------------------------------------------
 Role                          : Commander
 Commander IP address          : 172.31.20.10
 Commander UDP port            : 60000
 IP address of file server     : 172.31.1.90
 Type of file server           : SFTP
 Username of file server       : admin
 Default system-software file  : -
 Default system-software version : -
 Default configuration file    : -
 Default patch file            : -
 Default WEB file              : -
 Default license file          : -
 Default custom file 1         : -
 Default custom file 2         : -
 Default custom file 3         : -
 Auto clear up                 : Disable
 Auto join in                  : Enable
 Topology collection           : Disable
 Activating file time          : In 02:00
 Activating file method        : Reload
 Aging time of lost client(hours): -
 Backup configuration file mode  : Default
 Backup configuration file interval(hours): 2
-------------------------------------------------------------------------------
```

查看Commander上配置的所有Group的信息。

```
[Commander] display easy-operation group
The total number of group configured is : 4
The number of build-in group is       : 1
The number of custom group is         : 3

-------------------------------------------------------
 Groupname                     Type     MatchType
```

```
-------------------------------------------------------
 S5700-HI                    build-in device-type
 g1                        custom   ip-address
 g2                        custom   ip-address
 g3                        custom   mac-address
-------------------------------------------------------
```

查看Commander上配置的Group名称为g1的信息。

```
[Commander] display easy-operation group custom g1
-------------------------------------------------------------------------------
 Group name               : g1
 Configuration file       : -
 System-software file     : s7700.cc
 Patch file               : -
 WEB file                 : -
 License file             : license.dat
 Customs file 1           : header1.txt
 Customs file 2           : -
 Customs file 3           : -
 Activating file time     : Immediately
 Activating file method   : Default
 Ip-address list          :
  Ip-address       Ip-mask
  172.31.20.100    255.255.255.0
-------------------------------------------------------------------------------
```

步骤7 启动批量升级流程

```
[Commander] easy-operation
[Commander-easyoperation] upgrade group
Warning: This command will start the upgrade process of all groups and clients i
n these groups may reboot. Ensure that configurations of the clients have been s
aved. Continue?[Y/N]:y
```

在此过程中，可以执行命令**display easy-operation download-status**查看各Client的下载状态。

```
[Commander-easyoperation] display easy-operation download-status
The total number of client in downloading files is : 6

-------------------------------------------------------------------------------
  ID    Mac address    IP address      Method     Phase        Status
-------------------------------------------------------------------------------
  1     xxxx-xxxx-xxxx 172.31.20.100   Upgrade    Sys-file     Upgrading
  2     xxxx-xxxx-xxxx 172.31.10.15    Upgrade    Sys-file     Upgrading
  3     xxxx-xxxx-xxxx 172.31.10.20    Upgrade    Sys-file     Upgrading
  4     xxxx-xxxx-xxxx 172.31.10.10    Upgrade    Sys-file     Upgrading
  5     xxxx-xxxx-xxxx 172.31.10.18    Upgrade    Sys-file     Upgrading
  6     xxxx-xxxx-xxxx 172.31.10.11    Upgrade    Web-file     Upgrading
```

----结束

配置文件

Commander的配置文件

```
#
sysname Commander
#
easy-operation commander ip-address 172.31.20.10
easy-operation commander enable
#
easy-operation
 client auto-join enable
 sftp-server 172.31.1.90 username admin password %^%#=.X8C_TN##%&9P>3RK503O@w-=Fr
%>naT#E3P4{0%^%#
 backup configuration interval 2
 activate-file reload
 activate-file in 02:00
```



```
 group build-in S5700-HI
  system-software s5700-hi.cc
 group custom ip-address g1
  system-software s7700.cc
  license license.dat
  custom-file header1.txt
  match ip-address 172.31.20.100 255.255.255.0
 group custom ip-address g2
  system-software s5700-x-li.cc
  match ip-address 172.31.10.10 255.255.255.0
 group custom mac-address g3
  web-file web_1.web.7z
  custom-file header.txt
  match mac-address xxxx-xxxx-xxxx xxxx-xxxx-xxxx
#
return
```

Client1～Client6的配置文件

```
#
easy-operation commander ip-address 172.31.20.10
#
return
```

3.15.7 通过 Commander 实现批量配置设备示例

组网需求

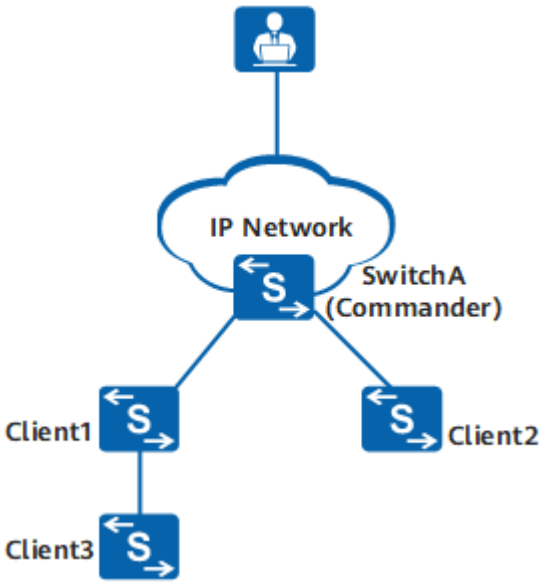
如图3-23所示，在运行EasyDeploy功能的某企业网络中，Client1～Client3是某企业内部各楼宇中的设备，与SwitchA及文件服务器间的路由可达。用户希望通过Commander实现对各个Client的批量配置功能。

Client1～Client3的设备情况，如表3-9所示。

表 3-9 设备情况说明

新加入的设备	设备型号	命令行脚本
Client1	S5732-H	cfg1.bat
Client2	S6730-H	cfg2.bat
Client3	S6730-H	cfg2.bat

图 3-23 通过 Commander 实现批量配置设备组网图



配置思路

采用以下思路配置设备：

1. 将离线制作的命令行脚本上传到SwitchA上。
2. 下发命令行。

操作步骤

步骤1 离线制作命令行脚本

新建文本文档，在文本文档中录入需要下发的命令行，录入完成之后保存，然后将文件扩展名“.txt”替换为“.bat”。

命令行脚本制作完成后，将脚本上传到Commander上。

步骤2 下发命令行

```
<HUAWEI> system-view
[HUAWEI] sysname SwitchA
[SwitchA] easy-operation
[SwitchA-easyoperation] execute cfg1.bat to client 1
Warning: This operation will start the batch command executing process to the cl
ients. Continue?[Y/N]:y
Info: This operation will take some seconds, please wait..
[SwitchA-easyoperation] execute cfg2.bat to client 2 to 3
Warning: This operation will start the batch command executing process to the cl
ients. Continue?[Y/N]:y
Info: This operation will take some seconds, please wait..
```

步骤3 检查配置结果

查看批量配置的执行结果。

```
[SwitchA-easyoperation] display easy-operation batch-cmd result
This operation will take some seconds, please wait..
-------------------------------------------------------------
 ID   Total  Successful     Failed     Time
```

```
-------------------------------------------------------------
1    50   50          0       2013-09-04  21:45:29
2    30   30          0       2013-09-04  21:55:29
3    30   30          0       2013-09-04  21:55:29
-------------------------------------------------------------
```

----结束

3.15.8 将有配置设备加入 Commander 管理示例

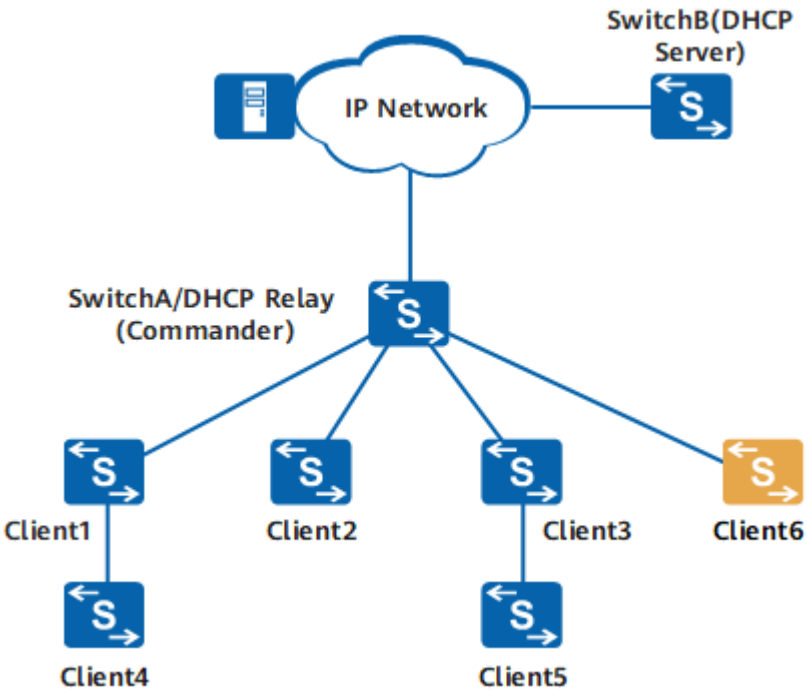
组网需求

如图3-24所示，在运行EasyDeploy功能的某企业网络中，SwitchA为Commander及DHCP中继，DHCP服务器和文件服务器与SwitchA之间路由可达。

现在希望将网络中一台有配置设备Client6加入Commander的管理，以便对其进行监控和管理。

Commander的IP地址是192.168.1.6/24，新Client的MAC地址是xxxx-xxxx-xxxx。

图 3-24 将有配置设备加入 Commander 管理组网图



配置思路

采用以下思路配置设备：

1. 配置待加入设备与Commander之间路由可达。
2. 在Client上配置Commander的IP地址。
3. 在Commander上配置Client的匹配规则，以便Commander能识别新加入的设备。

说明

有配置设备加入Commander管理功能的实现基于已部署EasyDeploy功能的网络，加入有配置设备前已完成文件服务器、DHCP以及Commander的配置部署。

操作步骤

步骤1 在Client6上配置Commander的IP地址

```
<HUAWEI> system-view
[HUAWEI] sysname Client6
[Client6] easy-operation commander ip-address 192.168.1.6
Warning: The pre-shared key can be modified to improve security. Continue? [Y/N]:y
Enter the pre-shared key:******
Confirm the pre-shared key:******
```

步骤2 在SwitchA上配置新加入的Client的信息

```
<HUAWEI> system-view
[HUAWEI] sysname SwitchA
[SwitchA] easy-operation
[SwitchA-easyoperation] client 6 mac-address xxxx-xxxx-xxxx
[SwitchA-easyoperation] quit
```

说明

如果要加入Commander管理的设备数量过多，建议在Commander上使能Client自动加入功能。

步骤3 检查配置结果

查看Client信息库的信息。

```
[SwitchA] display easy-operation client
The total number of client is : 6

--------------------------------------------------------------------------------
ID   Mac address    ESN                 IP address      State
--------------------------------------------------------------------------------
1    xxxx-xxxx-xxxx 2102113089P0xxxxxxx          192.168.1.208   RUNNING
2    xxxx-xxxx-xxxx -                   -            INITIAL
3    -              210235182810xxxxxxx          192.168.1.210   INITIAL
4    xxxx-xxxx-xxxx 210235126318xxxxxxx          192.168.1.167   RUNNING
5    xxxx-xxxx-xxxx 210235345120xxxxxxx          192.168.1.105   RUNNING
6    xxxx-xxxx-xxxx 210235276310xxxxxxx          192.168.1.254   RUNNING
--------------------------------------------------------------------------------
```

查看新加入的MAC地址为xxxx-xxxx-xxxx的Client的详细信息。

```
[SwitchA] display easy-operation client mac-address xxxx-xxxx-xxxx
--------------------------------------------------------------------------------
Client ID                : 6
Host name                : HUAWEI
Mac address              : xxxx-xxxx-xxxx
ESN                      : 210235276310xxxxxxx
IP address               : 192.168.1.254
Model                    : S5720C-EI
Device Type              : S5720-EI
System-software file     : flash:/s5720-ei-V200R022C00.cc
System-software version  : V200R022C00
Configuration file       : flash:/254.cfg
Patch file               : -
WEB file                 : -
License file             : -
System CPU usage         : 6%
System Memory usage      : 55%
Backup configuration file : -
Backup result            : -
Last operation result    : -
```



```
 Last operation time          : 0000-00-00  00:00:00
 State                        : RUNNING
 Aging time left (hours)      : -
------------------------------------------------------------------------------
```

----结束

配置文件

SwitchA的配置文件

```
#
sysname SwitchA
#
easy-operation
 client 6 mac-address xxxx-xxxx-xxxx
#
return
```

Client6的配置文件

```
#
sysname Client6
#
easy-operation commander ip-address 192.168.1.6
#
return
```

3.15.9 通过 eSight 对园区总部进行零配置部署

前提条件

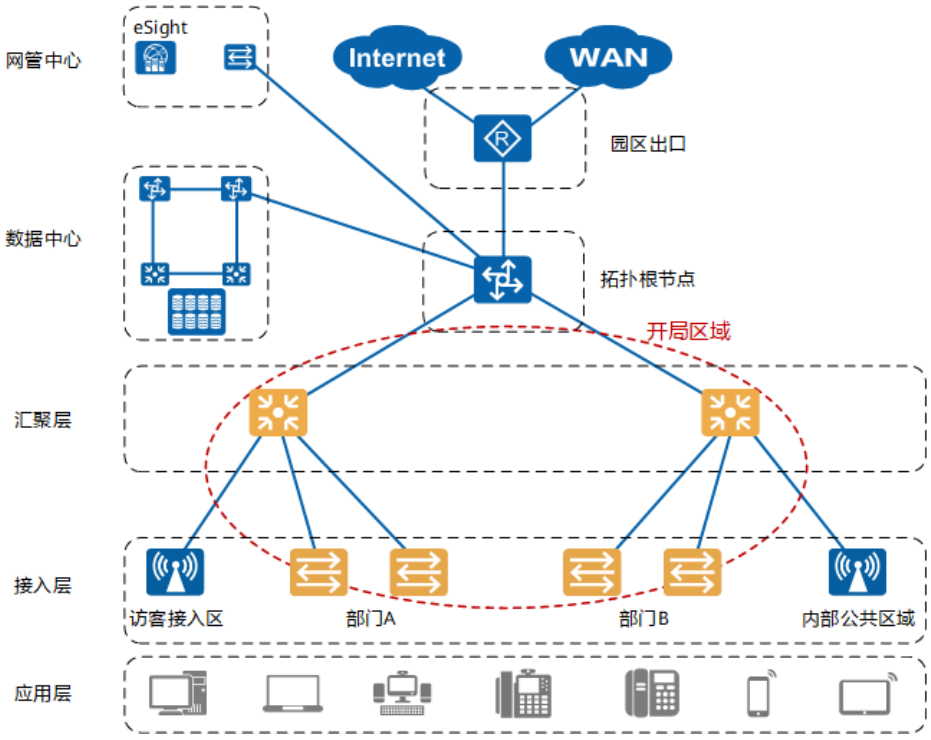
- 根设备和待部署设备支持零配置部署特性，具体的设备类型请参考《 eSight规格清单 》。
- 根设备已加载到eSight中进行管理，且设备和eSight可以通过SNMP和Telnet协议正常通讯。
- 已配置DHCP服务器，且DHCP服务器将根设备作为网关。
- 零配置部署过程中设备Console口不能有I/O输入。
- 设备软件包、License文件、补丁文件已制作好，并上传到网管，如尚未上传，请到 “配置 > 配置管理 > 设备软件管理”完成版本文件上传操作。

组网需求

M公司新建的有线园区网中，汇聚层和接入层设备较多。以往的部署，网络规划设计、软件/硬件安装调试一般为不同人员，需要人工通过U盘的方式逐个设备关联部署文件，配置复杂且影响效率。网络管理员小王希望可以通过eSight对汇聚和接入层设备做统一的零配置部署，以减少管理成本。

如下图所示，红圈里为待部署的设备。eSight软件版本以V300R003C20版本为例。

图 3-25 通过 eSight 对园区总部进行零配置部署组网图



配置思路

采用如下的思路配置：

1. 选择根节点设备，在拓扑根节点上配置允许VLAN1通过（默认的VLAN 1设置成零配置部署专用VLAN）；
2. 将根设备设置成DHCP服务器；
3. 通过拓扑部署规划网络拓扑；
4. 准备待部署设备的配置文件；
5. 将设备配置文件与设备形成映射关系；
6. 根据规划的拓扑，硬调人员安装设备，将设备上电；
7. 软调人员在网管比对实际物理拓扑和规划的拓扑是否一致；
8. 软调人员比对无误之后，触发部署，部署设备下载文件。

数据规划

表 3-10 根设备

设备类型	设备IP	下行口1	下行口2
S5720-56C-PWR-HI-AC	10.137.58.61	GE0/0/1	GE0/0/2

表 3-11 汇聚层设备

设备类型	IP地址	上行口	下行口1	下行口2
S5720-32C-HI-24S-AC	10.137.58.1	GE0/0/1	GE0/0/2	GE0/0/3
S5720-32C-HI-24S-AC	10.137.58.2	GE0/0/1	GE0/0/2	GE0/0/3

表 3-12 接入层设备

设备类型	IP地址	上行口
S2750-28TP-EI-AC	10.137.58.3	GE0/0/1
S2750-28TP-EI-AC	10.137.58.4	GE0/0/1
S2750-28TP-EI-AC	10.137.58.5	GE0/0/1
S2750-28TP-EI-AC	10.137.58.6	GE0/0/1

操作步骤

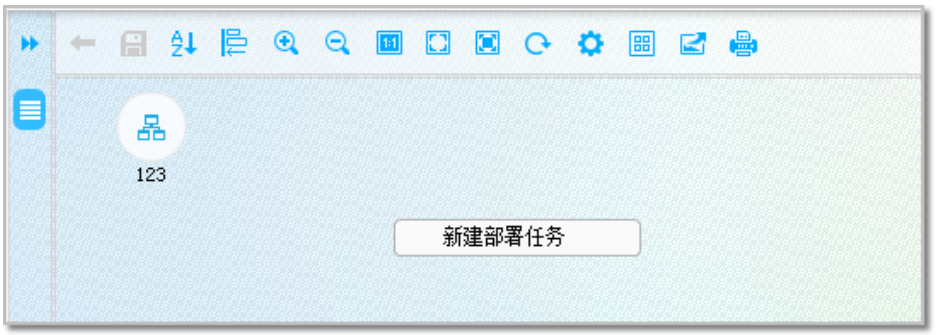
步骤1 在根设备上配置允许VLAN1通过（此处配置较简单不再赘述）。

步骤2 将根设备设置为DHCP服务器，具体设置请参见**配置DHCP服务器**。

步骤3 通过拓扑部署规划网络拓扑。

1. 在主菜单中选择“配置 > 零配置部署 > 拓扑规划部署”。

2. 在主拓扑空白处单击右键，选择“新建部署任务”。

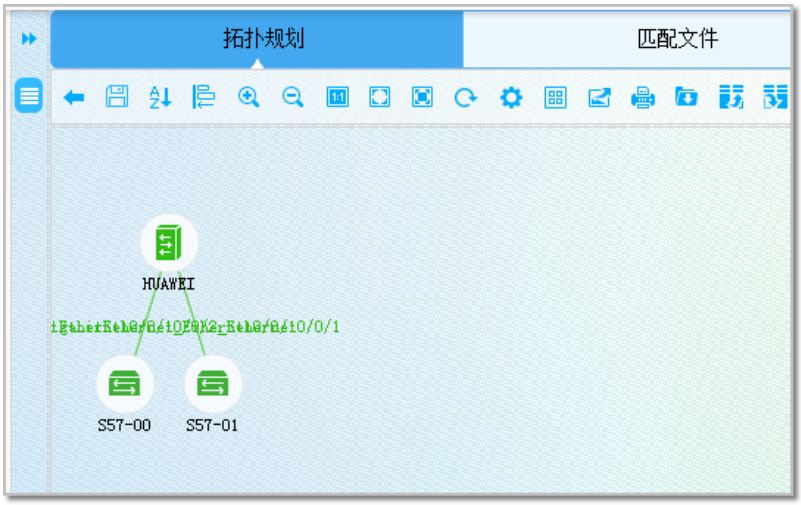


3. 在弹出的“创建部署任务”对话框中，将“任务名称”设置为“新增AB部门部署任务”。主拓扑即新增一个部署任务视图。
4. 双击“新增AB部门部署任务”视图，进入该任务的子视图页面。

5. 单击“添加根节点”图标，页面弹出“添加根设备”的选择对话框。根据子网选择待部署的设备根节点后，单击“确定”，页面即显示已添加的根节点。

   如果有规划表单，也可以使用模板导入设备生成拓扑。
6. 新增汇聚层设备：在“拓扑规划”拓扑页面中，在根设备的图标上单击右键，选择“新建对端设备 > 单台交换机”，弹出“新增下层设备”的对话框，在对话框中输入如下参数，单击“确定”。

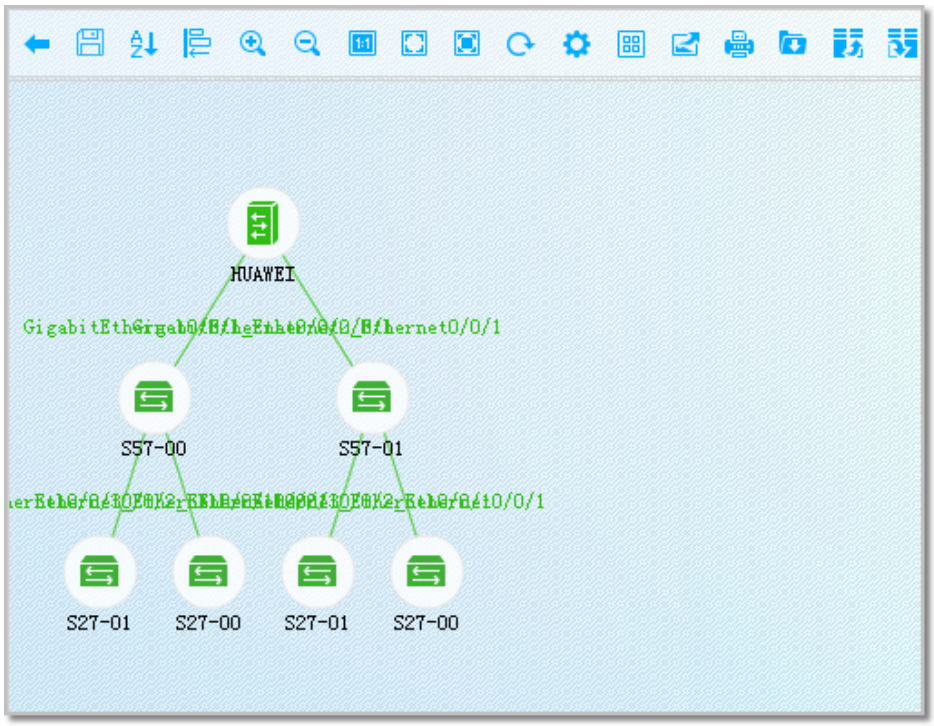
7. 页面显示已创建的汇聚层设备，在拓扑工具栏中单击，选择“上下树形”。页面即显示已排序好的根设备和汇聚层设备。



8. 在汇聚设备“S57-01”图标上单击右键，选择“新建对端设备 > 单台交换机”，弹出“新增下层设备”的对话框，在对话框中输入如下参数，单击“确定”。

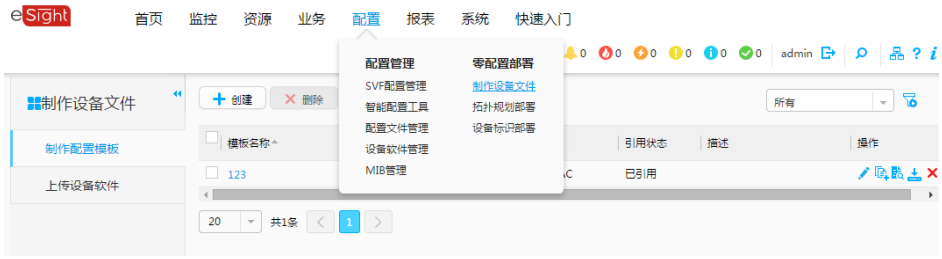
9. 在汇聚设备“S57-02”图标上单击右键，选择“新建对端设备 > 单台交换机”，弹出“新增下层设备”的对话框，在对话框中输入如下参数，单击“确定”。

10. 在拓扑工具栏中单击，选择“上下树形”。页面即显示已排序好的根设备、汇聚层设备和接入层设备。



步骤4 准备待部署设备的配置文件。

1. 在主菜单中选择“配置 > 零配置部署 > 制作设备文件”。

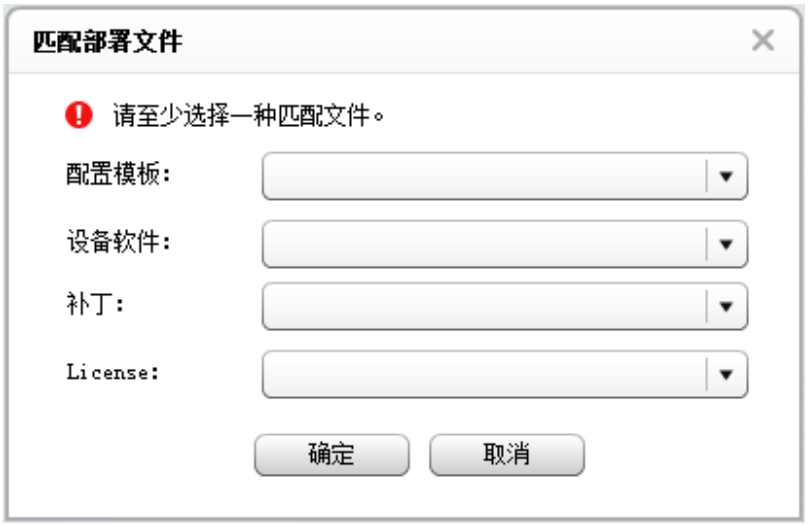


2. 单击“创建”，输入以下参数，单击“下一步”后，单击“确定”。完成汇聚层设备配置文件的创建。

3. 重复上一步，完成接入层设备配置文件的创建。

步骤5 将设备配置文件、部署大包、license文件与设备形成映射关系；

1. 将拓扑切换到“匹配文件”页面。
2. 框选汇聚层的两个设备，在汇聚层设备图标上单击右键，选择“匹配部署文件”。在页面中选择对应的部署文件，单击“确定”。
3. 框选接入层的四个设备，在接入层设备图标上单击右键，选择“匹配部署文件”。在页面中选择对应的部署文件，单击“确定”。



步骤6 根据规划的拓扑，硬调人员安装设备，将设备上电；

步骤7 软调人员在网管比对实际物理拓扑和规划的拓扑是否一致。使能拓扑收集过程后，eSight从拓扑根节点上收集部署区域网络拓扑，并和规划拓扑映射，展示差异供用户纠错。

1. 将拓扑切换到“对比拓扑”页面，页面下方会显示拓扑比对的结果。

步骤8 软调人员比对无误之后，触发部署，部署设备下载文件。

1. 将拓扑切换到“部署”页面，框选所有的待部署子设备，单击右键后，选择“部署”。
2. 页面显示部署下发的结果，框选所有的待部署子设备，单击右键后，选择“激活”，设备将重新启动后加载新的配置文件，即完成整个部署下发过程。

----结束

操作结果

完成整个部署后，在“监控 > 拓扑 > 拓扑管理”中，可查看到新部署的设备，且设备的告警信息可以正常上报到网管。

3.15.10 通过手抄 MAC/ESN 方式对分支进行零配置部署

前提条件

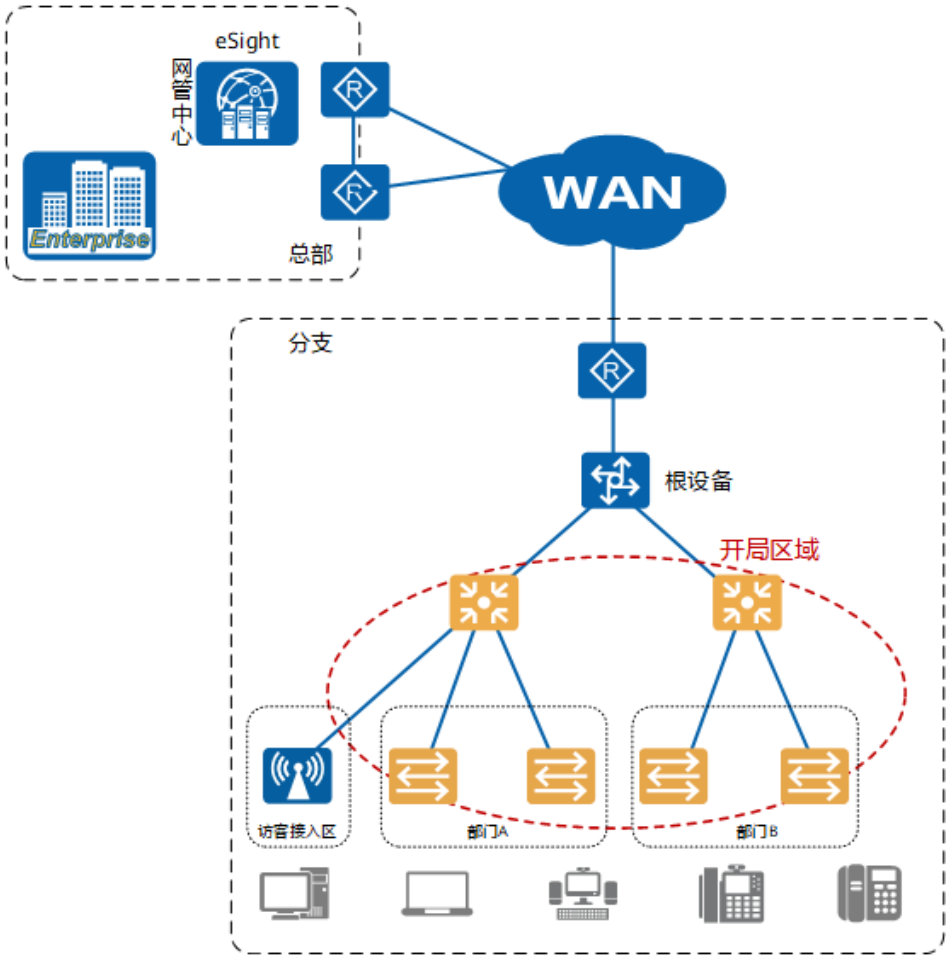
- 根设备已加载到eSight中进行管理，且设备和eSight可以通过SNMP和Telnet协议正常通讯。
- 已配置DHCP服务器，且DHCP服务器将根设备作为网关。
- 零配置部署过程中设备Console口不能有I/O输入。
- 设备软件包、License文件、补丁文件已制作好，并上传到网管，如尚未上传，请到 “配置 > 设备软件管理 > 版本管理”完成版本文件上传操作。

组网需求

M公司新建的有线园区网中，汇聚层和接入层设备较多，且配置较为复杂。网络管理员小王希望可以通过eSight对汇聚和接入层设备做统一的手抄MAC/ESN零配置部署，以减少管理成本。

如下图所示，红圈里为待部署的设备。eSight软件版本以V300R003C20版本为例。

图 3-26 通过手抄 MAC/ESN 方式对分支进行零配置部署



配置思路

采用如下的思路配置：

1. 选择根节点设备，在拓扑根节点上配置允许VLAN1通过；
2. 将根设备设置成DHCP服务器；
3. 规划设备部署文件；
4. 设备上电，用户手抄MAC/ESN；
5. 匹配设备MAC/ESN和设备部署文件；
6. 用户触发部署，设备完成部署文件加载，完成部署操作。

数据规划

表 3-13 根设备

设备类型	设备IP	下行口1	下行口2
S5720-56C-PWR-HI-AC	10.137.58.61	GE0/0/1	GE0/0/2

表 3-14 汇聚层设备

设备类型	IP地址	上行口	下行口1	下行口2
S5720-32C-HI-24S-AC	10.137.58.1	GE0/0/1	GE0/0/2	GE0/0/3
S5720-32C-HI-24S-AC	10.137.58.2	GE0/0/1	GE0/0/2	GE0/0/3

表 3-15 接入层设备

设备类型	IP地址	端口
S2750-28TP-EI-AC	10.137.58.3	GE0/0/1
S2750-28TP-EI-AC	10.137.58.4	GE0/0/1
S2750-28TP-EI-AC	10.137.58.5	GE0/0/1
S2750-28TP-EI-AC	10.137.58.62	GE0/0/1

表 3-16 设备 MAC/ESN

位置说明	IP地址	ESN	设备类别	设备型号	配置文件	其他文件
汇聚1	00E0-FC12-AA4B	—	S5700	S5700-28C-HI	N1.zip	S5700.cc
汇聚2	00E0-FC12-AA5B	—	S5700	S5700-28C-HI	N2.zip	S5700.cc
接入1	—	AAC1223431	S2700	S2750-28TP-EI-AC	N3.zip	S2700.cc
接入2	—	AAC1223432	S2700	S2750-28TP-EI-AC	N4.zip	S2700.cc

位置说明	IP地址	ESN	设备类别	设备型号	配置文件	其他文件
接入3	—	BAC1223433	S2700	S2750-28TP-EI-AC	N5.zip	S2700.cc
接入4	—	BAC1223436	S2700	S2750-28TP-EI-AC	N6.zip	S2700.cc

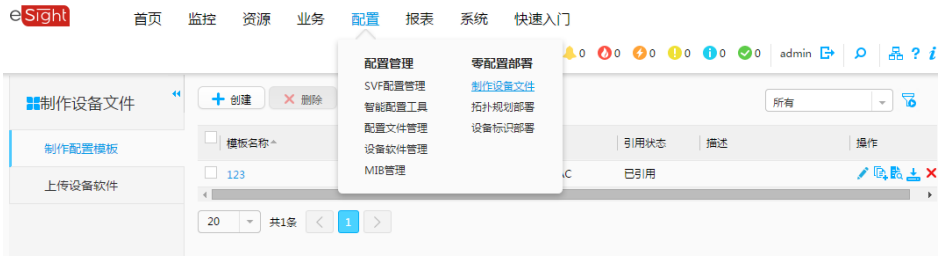
操作步骤

步骤1 在根设备上配置允许VLAN1通过（此处配置较简单不再赘述）。

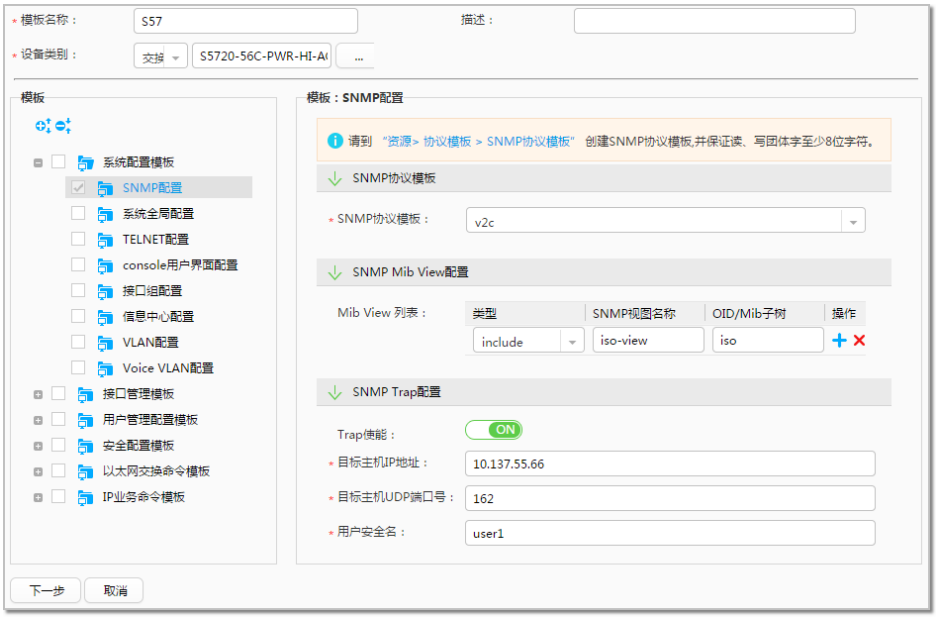
步骤2 将根设备设置为DHCP服务器，具体设置请参见**配置DHCP服务器**。

步骤3 准备待部署设备的配置文件。

1. 在主菜单中选择“配置 > 零配置部署 > 制作设备文件”。

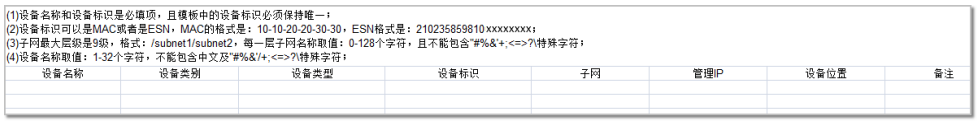


2. 单击“创建”，输入以下参数，单击“下一步”后，单击“确定”。完成汇聚层设备配置文件的创建。



3. 重复上一步，完成接入层设备配置文件的创建。

步骤4 部署设备连线，上电；手抄MAC/ESN并记录设备位置、型号等信息，并记录到以下格式的excel文档中。



步骤5 匹配待部署设备的配置文件、软件包、补丁包、license文件。

1. 在主菜单中选择“配置 > 零配置部署 > 设备标识部署”。

2. 单击“创建”后，单击“新建设备 > 批量导入”。

3. 在“批量导入”对话框中，上传步骤2中记录的excel文件，单击“确定”，完成部署任务创建。
4. 选中已创建的部署任务，单击“匹配部署文件”，选择对应的配置文件、设备软件、补丁和License文件。
5. 单击“确定”，完成部署文件的匹配任务。

步骤6 用户触发部署，部署交换机进行相关文件下载，完成后重启激活设备。

1. 选择以上刚创建的手动部署任务，单击“部署”。
2. 单击“激活”，将重启设备，设备将加载最新的部署文件，即完成整个部署任务的下发。

----结束

操作结果

完成整个部署后，在“监控 > 拓扑 > 拓扑管理”中，可查看到新部署的设备，且设备的告警信息可以正常上报。

4 U 盘开局配置

4.1 U盘开局简介
4.2 U盘开局原理描述
4.3 U盘开局配置注意事项
4.4 制作索引文件
4.5 配置U盘开局
4.6 U盘开局配置举例

4.1 U 盘开局简介

定义

U盘开局是指设备在开局部署时，用户预先将开局文件存储在U盘中，然后将U盘插入设备，通过从U盘下载开局文件来对设备实现目标版本以及相关业务的部署。

目的

随着网络规模的扩大，网络中需要部署的设备数量越来越多，开局部署也日渐增多。相比传统的通过专业工程师逐台的去给设备开局的模式，U盘开局功能只需要让专业工程师把所有开局文件存储到U盘中即可，具体开局任务可以通过开局现场非专业人员来进行。这样即简化了开局部署流程，又降低了开局部署成本。

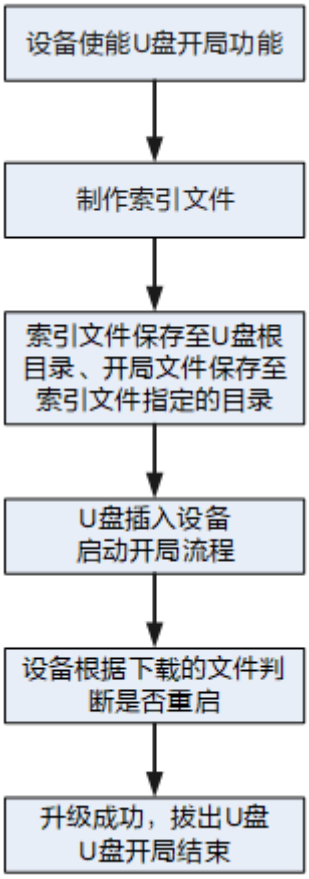
4.2 U 盘开局原理描述

U 盘开局流程

U盘开局之前，需要先制作U盘开局索引文件并将索引文件保存至U盘根目录下。把需要加载的开局文件保存至U盘指定目录（根据索引文件的要求保存至相应目录）。将U盘插入设备中，设备会根据开局文件自动完成文件的加载。

U盘开局流程如**图4-1**所示:

图 4-1 U 盘开局流程图



开局文件分类

可以通过U盘中的索引文件实现对设备所需文件的自动加载。

- **必选文件**
  - 索引文件：名称必须为smart_config.ini
- **可选文件**
  - 系统软件：后缀名为.cc
  - 配置文件：后缀名为.cfg或.zip
  - 补丁文件：后缀名为.pat
  - Web网页文件：后缀名为.web.7z
  - 用户自定义文件
  - 脚本文件：后缀名为.bat

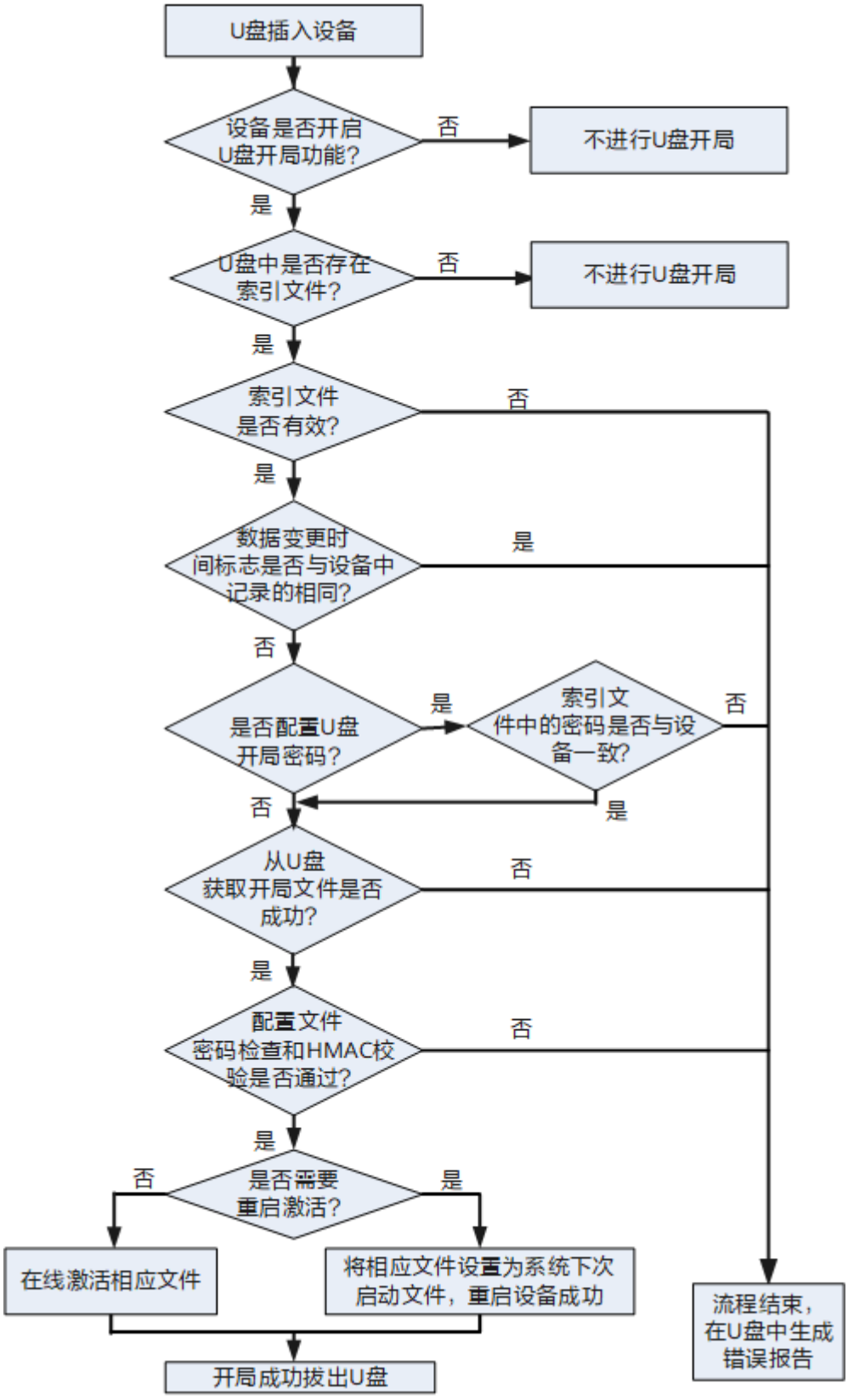
    可通过脚本文件，在U盘开局的同时，导入堆叠的相关配置。

用户可以根据需要选择其中的一种或多种可选文件进行U盘开局。

U 盘开局设备运行流程

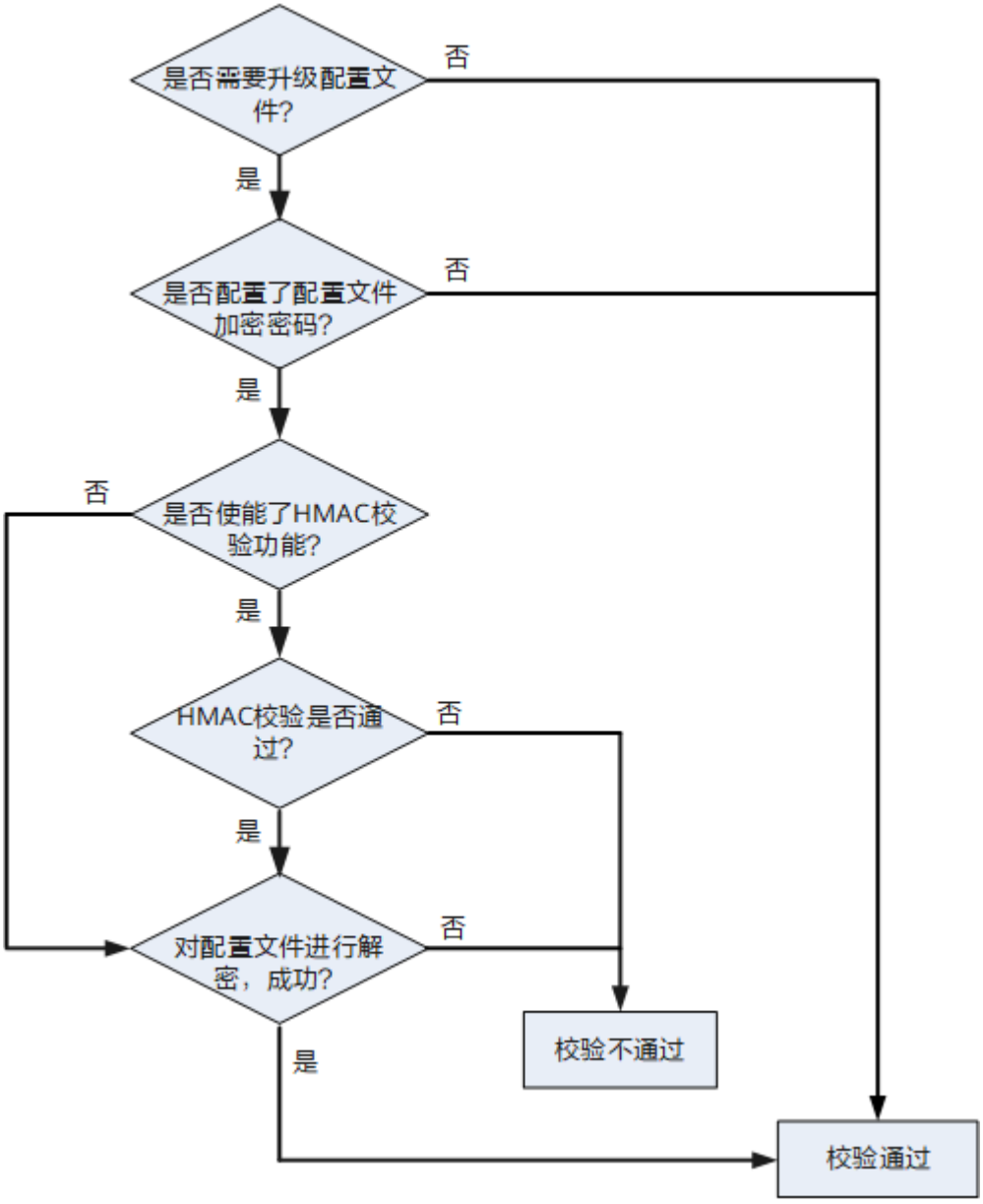
U盘插入设备后的开局流程如图4-2所示：

图 4-2 U 盘开局设备运行流程图



其中对配置文件进行密码检查和HMAC校验流程如图4-3所示：

图 4-3 U 盘开局时对配置文件进行密码检查和 HMAC 校验流程图



1. U盘插入需要升级的设备，设备检测到U盘在位。
2. 设备是否开启了U盘开局功能：
   - 如果是空配置设备，则U盘开局功能一直是开启的，则进入步骤3。
   - 如果是非空配置设备开启了U盘开局功能，则进入步骤3。
   - 如果是非空配置设备未开启U盘开局功能，则不进行U盘开局。
3. 设备检测U盘中是否存在U盘开局索引文件：
   - 如果文件存在，进入步骤4。
   - 如果文件不存在，则不进行U盘开局。

4. 设备检测U盘开局索引文件格式的合法性：
   - 如果合法，进入步骤5。
   - 如果文件非法，开局失败，流程结束，在U盘中生成错误报告。
5. 设备将索引文件中指定的数据变更时间标志与设备中记录的上次U盘开局的时间标志进行比较：
   - 如果不相同，进入步骤6。
   - 如果相同，开局失败，流程结束，在U盘中生成错误报告。
6. 判断设备上是否配置U盘开局的密码：
   - 如果配置了密码，会再次判断索引文件中指定的密码是否与设备中配置的一致，如果一致，进入步骤7。如果不一致，开局失败，流程结束，在U盘中生成错误报告。
   - 如果没有配置密码，进入步骤7。
7. 系统按照索引文件中的描述信息从U盘中获取开局文件，并将其保存至指定的存储介质中：
   - 如果获取文件成功，进入步骤8。
   - 如果获取文件失败，开局失败，流程结束，在U盘中生成错误报告。
8. 进行配置文件密码检查和HMAC校验：
   - 如果升级文件中不包含配置文件，则进入步骤9。
   - 如果升级文件中包含配置文件，未设置配置文件加密密码，则进入步骤9。
   - 如果升级文件中包含配置文件，设置了配置文件加密密码，但未使能HMAC校验功能，则对配置文件进行解密，解密成功，则进入步骤9；不成功，则开局失败，流程结束，在U盘中生成错误报告。
   - 如果升级文件中包含配置文件，设置了配置文件加密密码，并且使能了HMAC校验功能，则首先对配置文件进行HMAC校验，再对配置文件进行解密。HMAC校验通过并且配置文件解密成功，则进入步骤9；否则开局失败，流程结束，在U盘中生成错误报告。
9. 根据获取的文件或者指定的激活方式，设备自动判断是否需要重启激活。
   - 如果不需要重启，则在线激活相应文件，进入步骤10。
   - 如果需要重启，设备会将相应文件设置为下次启动文件，自动重启成功后，进入步骤10。
10. U盘开局成功，流程结束。将U盘从设备中拔出。

说明

- 如果开局成功，系统会在U盘根目录中生成文件名为**usbload_verify.txt**的开局成功报告。
- 如果开局失败，系统会在U盘根目录中生成文件名为**usbload_error.txt**的开局失败报告，用户可根据此报告定位出错原因。

  如果**usbload_error.txt**报告中有“Activating file *vrpcfg.zip* failed.”信息（*vrpcfg.zip*表示配置文件名称，请以实际为准），说明激活配置文件失败，请检查配置文件是否正确，如Console接口登录密码是否正确。

4.3 U 盘开局配置注意事项

涉及网元

无需其他网元配合。

License 支持

本特性是交换机的基本特性，无需获得License许可即可应用此功能。

V200R022C00 版本特性支持情况

仅如下系列中有USB接口的款型支持U盘开局：

S5720-LI、S5720S-LI、S5720I-SI、S5735S-H、S5736-S、S5731-H、S5731-H-K、S5731-S、S5731S-S、S5731S-H、S5732-H、S5732-H-K、S5735-L-I、S5735-L1、S5735-L、S5735S-L1、S5735S-L、S5735S-L-M、S500、S5735-S、S5735S-S、S5735-S-I、S6735-S、S6720-EI、S6720S-EI、S6730-H、S6730-H-K、S6730S-H、S6730-S、S6730S-S

说明

如需了解交换机软件配套详细信息，请点击**硬件中心**，并选择产品型号进行查询。

S5731-L和S5731S-L属于远端模块，不支持Web管理、YANG和命令行，仅支持通过中心交换机对其下发配置，相关操作请参见《S300, S500, S2700, S5700, S6700 V200R022C00 配置指南-设备管理》中的“智能极简园区网络配置（小行星方案）”。

特性依赖和限制

使用U盘开局前

- U盘规格：文件系统格式是FAT32，硬件接口是标准的USB2.0（S5700-LI提供USB1.1接口）。因不同厂商U盘型号的兼容性和驱动存在差异，如果出现U盘不能使用，请尝试更换主流厂商的U盘，交换机支持不大于128GB容量的U盘。
- U盘开局功能与SVF、EasyDeploy、WEB初始化模式功能互斥。
- U盘开局前，保证开局设备可以正常启动，并且保证设备有足够的内存空间保存开局文件。
- 由于设备为空配置设备，还没有相应的安全保证措施。因此当具体开局任务由开局现场非专业人员来进行时，请保证该人员不会对设备、U盘及开局文件进行非法操作。
- U盘开局配置文件中必须配置Console接口的登录密码，否则会导致开局失败，失败原因可查看“usbload_error.txt”文件信息。
- U盘开局配置文件中vty用户登录界面验证方式请勿设置为**authentication-mode none**，否则会导致开局失败。
- 不支持同时插入2个U盘进行开局。
- 不支持通过命令行读取U盘中的内容，不支持通过**dir**命令查看U盘中的文件和目录信息（无论开局前、开局中还是开局后），不支持U盘和设备存储器Flash中的内容互相拷贝。
- 索引文件需要与当前设备的版本配套使用。例如，从低版本升级至高版本，如果索引文件中有低版本不支持的字段时，升级过程中该字段不生效。
- smart_config.ini格式的索引文件支持对配置文件进行加密和HMAC校验功能，usbload_config.txt格式的索引文件不支持。因此，当升级文件中包含配置文件时，建议使用smart_config.ini格式的索引文件，设置配置文件加密密码并使能HMAC校验功能，以提高安全性。从V200R013C00版本开始，设备仅支持smart_config.ini格式索引文件进行U盘开局。

- 从V200R005C00版本开始，设备支持smart_config.ini格式索引文件进行U盘开局，此格式索引文件支持堆叠场景，U盘必须插入堆叠主交换机中。如果插入备交换机或从交换机，U盘开局流程不响应。
- V200R021C01及之后版本：开局成功后，USB指示灯绿色常亮，如果设备重启后发生主备倒换，则USB指示灯不亮。
- S5700S-28P-PWR-LI-AC、S5700S-28X-LI-AC、S5700S-52X-LI-AC、S5700S-LI、S5710-X-LI、S5720-EI、S5720-HI、S5720I-SI、S5720-LI、S2730S-S、S5735-L-I、S5735-L1、S300、S5735-L、S5735S-L1、S5735S-L、S5735S-L-M、S5720S-LI、S5720S-SI、S5720-SI、S500、S5735-S、S5735S-S、S5735-S-I、S5730-HI、S5731-H、S5731-H-K、S5731-S、S5731S-H、S5731S-S、S5732-H、S5732-H-K、S6720-EI、S6720-HI、S6720-LI、S6720S-EI、S6720S-LI、S6720S-SI、S6720-SI、S6730-H、S6730-H-K、S6730S-H、S6730-S、S6730S-S、S6735-S系列设备仅支持smart_config.ini格式索引文件。
- 当使用usbload_config.txt格式索引文件进行U盘开局时，只支持单台设备的场景，不支持多台设备堆叠的场景。在多台设备堆叠场景下，U盘如果插入备交换机或者从交换机，则开局流程不响应；如果插入主交换机，则开局失败，主交换机的U盘开局指示灯红色快闪，并记录错误报告，报告内容为“The usbload_config.txt index file can not be used for USB deployment of a multi-member stack”。
- 在V200R013C00版本，当设备在云模式零配置状态时，U盘开局支持下发堆叠口基本配置，包括如下命令：
  a. interface stack-port
  b. port interface enable
  c. shutdown interface
  d. stack slot priority
  e. stack slot renumber
- 从V200R019C00版本开始，当设备在NETCONF模式零配置状态时，U盘开局支持下发堆叠口基本配置，包括如下命令：
  a. interface stack-port
  b. port interface enable
  c. shutdown interface
  d. stack slot priority
  e. stack slot renumber
- 对于S5720-HI，如果设备启动U盘开局后需要重启，并且重启后设备将升级到V200R009C00或之后的版本，则重启前，系统将对下次启动生效的配置文件进行检查，检查配置文件中是否包含与下次运行版本相冲突的WLAN特性的配置。如果包含冲突配置，则无法重启，开局失败，同时在U盘根目录下生成错误报告usbload_error.txt文件，并记录失败原因。此时，需要用户将配置文件经**eDesk pro**工具进行转换后再设置为下次启动配置文件。

使用U盘开局时

- 使用U盘进行写操作时，请务必保证关闭U盘写保护功能。
- U盘开局过程中设备不能断电，否则会造成升级失败甚至会造成设备无法启动。
- U盘开局结束之前不能将U盘拔出，否则可能会造成U盘内的数据损坏。
- 当使用U盘对S5720-EI、S5720-HI、S5720I-SI、S5720-LI、S2730S-S、S5735-L-I、S5735-L1、S300、S5735-L、S5735S-L1、S5735S-L、S5735S-L-M、S5720S-

LI、S5720S-SI、S5720-SI、S500、S5735-S、S5735S-S、S5735-S-I、S5730-HI、S5731-H、S5731-H-K、S5731-S、S5731S-H、S5731S-S、S5732-H、S5732-H-K、S6720-EI、S6720-HI、S6720-LI、S6720S-EI、S6720S-LI、S6720S-SI、S6720-SI、S6730-H、S6730-H-K、S6730S-H、S6730-S、S6730S-S、S6735-S进行开局时，不能使用已分区的U盘，否则设备可能无法找到U盘上的文件，导致U盘开局失败。

- 如果是非空配置设备进行U盘开局，必须通过命令**set device usb-deployment password**配置U盘开局的认证密码。
- S5700-LI支持smart_config.ini和usbload_config.txt两种格式的索引文件。如果U盘中两种索引文件都存在，则优先使用smart_config.ini文件。U盘开局时，建议U盘中不要同时存放两种格式的索引文件。
- 在堆叠系统中，只要有一台设备不支持U盘开局，整个堆叠系统开局失败。
- 设备带U盘重启开局，可能会由于设备配置未恢复造成开局失败，则可通过拔插U盘解决。

4.4 制作索引文件

U 盘开局索引文件的制作方法

用户可以在PC机上编辑U盘开局索引文件，具体步骤如下：

1. 新建一个空的文本文档。
2. 按照U盘开局索引文件格式编辑文件内容。
3. 将此文本文档另存为“smart_config.ini”。
4. 将索引文件smart_config.ini拷贝至U盘，此文件必须保存至U盘根目录下。

U 盘开局索引文件格式

说明

- smart_config.ini类型的索引文件，每一行的内容不能超过512个字符，否则索引文件无效。
- smart_config.ini索引文件中的字段名不区分大小写。
- 索引文件中加载文件的字段均为可选，但至少要指定一种文件类型的字段。系统软件名、配置文件名及补丁文件名支持的最大长度为48个字节，其他类型文件名支持的最大长度为64个字节。

```
BEGIN LSW
[GLOBAL CONFIG]
TIMESN=
AUTODELFILE=
ACTIVEMODE=
USB-DEPLOYMENT PASSWORD=
[DEVICEn DESCRIPTION]
OPTION=
ESN=
MAC=
AUTODELFILE=
ACTIVEMODE=
DEVICETYPE=
VENDOR=
HMAC=
DIRECTORY=
SYSTEM-SOFTWARE=
SYSTEM-CONFIG=
SYSTEM-LICENSE=
```

```
SYSTEM-PAT=
SYSTEM-WEB=
SYSTEM-SCRIPT=
SYSTEM-USERDEF1=
SYSTEM-USERDEF2=
SYSTEM-USERDEF3=
END LSW
```

smart_config.ini索引文件支持注释信息，注释信息以英文半角的分号“;”开始。可以在字段的同一行后直接增加注释（字段内容与注释之间需要有空格隔开），也可以是单独的注释行。

表 4-1 smart_config.ini 索引文件字段含义

字段	描述
BEGIN LSW	必选字段。起始标志，此字段不能修改。
GLOBAL CONFIG	必选字段。全局配置起始标志，此字段不能修改。
TIMESN	必选字段。数据变更时间标志，字符串格式，长度范围为1～16，不能包含空格。建议格式：年月日.时分秒。 例如，2011年06月28日08时09分10秒，可设置为TIMESN=20110628.080910。 每个TIMESN对应某台升级的设备。在U盘开局过程中，设备会在重启前记录此TIMESN（升级后不需要重启的则在升级完成后记录），下次升级不可使用此TIMESN。如果由于某些原因造成在设备重启后升级失败，则需要将TIMESN重新修改后再进行U盘开局。
AUTODELFILE	可选字段。表示是否允许升级后自动删除原有系统软件。 ● AUTODELFILE=YES：删除 ● AUTODELFILE=NO：不删除 缺省情况下，AUTODELFILE为NO。如果该字段不存在、为空或是不合法值，均表示为缺省情况。 有两种AUTODELFILE字段：全局字段和单台设备字段。 ● 位于[GLOBAL CONFIG]字段内的是全局字段，位于[DEVICE*n* DESCRIPTION]内的是单台设备字段。 ● 如果单台设备设置了此字段的值为YES或NO，则以单台设备设置的生效。如果单台设备没有设置此字段或者此字段为空，则以全局设置的生效。

字段	描述	
ACTIVEMODE	可选字段。表示文件拷贝完成后的文件激活方式。 ● DEFAULT：按照各个文件的默认方式激活。 其中，系统软件、配置文件默认激活方式是重启设备；补丁文件默认激活方式是不重启设备，在线激活；Web网页文件、用户自定义文件不做激活处理，下载成功后U盘开局即结束。 ● RELOAD：采用重启设备的方式激活。 缺省情况下，ACTIVEMODE为DEFAULT。如果该字段不存在、为空或是不合法值，均表示为缺省情况。 有两种ACTIVEMODE字段：全局字段和单台设备字段。 ● 位于[GLOBAL CONFIG]字段内的是全局字段，位于[DEVICE*n* DESCRIPTION]内的是单台设备字段。 ● 如果单台设备设置了此字段的值为DEFAULT或RELOAD，则以单台设备设置的生效。如果单台设备没有设置此字段或者此字段为空，则以全局设置的生效。	
USB-DEPLOYMENT PASSWORD	可选字段。U盘开局的认证密码。如果待开局设备的配置中包含开局认证密码，则此字段中必须填入相应的密码，如果待开局设备中未配置密码，该字段为空或不存在即可。同一个索引文件只能使用同一个密码。如果一个索引文件需要对多个设备开局，则设备上配置的开局认证的密码必须相同。 **说明** 如果是非空配置设备进行U盘开局，必须通过命令**set device usb-deployment password**配置U盘开局的认证密码。	
DEVICE*n* DESCRIPTION	必选字段。单台设备文件信息描述起始标志，*n*表示设备的编号，从0开始，最大为65535。 **说明** ● DEVICE*n* DESCRIPTION字段下表示单台设备信息的每个字段不可以重复出现，否则将不匹配这个DEVICE*n*。 ● DEVICE按照文件中定义的顺序从上到下进行匹配，匹配到一组之后不会再匹配其它DEVICE*n*。	
OPTION	可选字段。单台设备文件信息有效标志，表示该设备文件信息是否有效。 ● OPTION=OK：有效 ● OPTION=NOK：无效，此单台设备的文件信息都无需判断 缺省情况下，OPTION为OK。如果该字段不存在、为空或是不合法值，均表示为缺省情况。	
ESN	可选字段。设备序列号。如果ESN=DEFAULT，表示不匹配ESN序列号，否则需要和设备匹配ESN。 缺省情况下，ESN为DEFAULT。如果该字段不存在或为空，则表示为缺省情况。	待升级的设备将在索引文件中按DEVICE从上往下进行匹配，匹配的优先级为：MAC > ESN > DEVICETYPE > DEFAULT。一旦匹配上，则按匹配上的DEVICE信息进行加载文件，如果此过程出错，将不会再次进行匹配，只会输出错误报告。

字段	描述
MAC	可选字段。设备MAC地址，格式为：XXXX-XXXX-XXXX，X为十六进制数。如果MAC=DEFAULT，表示不匹配MAC地址，否则需要和设备匹配MAC地址。 缺省情况下，MAC为DEFAULT。如果该字段不存在或为空，则表示为缺省情况。
DEVICETYPE	可选字段。表示与设备的类型匹配，取值请参考硬件描述中的产品子系列，例如S5732-H。如果DEVICETYPE=DEFAULT，表示不匹配设备类型。否则需要和设备的类型匹配。 缺省情况下，DEVICETYPE为DEFAULT。如果该字段不存在或为空，则表示为缺省情况。
VENDOR	可选字段，表示匹配设备厂商的类型。如果该字段为空，表示不匹配厂商类型。
HMAC	可选字段。配置文件的HMAC校验值，用于对加载的配置文件进行校验。该值为64位的字符串，是通过计算工具对U盘中的配置文件以HMAC-SHA256算法计算出的值。其中用作计算的密钥必须与在设备上通过**set device usb-deployment hmac-key**命令设置的HMAC密钥保持一致。 缺省情况下，不对配置文件进行校验。 **说明** 可通过HMAC-SHA256计算工具（如OpenSSL或者HashCalc）生成配置文件的HMAC值。 当U盘开局的升级文件中包含配置文件时，为提高安全性，建议通过命令**set device usb-deployment config-file password**配置加密和解密的密码，对配置文件按照标准zip格式压缩，压缩时指定密码，再保存至U盘，通过命令**set device usb-deployment hmac-key**命令配置U盘开局时HMAC校验功能的HMAC密钥，同时通过命令**set device usb-deployment hmac**使能HMAC校验功能。

字段	描述
DIRECTORY	可选字段。文件在U盘中存放的目录。 ● 此字段为空或不存在时，表示文件位于U盘根目录下。 ● DIRECTORY=/abc，表示文件位于U盘的abc文件夹下。 缺省情况下，DIRECTORY字段为空。 索引文件中文件目录的格式必须与设备的文件系统一致： ● 目录深度小于等于4级。目录必须以“/”开头，每一级目录以“/”隔开，但不能以“/”结束，例如/abc/test是合法目录，/abc/test/则是非法目录。 ● 每一级目录的字符串长度范围是1～15。 ● 目录名使用的字符不可以是空格、“~”、“*”、“/”、“\”、“:”、“'”、“"”、“<”、“>”、“|”、“?”、“[”、“]”、“%”等字符，目录名称不区分大小写。
SYSTEM-SOFTWARE	可选字段。系统软件名称，后缀名为“.cc”。 如果指定了此字段，则设备在拷贝系统软件前，会将此系统软件的版本号与设备正在运行的系统软件版本号比较，如果相同则不进行拷贝以及系统软件的升级。
SYSTEM-CONFIG	可选字段。配置文件名称，后缀名为“.cfg”或“.zip”。
SYSTEM-LICENSE	可选字段。License文件名称，后缀名为“.dat”。
SYSTEM-PAT	可选字段。补丁文件名称，后缀名为“.pat”。
SYSTEM-WEB	可选字段。Web网页文件名称，后缀名为“.web.7z”。

字段	描述
SYSTEM-SCRIPT	可选字段。表示脚本文件的名称。 可通过指定此字段，在U盘开局的同时，导入堆叠的相关配置。设备重启后，堆叠配置将会生效。 脚本文件以“.bat”为后缀，文件名长度为5～64个字符，格式与配置文件一致，“!”表示注释。脚本文件样例： # stack slot 0 renumber 2 !修改堆叠ID # interface stack-port 0/1 port interface xgigabitethernet 0/0/27 enable # interface stack-port 0/2 port interface xgigabitethernet 0/0/28 enable **说明** ● 不支持unix和linux系统编辑生成的脚本文件，因为此系统生成的文件内容设备无法识别。 ● U盘开局执行脚本文件下发配置错误时，无法进行回滚操作。可以通过改写脚本文件，修改错误配置并且删除已下发成功的配置，重新执行脚本文件实现U盘开局。 ● 如果脚本文件中包含非堆叠的配置命令且不会保存至配置文件中的命令，则此类命令在设备重启后会丢失。 ● 脚本文件的堆叠命令中，如果*slot-id*与当前设备的slot ID不一致，则会导致脚本文件执行失败。同时，当有**stack slot** *slot-id* **renumber** *new-slot-id*命令时，其他的堆叠命令中涉及*slot-id*的都需要和当前的*slot-id*一致。例如下面的脚本文件是错误的，当前设备的slot ID为0不是2，2是设备重启生效后的slot ID。 # stack slot 0 renumber 2 # interface stack-port 2/1 port interface XGigabitEthernet 2/0/1 enable ● 堆叠线的连接可以在U盘开局前也可以在完成U盘开局后进行。对于已经连接堆叠线的多个设备，如果导入脚本文件重启后成为堆叠系统非主设备时，不会在设备上生成U盘开局成功的报告。
SYSTEM-USERDEF1 SYSTEM-USERDEF2 SYSTEM-USERDEF3	可选字段。用户自定义文件。
END LSW	必选字段。文件结束标志。

说明

- 编写索引文件时，按照固定格式输入一行后必须回车换行后再进行新内容的编写，编写完成请注意保存索引文件。
- 如果某项关键字没有匹配或者没有搜索到，则认为该项的参数内容为空。

4.5 配置 U 盘开局

前置任务

设备上电，运行正常。

操作步骤

U盘开局之前，需要先制作U盘开局索引文件，然后将索引文件和需要加载的开局文件保存到U盘中，最后将U盘插入设备中启动U盘开局流程。

1. 执行命令**system-view**，进入系统视图。
2. 执行命令**undo set device usb-deployment disable**，使能设备的U盘开局功能。

   缺省情况下，U盘开局功能是去使能的。建议U盘开局结束后，将此功能关闭。但是如果设备是空配置设备，则U盘开局功能一直是使能的。
3. （可选）执行命令**set device usb-deployment config-file password** *password*，配置U盘开局时用于对配置文件进行加密和解密的密码。

   说明

   当U盘开局升级文件中包含配置文件时，为提高安全性，建议通过此命令配置密码，并将配置文件通过此密码按照标准zip格式压缩加密后保存至U盘。如果需要对配置文件进行HMAC校验，则必须要通过此步骤配置密码。

   如果是非空配置设备进行U盘开局，可以通过命令**set device usb-deployment password**配置U盘开局的认证密码。
4. （可选）执行命令**set device usb-deployment hmac-key**，配置U盘开局时HMAC校验功能的HMAC密钥。

   说明

   U盘开局时，如果使能了HMAC校验功能，则使用**set device usb-deployment hmac-key**命令配置的HMAC密钥计算需要加载的配置文件的HMAC值，然后将该值与索引文件中的“HMAC”字段值进行比较。如果一致，则文件合法，可以进行U盘开局；如果不一致，则文件非法，不能进行U盘开局。
5. （可选）执行命令**set device usb-deployment hmac**，使能配置文件的HMAC校验功能。

   说明

   用户在进行U盘开局时，如果升级文件中包含配置文件，可以对加载的配置文件进行HMAC校验，以保证文件的合法性。
6. 制作索引文件。

   具体的制作方法请参见**4.4 制作索引文件**。
7. 将制作好的索引文件保存到U盘根目录下。需要将此文件中定义的开局文件保存到指定目录，缺省为根目录。
8. 将U盘插入设备中，启动开局流程。

须知

由于设备为空配置设备，还没有相应的安全保证措施。因此当具体开局任务由开局现场非专业人员来进行时，请保证该人员不会对设备、U盘及开局文件进行非法操作。

- 进入开局流程后，系统首先按照smart_config.ini索引文件中的描述信息从U盘中获取开局文件拷贝到设备缺省的存储介质中。如果是堆叠环境，在主交换机拷贝完成后，会将这些文件拷贝至所有成员交换机上。
- 文件拷贝完成后，设备会根据索引文件中**ACTIVEMODE**字段指定的方式激活文件。
- 如果此次升级需要设备重启生效，则在重启前会延时10秒，在此时间内，设备USB灯黄色常亮。

通过指示灯查看 U 盘开局状态

S6735-S、S6720S-EI、S5720I-6X-PWH-SI-AC和S5720I-10X-PWH-SI-AC：通过SYS指示灯的状态，判断U盘开局进行的状态。

- 黄色慢闪（每2秒闪一次）：U盘开局成功。
- 绿色快闪（每秒闪四次）：U盘数据读取中。
- 红色快闪（每秒闪四次）：U盘开局失败。

通过USB指示灯的状态，判断U盘开局进行的状态（S5720I-6X-PWH-SI-AC和S5720I-10X-PWH-SI-AC除外）。

- 绿色常亮：U盘开局成功。
- 绿色快闪（每秒闪四次）：U盘数据读取中。
- 红色快闪（每秒闪四次）：U盘开局失败。
- 绿色慢闪：文件拷贝完成且校验成功，U盘可以拔出。
- 常灭：可能原因有U盘中无索引文件、未插U盘、USB接口损坏、指示灯坏、插入非开局U盘、重启过程中。

说明

- U盘开局成功后，系统会在U盘根目录下生成开局成功报告**usbload_verify.txt**文件。此时，可以拔出U盘，U盘开局结束。
- 如果U盘开局失败，系统也会在U盘根目录下生成错误报告**usbload_error.txt**文件，可以通过查看此文件定位失败原因。
- U盘开局结束后，建议执行**set device usb-deployment disable**命令，去使能设备的U盘开局功能，防止因U盘误插入而引起不必要的版本升级，导致业务中断。

4.6 U 盘开局配置举例

4.6.1 配置 U 盘开局示例

组网需求

在设备部署过程中，为了降低人工成本、节省部署的时间，用户希望为两台新设备实现自动升级及配置。需求如下：

- 设备升级时间为2013年07月28日02时09分。
- 第一台设备S5732-H从V200R022C00版本升级至较高版本，MAC地址为xxxx-xxxx-xxxx，系统软件名称S5732-H-new.CC，用户自定义文件userfile.txt，要求升级完成后，删除原有的系统软件。
- 第二台设备S5732-H从V200R022C00版本升级至较高版本，ESN号为020TEA10xxxxxxxx，系统软件名称为S5732-H-new.CC，需要加载的配置文件为vrpcfgnew.zip，补丁文件为patch.pat。

配置思路

采用如下思路配置：

1. 制作U盘开局索引文件smart_config.ini。
2. 将索引文件smart_config.ini和开局文件保存至U盘根目录下。
3. 将U盘插入设备的USB接口启动开局流程，实现设备自动完成软件升级。

操作步骤

步骤1 编辑U盘开局索引文件smart_config.ini。

新建一个索引文件，命名为“smart_config.ini”。索引文件的内容与格式如下：

```
BEGIN LSW
[GLOBAL CONFIG]
TIMESN=20130728.020900
[DEVICE0 DESCRIPTION]
MAC=xxxx-xxxx-xxxx
AUTODELFILE=YES
DEVICETYPE=S5732-H
SYSTEM-SOFTWARE=S5732-H-new.CC
SYSTEM-USERDEF1=userfile.txt
[DEVICE1 DESCRIPTION]
ESN=020TEA10xxxxxxxx
DEVICETYPE=S5732-H
SYSTEM-SOFTWARE=S5732-H-new.CC
SYSTEM-CONFIG=vrpcfgnew.zip
SYSTEM-PAT=patch.pat
END LSW
```

步骤2 将索引文件smart_config.ini及其他所有开局文件保存至U盘根目录下。

步骤3 将U盘插入S5732-H中启动开局流程，观察指示灯，监控U盘开局的状态。

设备重启后，系统检测开局状态：SYS指示灯黄色慢闪（每2秒闪一次），表示U盘开局成功；SYS指示灯红色闪烁，表示U盘开局失败，可查看U盘根目录下usbload_error.txt文件定位出错原因。

确认U盘开局成功后，拔出U盘，再插入另外一台待升级的设备中。

步骤4 将U盘插入S5735-L中启动开局流程，观察指示灯，监控U盘开局的状态。

设备重启后，系统检测开局状态：USB指示灯绿色常亮，表示U盘开局成功；USB指示灯红色快闪（每秒闪两次），表示U盘开局失败，可查看U盘根目录下usbload_error.txt文件定位出错原因。

确认U盘开局成功后，拔出U盘，U盘开局结束。

----结束

5 首次登录设备

5.1 首次登录设备简介
5.2 通过Console口首次登录设备
5.3 通过Web网管首次登录设备（传统管理模式设备）
5.4 通过Web网管首次登录设备（NETCONF模式设备）
5.5 配置系统基本信息
5.6 配置通过Console口首次登录设备后进行基本配置的示例

5.1 首次登录设备简介

要对一台新出厂的设备进行业务配置，通常需要本地登录设备。本地登录以后，完成设备名称、管理IP地址和系统时间等系统基本配置，并配置Telnet或STelnet协议实现远程登录。

设备支持的首次登录方式有：

- Console口登录
- Web网管登录

说明

配置Telnet或STelnet协议实现远程登录具体操作参见**配置通过Telnet登录设备**或**配置通过STelnet登录设备**。

相关信息

技术论坛

- **首次登录交换机**
- **通过Console口登录和Telnet登录**

视频

- **如何通过串口登录设备**

5.2 通过 Console 口首次登录设备

PC端通过设备的Console口登录，从而实现对首次上电的设备进行基本配置和管理。

前置任务

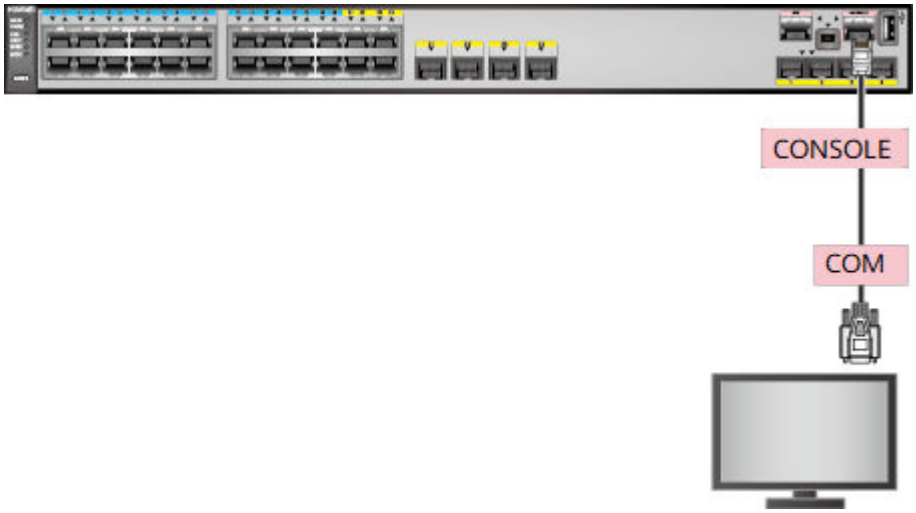
在配置通过Console口登录设备之前，需要完成以下任务：

- 设备正常上电。
- 准备好Console通信电缆。
- 准备好终端仿真软件。
  不同终端仿真软件的使用方法请参照具体软件的使用指导或联机帮助。

操作步骤

步骤1 将Console通信电缆的DB9（孔）插头插入PC机的串口（COM）中，再将RJ-45插头端插入设备的Console口中，如图5-1所示。

图 5-1 通过 Console 口连接设备



说明

如果维护终端（PC端）上没有DB9串口，可单独购买一根DB9串口转USB的转接线，将USB口连接到维护终端。

步骤2 在PC上打开终端仿真软件，新建连接，设置连接的接口以及通信参数。

设置终端软件的通信参数需与设备的缺省值保持一致，设置终端软件的通信参数如表5-1所示。

表 5-1 设备缺省值

参数	缺省值
传输速率	9600bit/s

参数	缺省值
流控方式	不进行流控
校验方式	不进行校验
停止位	1
数据位	8

说明

缺省情况下，设备不进行流控，而设备终端软件流控方式中RTS/CTS选项处于勾选状态，因此需要将该选项去掉勾选，否则终端界面无法输入命令行。

步骤3 终端界面会出现如下显示信息，提示用户设置密码。（以下显示信息仅为示意）

```
An initial password is required for the first login via the console.
Set a password and keep it safe. Otherwise you will not be able to login via the
console.

Please configure the login password (8-16)
Enter Password:
Confirm Password:
Warning: The authentication mode was changed to password authentication and the user level was
changed to 15 on con0 at the first user
login.
Warning: There is a risk on the user-interface which you login through. Please change the configuration of
the user-interface as soo
n as possible.

<HUAWEI>
```

- 为充分保证设备安全，请定期修改密码
- 采用交互方式输入的密码不会在终端屏幕上显示出来。

----结束

5.3 通过 Web 网管首次登录设备（传统管理模式设备）

背景信息

当用户需要对处于出厂配置状态的设备进行配置（设备出厂的管理模式为传统管理模式），且用户未携带Console通信电缆或者PC没有可用的串口时，可以通过Web网管首次登录设备并进行配置。

用户可以通过PC直连ETH管理接口或长按“MODE”按键两种方式实现通过Web网管首次登录设备。

- 对于有ETH管理接口的设备，支持PC直连ETH管理接口方式。
- 对于有“MODE”按键的设备，支持长按“MODE”按键方式。

说明

- 如果已使用MODE模式按键首次登录了设备（长按MODE按键6s或以上）并保存了配置，会清除ETH口上的默认配置。建议优先使用ETH口首次登录设备。
- Web网管首次登录设备与SVF、EasyDeploy、U盘开局功能互斥。

前置任务

通过Web网管首次登录设备之前，需要完成以下任务：

- 设备正常上电。
- 设备处于出厂配置状态。

缺省配置

表 5-2 设备的缺省配置

参数	缺省值
用户级别	15
登录IP地址	192.168.1.253 **说明** 出厂配置状态下，有ETH管理接口的设备上ETH管理接口的缺省IP地址为192.168.1.253。其他设备长按“MODE”按键后，系统默认在设备Vlanif1上配置缺省IP地址192.168.1.253。

操作步骤

步骤1 连接设备和PC。

说明

通过Web网管首次登录设备时，建议用户不要通过串口连接设备。通过串口进行任何操作，都将导致通过Web网管首次登录设备失败。

- 通过PC直连ETH管理接口首次登录设备。

  设备的ETH管理接口上存在缺省IP地址192.168.1.253/24，直接将设备的ETH管理接口和PC用网线进行连接。
- 通过长按“MODE”按键进入初始设置模式，实现首次登录设备。

  将设备的任意以太网电接口和PC用网线进行连接。长按“MODE”按键6s或以上，当设备所有的模式灯变为绿色常亮时，设备处于初始设置模式，此时系统默认在设备Vlanif1上配置缺省IP地址192.168.1.253/24。

说明

- 如果设备不是处于出厂配置状态，长按“MODE”按键6s后，所有模式灯处于绿色快闪状态，10s后模式灯恢复到原先状态，不影响设备原配置。
- 如果设备处于出厂配置状态，但是设备刚启动或者通过串口对设备进行了操作，那么长按“MODE”按键6s后，设备有可能进入初始设置模式失败。此时所有模式灯快速闪烁10s后，恢复到原先状态。
- 长按“MODE”按键6s，进入初始设置模式10分钟后，如果用户没有保存配置信息，设备将会自动退出初始设置模式，恢复出厂配置。

步骤2 配置PC的IP地址。

为了保证PC和设备之间路由可达，需要将PC的IP地址配置成与设备默认的IP地址在同一网段。

步骤3 通过Web网管登录设备。

在PC上打开浏览器，在地址栏中输入https://192.168.1.253，按回车键后将显示Web网管新建用户界面，如图5-2所示。在创建新用户后将自动跳转到Web网管登录界面，如图5-3所示。

说明

通过Web网管首次登录设备要求浏览器为Microsoft Edge、IE10.0、IE11.0、Firefox97.0～Firefox101.0或Chrome93.0～Chrome102.0。如果浏览器版本或浏览器补丁版本不在上述范围内，可能会出现Web页面显示异常，请及时更新浏览器和浏览器补丁。

首次登录Web网管，用户必须修改密码，只有这样才能进入Web网管系统主页面。

图 5-2 Web 网管新建用户界面

图 5-3 Web 网管首次登录界面

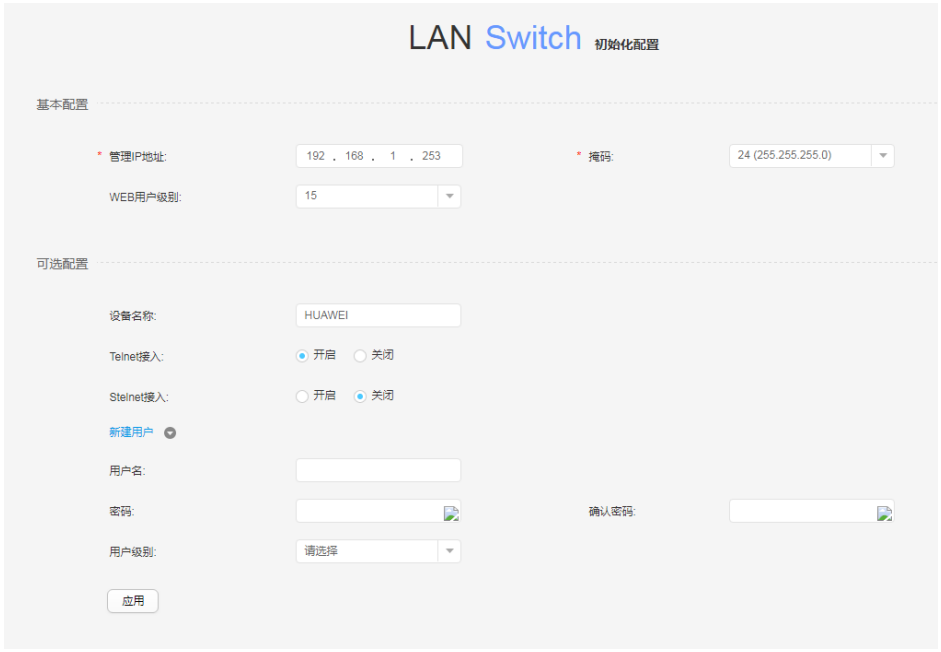
1. 输入已创建的用户名和密码。
2. 不同的登录方式的后续操作如下所示：
   - 若设备是通过PC直连ETH管理接口方式首次登录，此时直接进入Web网管配置界面，实现对设备的维护。
   - 若设备是通过长按“MODE”按键方式首次登录，此时进入Web初始化配置界面，如图5-4所示。

     单击“应用”，保存配置信息。

     退出Web网管初始化配置界面后，根据配置的管理IP地址，会出现以下两种情况：

     - 配置的管理IP地址与192.168.1.253/24在同一网段。在退出Web网管首次登录界面时，会直接跳转到通过Web网管登录的界面。
     - 配置的管理IP地址与192.168.1.253/24不在同一网段。在退出Web网管首次登录界面时，无法通过Web网管登录设备。此时需重新配置PC的IP地址，使得PC和设备之间路由可达。

图 5-4 Web 网管初始化配置界面



基本配置中信息含义如表5-3所示。配置完成后，用户可以通过Web网管登录设备。可选配置中信息含义如表5-4所示，配置完成后，用户可以通过Telnet或者STelnet登录设备。

说明

Telnet为不安全的协议，实际应用中建议使用Stelnet登录设备。

表 5-3 基本配置

配置项	说明
管理IP地址	指定设备的管理IP地址，点分十进制形式。 **说明** 为了防止网络中存在两台IP地址相同的设备，建议在首次登录之后，修改设备上的缺省IP地址。
掩码	下拉列表框中选择子网掩码。
WEB用户级别	下拉列表框中选择用户级别。 Web用户分为两个级别，管理用户和监控用户。当用户级别配置在3级或3级以上，具有管理级权限，为Web网管的管理用户。3级以下的用户为Web网管的监控用户。管理用户有所有Web页面的操作权限，监控用户只有Ping和Trace Route的操作权限。

表 5-4 可选配置

配置项	说明
设备名称	指定设备名称。 设备名称中不能出现“?”，且空格不能放在开头。
Telnet接入	设置Telnet功能：开启/关闭Telnet功能。
Stelnet接入	设置STelnet功能：开启/关闭STelnet功能。
用户名	输入新建Telnet或者STelnet登录用户名。 用户名中不能出现“/”、“:”、“*”、“?”、“"”、“<”、“>”、“|”、“'”和“%”等字符，且“@”不能在首位。

配置项	说明
密码	输入密码。 为提升密码安全性，密码至少同时包含小写字母、大写字母、数字、特殊符号（例如“!”、“$”、“#”和“%”等）这四种形式中的两种，并且不能包括空格和单引号。
确认密码	再次输入密码。 格式与“密码”保持一致。
用户级别	下拉列表框中选择用户级别。 Web用户分为两个级别，管理用户和监控用户。当用户级别配置在3级或3级以上，具有管理级权限，为Web网管的管理用户。3级以下的用户为Web网管的监控用户。管理用户有所有Web页面的操作权限，监控用户只有Ping和Trace Route的操作权限。

----结束

5.4 通过 Web 网管首次登录设备（NETCONF 模式设备）

背景信息

NETCONF模式下的设备与传统管理模式下的设备，在通过Web网管首次登录时是有差别的。设备被切换成了NETCONF模式后，可以通过本节内容实现Web网管首次登录。

用户可以通过PC直连ETH管理接口或长按“MODE”按键两种方式实现通过Web网管首次登录设备。

- 对于有ETH管理接口的设备，支持PC直连ETH管理接口方式。
- 对于有“MODE”按键的设备，支持长按“MODE”按键方式。

说明

- 如果已使用MODE模式按键首次登录了设备（长按MODE按键6s或以上）并保存了配置，会清除ETH口上的默认配置。建议优先使用ETH口首次登录设备。
- Web网管首次登录设备与SVF、EasyDeploy、U盘开局功能互斥。

前置任务

通过Web网管首次登录设备之前，需要完成以下任务：

- 设备正常上电。
- 设备处于出厂配置状态。

缺省配置

表 5-5 设备的缺省配置

参数	缺省值
用户级别	15
登录IP地址	192.168.1.253 **说明** • 出厂配置状态下，有ETH管理接口的设备上ETH管理接口的缺省IP地址为192.168.1.253。其他设备长按“MODE”按键后，系统默认在设备Vlanif4094上配置缺省IP地址192.168.1.253。 • 为了防止网络中存在两台IP地址相同的设备，建议在首次登录之后，修改设备上的缺省IP地址。

操作步骤

步骤1 连接设备和PC。

说明

通过Web网管首次登录设备时，建议用户不要通过串口连接设备。通过串口进行任何操作，都将导致通过Web网管首次登录设备失败。

- 通过PC直连ETH管理接口首次登录设备。

  设备的ETH管理接口上存在缺省IP地址192.168.1.253/24，直接将设备的ETH管理接口和PC用网线进行连接。

- 通过长按“MODE”按键进入初始设置模式，实现首次登录设备。

  将设备的第一个以太网电接口和PC用网线进行连接。长按“MODE”按键6s或以上，当设备所有的模式灯变为绿色常亮时，设备进入初始设置模式，此时系统默认在设备Vlanif4094上配置缺省IP地址192.168.1.253/24。

说明

- 如果设备不是处于出厂配置状态，长按“MODE”按键6s后，所有模式灯处于绿色快闪状态，10s后模式灯恢复到原先状态，不影响设备原有配置。
- 如果设备处于出厂配置状态，但是设备刚启动或者通过串口对设备进行了操作，那么长按“MODE”按键6s后，设备有可能进入初始设置模式失败。此时所有模式灯快速闪烁10s后，恢复到原先状态。
- 长按“MODE”按键6s，进入初始设置模式1小时后，如果用户没有保存配置信息，设备将会自动退出初始设置模式，恢复出厂配置。

步骤2 配置PC的IP地址。

为了保证PC和设备之间路由可达，需要将PC的IP地址配置成与设备默认的IP地址在同一网段。

步骤3 通过Web网管登录设备。

在PC上打开浏览器，在地址栏中输入https://192.168.1.253，按回车键后将显示Web网管新建用户界面，如图5-5所示。在创建新用户后将自动跳转到Web网管登录界面，如图5-6所示。

说明

通过Web网管首次登录设备要求浏览器为Microsoft Edge、IE10.0、IE11.0、Firefox97.0～Firefox101.0或Chrome93.0～Chrome102.0。如果浏览器版本或浏览器补丁版本不在上述范围内，可能会出现Web页面显示异常，请及时更新浏览器和浏览器补丁。

首次登录Web网管，用户必须修改密码，只有这样才能进入Web网管系统主页面。

图 5-5 Web 网管新建用户界面

图 5-6 Web 网管首次登录界面

1. 输入已创建的用户名和密码，并单击“登录”或直接按回车键进入Web网管界面。
2. 不同的登录方式的后续操作如下所示：

- 若设备是通过PC直连ETH管理接口方式首次登录，此时直接进入Web网管配置界面，实现对设备的维护。
- 若设备是通过长按“MODE”按键方式首次登录，此时进入Web初始化配置界面，如图5-7所示。

  单击“应用”，保存配置信息，在退出初始化配置界面后，直接跳转到通过Web网管登录的界面。用户再次登录后实现对设备的维护。

图 5-7 初始化配置界面

说明

在初始化配置界面勾选配置管理方式，点击应用，设备将自动配置其他管理方式。

----结束

5.5 配置系统基本信息

背景信息

本章节介绍了交换机的基本系统参数的设置方法。以下是本页面中所涉及的任务：

1. 设置系统名称。
2. 设置设备所在地区和时区。
3. 配置设备的日期和时间。
4. 查看设备的日期和时间。
5. 配置设备管理IP地址和缺省网关。
6. 查看IP路由信息。
7. 配置STelnet协议实现登录设备。
8. 查看当前设备配置信息。

操作步骤

步骤1 执行命令**sysname** *host-name*，设置设备名称。

```
<HUAWEI> system-view
[HUAWEI] sysname Switch
[Switch] undo sysname    //恢复主机名到缺省情况
```

步骤2 执行命令**clock timezone**，配置设备所在地区及其对应的时区。

```
[HUAWEI] clock timezone Beijing add 08:00:00
[HUAWEI] quit
```

步骤3 执行命令**clock datetime**设置当前时间和日期。

```
<HUAWEI> clock datetime 08:00:00 2018-12-01
```

步骤4 执行命令**display clock**，查看系统当前日期和时钟。

```
<HUAWEI> display clock
2018-12-01 08:02:30+08:00
Saturday
Time Zone(Beijing) : UTC+08:00
```

步骤5 执行命令**ip address**，配置设备管理IP地址，执行命令**ip route-static**，配置设备缺省网关。

- 对于有管理网口的设备，在管理网口下配置管理IP地址。

  ```
  <HUAWEI> system-view
  [HUAWEI] interface MEth 0/0/1
  [HUAWEI-MEth0/0/1] ip address 10.10.10.2 255.255.255.0    //设备管理IP
  [HUAWEI-MEth0/0/1] quit
  [HUAWEI] ip route-static 0.0.0.0 0 10.10.10.1    //设备缺省网关
  ```

- 对于没有管理网口的设备，在Vlanif接口下配置管理IP地址。

  ```
  <HUAWEI> system-view
  [HUAWEI] interface Vlanif 10
  [HUAWEI-Vlanif10] ip address 10.10.10.2 255.255.255.0    //设备管理IP
  [HUAWEI-Vlanif10] quit
  [HUAWEI] ip route-static 0.0.0.0 0 10.10.10.1    //设备缺省网关
  ```

步骤6 执行命令**display ip interface brief**，查看接口上IP地址的简要信息。执行命令**display ip routing-table**，查看IP路由信息。

```
[HUAWEI] display ip interface brief
*down: administratively down
^down: standby
(l): loopback
(s): spoofing
(E): E-Trunk down
The number of interface that is UP in Physical is 2
The number of interface that is DOWN in Physical is 1
The number of interface that is UP in Protocol is 2
The number of interface that is DOWN in Protocol is 1

Interface                   IP Address/Mask      Physical   Protocol
NULL0                       unassigned           up         up(s)
Vlanif10                    10.10.10.2/24        up         up

[HUAWEI] display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 5        Routes : 5

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        0.0.0.0/0   Static  60   0           RD  10.10.10.1      Vlanif10
       10.0.0.0/8   Direct  0    0           D   10.0.0.1        InLoopBack0
       10.0.0.1/32  Direct  0    0           D   10.0.0.1        InLoopBack0
   10.10.10.0/24    Direct  0    0           D   10.10.10.2      Vlanif10
   10.10.10.2/32    Direct  0    0           D   10.0.0.1        Vlanif10
```

步骤7 执行命令**ssh user**，配置SSH用户相关参数；执行命令**local-user**，配置本地用户相关参数，实现通过SSH协议登录设备。

```
<HUAWEI> system-view
[HUAWEI] user-interface vty 0 4
[HUAWEI-ui-vty0-4] authentication-mode aaa    //配置VTY用户认证方式为AAA认证
[HUAWEI-ui-vty0-4] protocol inbound ssh    //VTY用户界面所支持的协议缺省为SSH协议。
[HUAWEI-ui-vty0-4] quit
[HUAWEI] aaa
[HUAWEI-aaa] local-user admin password irreversible-cipher YsHsjx_202206    //创建与SSH用户同名的本地用户和对应的登录密码
[HUAWEI-aaa] local-user admin service-type ssh terminal    //配置本地用户的服务方式
[HUAWEI-aaa] local-user admin privilege level 15    //配置本地用户级别
[HUAWEI-aaa] quit
[HUAWEI] ssh user admin    //创建SSH用户
[HUAWEI] ssh user admin authentication-type password    //配置SSH用户的认证方式为password
[HUAWEI] ssh user admin service-type stelnet    //配置SSH用户的服务方式
[HUAWEI] ssh server-source -i Vlanif 10    //对于有管理网口的设备，则服务器端的源接口配置为管理网口。
[HUAWEI] stelnet server enable    //使能设备的STelnet服务器功能
```

说明

确保SSH用户名称与本地用户名称相同。

本页面只介绍了使用Password认证方式实现通过STelnet协议登录设备。更多配置Telnet或STelnet协议实现远程登录的详细操作参见**配置通过Telnet登录设备**或**配置通过STelnet登录设备**。

步骤8 执行命令**display current-configuration**，查看设备当前配置。

```
<HUAWEI> system-view
[HUAWEI] display current-configuration | include ip
 ip address 10.10.10.2 255.255.255.0
ip route-static 0.0.0.0 0.0.0.0 10.10.10.1
```

----结束

查询系统信息的命令

可以使用如下命令查询系统信息：

- **display current-configuration**，查看系统配置。
- **display interface brief**，查看接口摘要信息。
- **display clock**，查看系统当前日期和时钟。
- **display ip interface brief**，查看接口上IP地址的简要信息。
- **display ip routing-table**，查看系统路由信息。
- **display user-interface**，查看用户界面的物理属性和配置。
- **display local-user**，查看本地用户列表。
- **display ssh user-information**，在SSH服务器端查看SSH用户信息。
- **display ssh server status**，查看SSH服务器的全局配置信息。
- **display ssh server session**，查看与SSH客户端连接的会话信息。

5.6 配置通过 Console 口首次登录设备后进行基本配置的示例

组网需求

通过Console口首次登录设备后，对设备进行基本配置并配置通过Telnet远程管理的0～4号用户的级别为15级，认证方式为AAA认证。PC2与设备之间路由可达。

图 5-8 通过 Console 口首次登录设备后进行基本配置组网图

配置思路

1. 通过Console口登录设备。
2. 对设备进行基本配置。

操作步骤

步骤1 PC1通过设备Console口登录设备，具体操作请参见**通过Console口首次登录设备**

步骤2 对设备进行基本配置

设置系统的日期、时间和时区。

```
<HUAWEI> clock timezone BJ add 08:00:00
<HUAWEI> clock datetime 20:20:00 2018-08-08
```

说明

在配置设备的当前时间和日期前，需要执行**clock timezone**命令配置时区。如果不配置时区，执行**clock datetime**命令配置的是UTC时间。

设置设备名称和管理IP地址。

```
<HUAWEI> system-view
[HUAWEI] sysname Server
[Server] vlan 10
[Server-vlan10] quit
[Server] interface vlanif 10
[Server-Vlanif10] ip address 10.137.217.177 24
[Server-Vlanif10] quit
[Server] interface gigabitethernet 0/0/10
[Server-GigabitEthernet0/0/10] port link-type access
[Server-GigabitEthernet0/0/10] port default vlan 10
[Server-GigabitEthernet0/0/10] quit
```

假如设备的网关是10.137.217.1，配置设备的缺省路由。

```
[Server] ip route-static 0.0.0.0 0 10.137.217.1
```

开启STelnet服务器功能，配置SSH用户认证方式为Password。

```
[Server] stelnet server enable
[Server] ssh user sys-admin service-type stelnet
[Server] ssh user sys-admin authentication-type password
[Server] ssh server-source all-interface
[Server] user-interface vty 0 4
[Server-ui-vty0-4] protocol inbound ssh
[Server-ui-vty0-4] authentication-mode aaa
[Server-ui-vty0-4] quit
```

设置Telnet用户的级别和认证方式。

```
[Server] telnet server-source -i Vlanif 10
[Server] telnet server enable
[Server] user-interface vty 0 4
```

```
[Server-ui-vty0-4] protocol inbound telnet
[Server-ui-vty0-4] authentication-mode aaa
[Server-ui-vty0-4] user privilege level 15
[Server-ui-vty0-4] quit
[Server] aaa
[Server-aaa] local-user admin1234 password irreversible-cipher YsHsjx_202206
[Server-aaa] local-user admin1234 privilege level 15
[Server-aaa] local-user admin1234 service-type telnet
[Server-aaa] quit
```

步骤3 验证配置结果

完成以上配置后，可以从PC2以Telnet方式远程管理设备。

进入Windows的命令行提示符，并执行以下命令，通过Telnet方式登录设备。

```
C:\Documents and Settings\Administrator> telnet 10.137.217.177
```

说明

当所处环境不足够安全时，建议选择较安全的STelnet接入方式登录设备，具体配置案例请参见**配置通过STelnet登录设备**。

按“Enter”键后，在登录窗口输入用户名和密码，验证通过后，出现用户视图的命令行提示符。（以下显示信息仅为示意）

```
Login authentication


Username:admin1234
Password:
Info: The max number of VTY users is 20, and the number
      of current VTY users on line is 1.
      The current login time is 2012-07-26 20:10:05+08:00.
<Server>
```

----结束

配置文件

Switch的配置文件

```
#
sysname Server
#
telnet server enable
telnet server-source -i Vlanif 10
#
clock timezone BJ add 08:00:00
#
aaa
 local-user admin1234 password irreversible-cipher $1a$aVW8S=aP=B<OWi1Bu'^R[=_!~oR*85r_nNY+kA(I}
[TiLiVGR-i/'DFGAI-O$
 local-user admin1234 privilege level 15
 local-user admin1234 service-type telnet
#
interface Vlanif10
 ip address 10.137.217.177 255.255.255.0
#
interface GigabitEthernet0/0/10
 port link-type access
 port default vlan 10
#
ip route-static 0.0.0.0 0.0.0.0 10.137.217.1
#
user-interface vty 0 4
 authentication-mode aaa
 user privilege level 15
```



```
 protocol inbound telnet
#
return
```

相关信息

技术论坛

- **首次登录交换机**

视频

- **如何通过串口登录设备**

6 登录设备命令行界面

6.1 登录方式介绍
6.2 用户界面介绍
6.3 用户认证方式和用户级别介绍
6.4 配置通过Console口登录设备
6.5 配置通过Telnet登录设备
6.6 配置通过STelnet登录设备
6.7 （可选）配置ACL限制用户通过Telnet/STelnet登录设备
6.8 命令行配置设备登录后的常用操作
6.9 登录设备命令行的配置举例
6.10 登录设备命令行界面失败处理办法
6.11 登录设备FAQ

6.1 登录方式介绍

用户对设备的管理方式有命令行方式（即CLI方式）和Web网管方式两种。

- 命令行方式

  通过Console口（也称串口）、Telnet或STelnet方式登录设备的命令行界面后，使用设备提供的命令行对设备进行管理和配置。此种方式需要配置相应登录方式的用户界面。

- Web网管方式

  设备通过内置的Web服务器提供图形化的操作界面，以方便用户直观方便地管理和维护设备。此方式仅可实现对设备部分功能的管理与维护，如果需要对设备进行较复杂或精细的管理，仍然需要使用命令行方式。

  Web网管方式的详细介绍，请参见**登录设备Web网管界面**。

用户可以通过**表6-1**所示方式登录设备命令行界面，对设备进行配置和管理。

表 6-1 用户登录方式（设备命令行界面）

登录设备方式	优点	缺点	应用场景	说明
通过Console口登录	使用专门的Console通信线缆(也称串口线)连接，保证可以对设备有效控制。	不能远程接入维护设备。	• 当对设备进行第一次配置时，可以通过Console口登录设备进行配置。 • 当用户无法进行远程接入设备时，可通过Console口进行本地登录。	通过Console口进行本地登录是登录设备最基本的方式，也是其他登录方式的基础。 缺省情况下，用户可以直接通过Console口本地登录设备，用户级别是15。
通过Telnet登录	• 便于对设备进行远程管理和维护。 • 不需要为每一台设备都连接一个终端，方便用户的操作。	传输过程采用TCP协议进行明文传输，存在安全隐患。	终端连接到网络上，使用Telnet方式登录设备，进行远程的配置。应用在对安全性要求不高的网络。	缺省情况下，用户不能通过Telnet方式直接登录设备。如果需要通过Telnet方式登录设备，可以先通过Console口本地登录设备。
通过STelnet登录	SSH（Secure Shell）协议实现在不安全网络上提供安全的远程接入，保证了数据的完整性和可靠性，保证了数据的安全传输。 **说明** 如不特别指出，本文中SSH即指SSH2.0。	配置较复杂。	如果网络对于安全性要求较高，可以通过STelnet方式登录设备。STelnet基于SSH协议，提供安全的信息保障和强大认证功能，保护设备不受IP欺骗等攻击。	缺省情况下，用户不能通过STelnet方式直接登录设备。如果需要通过STelnet方式登录设备，可以先通过Console口本地登录或Telnet远程接入设备。

6.2 用户界面介绍

当用户登录设备命令行界面时，系统会分配一个用户界面用来管理、监控设备和用户间的当前会话。每个用户界面有对应的用户界面视图（User-interface view），在用户界面视图下网络管理员可以配置一系列参数，比如认证模式、用户级别等，当用户使

用该用户界面登录的时候，将受到这些参数的约束，从而达到统一管理各种用户会话连接的目的。

设备支持两种类型的用户界面进行配置：

- Console用户界面：用来管理和监控通过Console口登录的用户。设备提供Console口，端口类型为EIA/TIA-232 DCE。用户终端的串行口可以与设备Console口直接连接，实现对设备的本地访问。
- 虚拟类型终端VTY（Virtual Type Terminal）用户界面：用来管理和监控通过VTY方式登录的用户。用户通过终端与设备建立Telnet或STelnet连接后，即建立了一条VTY通道。目前每台设备最多支持15个VTY用户同时访问。

说明

- LTT用户界面：集群场景下，从非主交换机Console口登录设备的用户界面类型，不支持配置。
- WEB用户界面：通过Web网管方式登录设备的用户界面类型，不支持配置。

用户与用户界面的关系

用户界面与用户并没有固定的对应关系。用户界面的管理和监控对象是使用某种方式登录的用户，虽然单个用户界面某一时刻只有一个用户使用，但它并不针对某个用户。

用户登录时，系统会根据用户的登录方式，自动给用户分配一个当前空闲的、编号最小的某类型的用户界面，整个登录过程将受该用户界面视图下配置的约束。比如用户A使用Console口登录设备时，将受到Console用户界面视图下配置的约束，当使用VTY 1登录设备时，将受到VTY 1用户界面视图下配置的约束。同一用户登录的方式不同，分配的用户界面不同；同一用户登录的时间不同，分配的用户界面可能不同。

说明

- 当配置VTY用户界面最大个数为0时，任何用户（Telnet、SSH用户）都无法通过VTY登录到设备，Web用户也无法通过Web网管登录设备。
- 当配置的VTY类型用户界面的最大个数小于当前在线用户的数量，系统会将目前未通过认证且占用VTY通道时间超过15秒的用户下线，新用户此时可以通过VTY登录到设备。
- 当配置的VTY类型用户界面的最大个数大于当前最多可以登录用户的数量，就必须为新增加的用户界面配置验证方式。
- 使用VTY通道登录设备时，为防止VTY连接数量超限导致用户无法接入，用户可执行如下操作查看并配置允许通过VTY通道登录的用户数。
  1. 执行命令**display user-interface maximum-vty**查看设备允许通过VTY连接登录设备的最大用户数。
  2. 执行命令**display user-interface**查看用户界面信息。其中，“+”表示被占用的通道。如果通道被占满，会导致后续用户无法登录，如果已登录用户登出后，可能会因为通道被其他用户占用而无法再次登录成功。此时，执行命令**user-interface maximum-vty** *number*设置允许登录的最大用户数目。
- 如果某VTY用户界面两次出现设备长时间不响应的情况，该VTY用户界面将被锁定，用户可以通过其他VTY用户界面登录，设备重启后可恢复。

用户界面的编号

用户界面的编号包括以下两种方式：

- 相对编号

  相对编号方式的形式是：用户界面类型 + 编号。

此种编号方式只能唯一指定某种类型的用户界面中的一个或一组。相对编号方式遵守的规则如下：

- Console用户界面的编号：CON 0。堆叠场景下，从非主交换机串口登录时，显示LTT 0。
- VTY用户界面的编号：第一个为VTY 0，第二个为VTY 1，依此类推。

- 绝对编号

  使用绝对编号方式，可以唯一的指定一个用户界面或一组用户界面。使用命令**display user-interface**可查看到设备当前支持的用户界面以及它们的绝对编号。

  对于一台设备，Console口用户界面只有一个，但VTY类型的用户界面有20个，可以在系统视图下使用**user-interface maximum-vty**命令设置最大用户界面个数，其缺省值为5。VTY 16～VTY 20一直存在于系统中，不受**user-interface maximum-vty**命令的控制。

  缺省情况下，Console、VTY用户界面在系统中的绝对编号，如表6-2所示。

表 6-2 用户界面的绝对、相对编号说明

用户界面	说明	绝对编号	相对编号
Console用户界面	用来管理和监控通过Console口登录的用户。	0	0
VTY用户界面	用来管理和监控通过Telnet或STelnet方式登录的用户。	34～48，50～54。 其中49保留，50～54为网管预留编号。	第一个为VTY 0，第二个为VTY 1，依此类推。缺省存在VTY 0～4通道。 ● 绝对编号34～48对应相对编号VTY 0～VTY 14 ● 绝对编号50～54对应相对编号VTY 16～VTY 20 其中VTY 15保留，VTY 16～VTY 20为网管预留编号。 只有当VTY0～VTY14全部被占用，且用户配置了AAA认证的情况下才可以使用VTY16～VTY20。

用户界面的用户认证与用户级别

配置用户界面的用户认证与用户级别参见6.3 用户认证方式和用户级别介绍。

6.3 用户认证方式和用户级别介绍

用户界面的认证方式

Console、Telnet登录用户的认证方式直接由用户界面中配置的认证方式决定。用户界面的认证方式有以下三种：

- AAA认证：登录时需输入用户名和密码。设备根据配置的AAA用户名和密码验证用户输入的信息是否正确，如果正确，允许登录，否则拒绝登录。
- Password认证：也称密码认证，登录时需输入正确的认证密码。如果用户输入的密码与设备配置的认证密码相同，允许登录，否则拒绝登录。
- None认证：也称不认证，登录时不需要输入任何认证信息，可直接登录设备。

须知

如果配置认证方式为不认证，任何用户不需要输入用户名和密码就会认证成功。因此，为保护设备或网络安全，建议不要使用None认证和方式，如需使用，需要安装空口令认证插件。

您可以通过华为官网（**企业**、**运营商**）搜索“插件使用指南”，请根据交换机型号及软件版本选择相应的《插件使用指南》。如无权限，请联系技术支持人员。

无论何种验证方式，当用户登录设备失败时，系统会启动延时登录机制。首次登录失败后，延时5秒才可再次登录，后续登录失败次数每增加一次，延时时间增加5秒，即第2次登录失败延时10秒，第3次登录失败延时15秒。

SSH 用户的认证方式

通过STelnet登录设备需配置用户界面支持的协议是SSH，必须设置用户界面认证方式为AAA认证。但SSH用户的认证方式由SSH支持的认证方式决定，SSH支持Password、RSA、DSA、ECC、Password-RSA、Password-DSA、Password-ECC和ALL，8种认证方式。

- Password认证：是一种基于“用户名+口令”的认证方式。通过AAA为每个SSH用户配置相应的密码，在通过SSH登录时，输入正确的用户名和密码就可以实现登录。
- RSA（Revest-Shamir-Adleman Algorithm）认证：是一种基于客户端私钥的认证方式。RSA是一种公开密钥加密体系，基于非对称加密算法。RSA密钥也是由公钥和私钥两部分组成，在配置时需要将客户端生成的RSA密钥中的公钥部分拷贝输入至服务器中，服务器用此公钥对数据进行加密。
- DSA（Digital Signature Algorithm）认证：是一种类似于RSA的认证方式，DSA认证采用数字签名算法进行加密。
- ECC（Elliptic Curve Cryptography）认证：是一种椭圆曲线算法，与RSA相比，在相同安全性能下密钥长度短、计算量小、处理速度快、存储空间小、带宽要求低。
- Password-RSA认证：SSH服务器对登录的用户同时进行密码认证和RSA认证，只有当两者同时满足情况下，才能认证通过。
- Password-DSA认证：SSH服务器对登录的用户同时进行密码认证和DSA认证，只有当两者同时满足情况下，才能认证通过。
- Password-ECC认证：SSH服务器对登录的用户同时进行密码认证和ECC认证，只有当两者同时满足情况下，才能认证通过。
- ALL认证：SSH服务器对登录的用户进行公钥认证或密码认证，只要满足其中任何一个，就能认证通过。

用户级别

系统支持对登录用户进行分级管理，用户所能访问命令的级别由用户的级别决定。用户级别由用户界面或AAA本地用户的认证方式决定，具体细节如表6-3所示。

表 6-3 不同登录设备方式的用户级别

登录设备方式	用户接入的认证方式	用户级别决定因素	配置命令
通过Console口登录 通过Telnet登录	用户界面：AAA认证	AAA本地用户级别	**local-user** *user-name* **privilege level** *level*
	用户界面：Password认证	用户界面级别	**user privilege level** *level*
通过STelnet登录	SSH用户的认证方式：Password认证	AAA本地用户级别	**local-user** *user-name* **privilege level** *level*
	SSH用户的认证方式：RSA认证、DSA认证、ECC认证	用户界面级别	**user privilege level** *level*
	SSH用户的认证方式：password-rsa认证、password-dsa认证和password-ecc认证	AAA本地用户级别	**local-user** *user-name* **privilege level** *level*
	SSH用户的认证方式：All认证	根据需要进行部署。 **说明** 如果SSH用户认证方式为all认证，且存在一个同名AAA用户，那通过Password认证、RSA认证、DSA认证或者ECC认证接入时用户优先级可能不同，由登录时的实际认证情况决定。	-

用户级别与命令级别的关系

命令的级别由低到高分为参观级、监控级、配置级和管理级四种，分别对应级别值0、1、2、3，用户级别与命令级别的对应关系如表6-4所示。

表 6-4 用户级别与命令级别的对应关系

用户级别	命令级别	级别名称	说明
0	0	参观级	网络诊断工具命令（ping、tracert）、从本设备出发访问外部设备的命令（Telnet客户端）等。
1	0、1	监控级	用于系统维护，包括display等命令。 **说明** 并不是所有display命令都是监控级，比如**display current-configuration**命令和**display saved-configuration**命令是3级管理级。
2	0、1、2	配置级	业务配置命令。
3～15	0、1、2、3	管理级	用于系统基本运行的命令，对业务提供支撑作用，包括文件系统、FTP、TFTP下载、用户管理命令、命令级别设置命令、用于业务故障诊断的debugging命令等。

说明

默认情况下，3～15级用户具有相同的管理员权限，部分特殊命令行请参照命令行实现说明。

6.4 配置通过 Console 口登录设备

Console口本地登录设备是一种权限很高的管理设备方式，当用户无法进行远程登录设备时，可通过电脑直连Console口进行本地登录。

通过 Console 口登录设备的常用功能配置

缺省情况下，用户可以直接通过首次登录的用户名和修改后的密码登录设备，而无需做额外配置。如果需要增加新的Console用户或修改用户信息，配置步骤如下：

1. 配置Console用户界面的认证方式。
2. 配置Console用户的认证信息及用户级别。

操作步骤

步骤1 配置Console用户界面的认证方式。

- 配置Console用户界面的认证方式为AAA：

  选择AAA认证，需要配置AAA用户的认证信息、接入类型和用户级别。

```
<HUAWEI> system-view
[HUAWEI] user-interface console 0    //进入Console用户界面
[HUAWEI-console0] authentication-mode aaa    //配置认证方式为AAA
[HUAWEI-console0] quit
```

- 配置Console用户界面的认证方式为Password：

  选择password认证，直接配置VTY用户界面的级别和登录密码。


```
<HUAWEI> system-view
[HUAWEI] user-interface console 0    //进入Console用户界面
[HUAWEI-console0] authentication-mode password    //配置Console用户界面的认证方式为Password
```

说明

- 实际场景中建议使用AAA认证。
- 如果用户通过Console口登录设备再进行Console用户界面配置，所配置的属性需退出当前登录，再次通过Console口登录才会生效。
- 为充分保证设备安全，请定期修改密码。

步骤2 配置Console用户的认证信息及用户级别。

- 配置Console用户的认证方式为AAA：

  选择AAA认证，需要配置AAA用户的认证信息、接入类型和用户级别。

```
[HUAWEI] aaa
[HUAWEI-aaa] local-user admin123 password irreversible-cipher YsHsjx_202206    //创建本地用户admin123，登录密码为YsHsjx_202206
[HUAWEI-aaa] local-user admin123 privilege level 15    //配置本地用户admin123的级别为15
Warning: This operation may affect online users, are you sure to change the user privilege level ?[Y/N]y
[HUAWEI-aaa] local-user admin123 service-type terminal    //配置本地用户admin123的接入类型为终端用户，即Console用户
```

- 配置Console用户的认证方式为Password：

  选择password认证，直接配置VTY用户界面的级别和登录密码。

```
[HUAWEI-console0] set authentication password cipher YsHsjx_202206    //配置登录密码为YsHsjx_202206。缺省情况下，Console口用户界面下用户的级别是15。
```

步骤3 通过Console口连接设备，输入Enter键后，在登录窗口输入AAA验证方式配置的登录用户名和密码，实现Console口登录设备。（本举例配置的用户名为admin123，密码为abcd@123）

```
Login authentication


Username:admin123
Password:
<HUAWEI>
```

----结束

检查配置结果

- 执行**display users** [**all**]命令，查看用户界面的用户登录信息。
- 执行**display user-interface console 0**命令，查看用户界面信息。
- 执行**display local-user**命令，查看本地用户的属性信息。
- 执行**display access-user**命令，查看在线连接的用户信息。

命令行功能说明

详细的命令行功能说明请参见《命令参考》手册。

表 6-5 常见功能命令

功能	配置命令	说明
Console用户界面的认证方式	**authentication-mode** { **aaa** | **password** }	缺省为Password认证。 如果选择**aaa**，需要配置AAA本地用户相关信息，包括： • **local-user** *user-name* { **password** { **cipher** | **irreversible-cipher** } *password*，创建本地用户，并配置本地用户的密码。 • **local-user** *user-name* { **privilege level** *level* }，配置本地用户的级别。 • **local-user** *user-name* **service-type** { **http** | **ssh** | **telnet** | **terminal** } *，配置本地用户的接入类型。
配置Console用户界面的登录密码	**set authentication password** [**cipher** *password*]	如果认证方式选择**password**，则需要使用该命令设置认证密码。
配置Console用户界面的用户级别	**user privilege level** *level*	缺省为15。 该命令设置的级别对AAA用户无效，AAA用户由AAA配置信息中本地用户的级别决定。

表 6-6 其他功能命令

功能	配置命令	说明
关闭Console口登录功能	**console0 disable**	Console口登录功能缺省开启。
Console用户界面的流控方式	**flow-control** { **hardware** | **none** | **software** }	缺省为none，即不进行流控。
Console用户界面的数据位	**databits** { **5** | **6** | **7** | **8** }	缺省为8位。
Console用户界面的校验位	**parity** { **even** | **mark** | **none** | **odd** | **space** }	缺省为none，即不进行校验。
Console用户界面的停止位	**stopbits** { **1** | **1.5** | **2** }	缺省为1位。

功能	配置命令	说明
Console用户界面的传输速率	**speed** *speed-value*	缺省为9600bit/s。
Console用户界面的登录连接超时时间	**idle-timeout** *minutes* [*seconds*]	缺省为10分钟。
Console用户界面的终端屏显的行数	**screen-length** *screen-length*	缺省为24行。
Console用户界面的终端屏显的列数	**screen-width** *screen-width*	缺省为80列。
Console用户界面的历史命令缓冲区的大小	**history-command max-size** *size-value*	缺省为10条。

6.5 配置通过 Telnet 登录设备

使用Telnet方式，管理员可以简单方便地远程管理交换机。配置通过Telnet登录设备前，需要确保终端PC和设备之间路由可达。

须知

使用Telnet协议存在安全风险，建议使用STelnet V2登录设备。

从V200R020C00版本开始，当需要授权客户可以登录服务器时，必须执行命令指定服务器端的源接口或源地址。

通过 Telnet 登录设备的常用功能配置

缺省情况下，设备未配置任何Telnet相关功能，如果需要使用该功能，需要配置Telnet服务及用户信息。配置步骤如下：

1. 使能Telnet服务器功能。
2. 配置VTY用户界面的支持协议类型。
3. 配置VTY用户界面的认证方式及用户级别。

操作步骤

步骤1 使能服务器功能。

```
<HUAWEI> system-view
[HUAWEI] telnet server-source -i Vlanif 10  //假设客户端使用IP地址10.10.10.20连接服务器，该地址对应的接口为Vlanif 10。该命令仅在V200R020C00及之后版本使用。
[HUAWEI] telnet server enable
```

步骤2 配置VTY用户界面的支持协议类型。

```
[HUAWEI] user-interface vty 0 4
[HUAWEI-ui-vty0-4] protocol inbound telnet    //指定VTY用户界面所支持的协议为Telnet
```

步骤3 配置VTY用户界面的认证方式和用户级别。

- 配置VTY用户界面的认证方式为AAA：

  选择AAA认证，需要配置AAA用户的认证信息、接入类型和用户级别。

  ```
  [HUAWEI-ui-vty0-4] authentication-mode aaa    //配置认证方式为AAA
  [HUAWEI-ui-vty0-4] quit
  [HUAWEI] aaa
  [HUAWEI-aaa] local-user admin123 password irreversible-cipher abcd@123    //创建本地用户admin123，登录密码为abcd@123
  [HUAWEI-aaa] local-user admin123 service-type telnet    //配置本地用户admin123的接入类型为Telnet方式
  [HUAWEI-aaa] local-user admin123 privilege level 15    //配置本地用户admin123的级别为15
  Warning: This operation may affect online users, are you sure to change the user privilege level ? [Y/N]y
  ```

- 配置VTY用户界面的认证方式为Password：

  选择password认证，直接配置VTY用户界面的级别和登录密码。

  ```
  [HUAWEI-ui-vty0-4] authentication-mode password    //配置认证方式为password
  [HUAWEI-ui-vty0-4] set authentication password cipher YsHsjx_202206    //配置登录密码为YsHsjx_202206
  [HUAWEI-ui-vty0-4] user privilege level 15    //配置VTY用户界面的级别为15
  ```

  说明

  实际场景中建议使用AAA认证。

  为充分保证设备安全，请定期修改密码。

步骤4 客户端Telnet登录设备。

进入管理员PC的Windows的命令行提示符，执行相关命令，通过Telnet方式登录设备。

```
C:\Documents and Settings\Administrator> telnet 10.10.10.20 23
```

输入Enter键后，在登录窗口输入AAA验证方式配置的登录用户名和密码，验证通过后，出现用户视图的命令行提示符，至此用户成功登录设备。（以下显示信息仅为示意）

```
Login authentication


Username:admin123
Password:
Info: The max number of VTY users is 15, and the number
      of current VTY users on line is 2.
      The current login time is 2018-12-22 18:33:18+00:00.
<HUAWEI>
```

----结束

检查配置结果

- 执行**display users** [**all**]命令，查看用户界面的用户登录信息。
- 执行**display tcp status**命令，查看当前建立的所有TCP连接情况。
- 执行**display telnet server status**命令，查看Telnet服务器的当前连接信息。

命令行功能说明

详细的命令行功能说明请参见《命令参考》手册。

表 6-7 常用功能命令

功能	配置命令	说明
开启Telnet服务器功能	**telnet server enable**	缺省情况为去使能状态。
VTY用户界面的认证方式	**authentication-mode** { **aaa** | **password** }	缺省未配置认证方式。 如果选择**aaa**认证，需要配置AAA本地用户相关信息，包括： • **local-user** *user-name* { **password** { **cipher** | **irreversible-cipher** } *password*，创建本地用户，并配置本地用户的密码。 • **local-user** *user-name* { **privilege level** *level* }，配置本地用户的级别。 • **local-user** *user-name* **service-type** { **http** | **ssh** | **telnet** | **terminal** } *，配置本地用户的接入类型。
VTY用户界面的登录密码	**set authentication password** [**cipher** *password*]	如果认证方式选择**password**，则需要使用该命令设置认证密码。
VTY用户界面所支持的协议	**protocol inbound** { **all** | **telnet** | **ssh** }	缺省为SSH认证。 执行此命令后，配置结果待下次登录请求时生效。
VTY用户界面的用户级别	**user privilege level** *level*	缺省为0。 该命令设置的级别对AAA用户无效，AAA用户由AAA配置信息中本地用户的级别决定。

表 6-8 其他功能命令

功能	配置命令	说明
开启VTY终端服务	**shell**	所有VTY终端服务缺省开启。
VTY用户界面的最大个数	**user-interface maximum-vty** *number*	VTY用户界面的最大个数为15个。

功能	配置命令	说明
VTY用户界面的登录连接超时时间	**idle-timeout** *minutes* [*seconds*]	缺省为10分钟。
VTY用户界面的终端屏显的行数	**screen-length** *screen-length*	缺省为24行。
VTY用户界面的终端屏显的列数	**screen-width** *screen-width*	缺省为80列。
VTY用户界面的历史命令缓冲区的大小	**history-command max-size** *size-value*	缺省为10条。
Telnet服务器的协议端口号	**telnet server port** *port-number*	缺省为23。 更改Telnet服务器的端口号，可有效防止攻击者通过缺省端口号登录Telnet服务器。
Telnet服务器的源接口	• **telnet server-source -i** *interface-type interface-number* • **telnet ipv6 server-source -a** *ipv6_address* [**vpn-instance** *vpn_name*]	缺省情况，未指定Telnet服务器的源接口。
指定Telnet客户端的源地址或源接口。	**telnet client-source** { **-a** *source-ip-address* | **-i** *interface-type interface-number* },	缺省情况下，Telnet客户端的源地址为0.0.0.0。 若**telnet**登录命令不指定源地址或源接口，则使用该命令配置的源地址或源接口。

6.6 配置通过 STelnet 登录设备

Telnet协议存在安全风险，推荐使用STelnet登录设备。登录设备前，需要确保终端PC和设备之间路由可达。

须知

使用STelnet V1协议存在安全风险，建议使用STelnet V2登录设备。

从V200R020C00版本开始，当需要授权客户可以登录服务器时，必须执行命令指定服务器端的源接口或源地址。

从V200R019C10版本开始，设备缺省情况下不支持安全性较低的算法，如需使用安全性较低的算法，需要安装WEAKEA插件。WEAKEA插件安装方法请参见WEAKEA插件使用指南。

通过 STelnet 登录设备的常用功能配置

缺省情况下，设备未配置任何STelnet相关功能，如果需要使用该功能，需要配置STelnet服务及用户信息。配置步骤如下：

1. 配置VTY用户界面的支持协议类型、认证方式和用户级别。
2. 开启STelnet服务器功能并创建SSH用户。
3. 配置SSH用户认证方式。
4. 在SSH服务器端生成本地密钥对，实现在服务器端和客户端进行安全地数据交互。

操作步骤

步骤1 配置VTY用户界面的支持协议类型、认证方式和用户级别。

```
[HUAWEI] user-interface vty 0 4
[HUAWEI-ui-vty0-4] authentication-mode aaa    //配置VTY用户界面认证方式为AAA认证
[HUAWEI-ui-vty0-4] protocol inbound ssh    //配置VTY用户界面支持的协议为SSH，默认情况下即SSH
[HUAWEI-ui-vty0-4] user privilege level 15    //配置VTY用户界面的级别为15
[HUAWEI-ui-vty0-4] quit
```

说明

通过STelnet登录设备需配置用户界面支持的协议是SSH，必须设置VTY用户界面认证方式为AAA认证。

步骤2 开启STelnet服务器功能。

```
[HUAWEI] ssh server-source -i Vlanif 10    //假设客户端使用IP地址10.10.10.20连接服务器，该地址对应的接口为Vlanif 10。该命令仅在V200R020C00及之后版本使用。
[HUAWEI] stelnet server enable    //使能设备的STelnet服务器功能
```

步骤3 配置SSH用户认证方式。

- 配置SSH用户认证方式为Password
  a. 创建SSH用户（两种方式）。

  ```
  [HUAWEI] ssh authentication-type default password    //配置SSH用户缺省采用密码认证
  ```

  或

  ```
  [HUAWEI] ssh user admin123    //创建SSH用户admin123
  [HUAWEI] ssh user admin123 service-type stelnet    //配置SSH用户的服务方式为STelnet
  [HUAWEI] ssh user admin123 authentication-type password    //配置SSH用户认证方式为password
  ```

  b. 使用Password认证方式时，需要在AAA视图下配置与SSH用户同名的本地用户。

  ```
  [HUAWEI] aaa
  [HUAWEI-aaa] local-user admin123 password irreversible-cipher YsHsjx_202206    //创建与SSH用户同名的本地用户和对应的登录密码
  [HUAWEI-aaa] local-user admin123 privilege level 15    //配置本地用户级别为15
  Warning: This operation may affect online users, are you sure to change the user privilege level ? [Y/N]y
  [HUAWEI-aaa] local-user admin123 service-type ssh    //配置本地用户的服务方式为SSH
  [HUAWEI-aaa] quit
  ```

- 配置SSH用户认证方式为RSA、DSA或ECC（以ECC认证方式为例，RSA、DSA认证方式步骤类似）

  使用RSA、DSA或ECC认证方式时，需要在SSH服务器上输入SSH客户端生成的密钥中的公钥部分。这样当客户端登录服务器时，自己的私钥如果与输入的公钥匹配成功，则认证通过。客户端公钥的生成请参见相应的SSH客户端软件的帮助文档。

  ```
  [HUAWEI] ssh user admin123    //创建SSH用户admin123
  [HUAWEI] ssh user admin123 service-type stelnet    //配置SSH用户的服务方式为STelnet
  ```



```
[HUAWEI] ssh user admin123 authentication-type ecc    //配置SSH用户认证方式为ecc
[HUAWEI] ecc peer-public-key key01 encoding-type pem    //配置ECC公共密钥编码格式，并进入ECC公共密钥视图,key01为公共密钥名称
Enter "ECC public key" view, return system view with "peer-public-key end".
[HUAWEI-ecc-public-key] public-key-code begin    //进入公共密钥编辑视图
Enter "ECC key code" view, return last view with "public-key-code end".
[HUAWEI-dsa-key-code] 308188    //拷贝复制客户端的公钥，必须为十六进制字符串，如果是其他进制，请提前转换
[HUAWEI-dsa-key-code] 028180
[HUAWEI-dsa-key-code] B21315DD 859AD7E4 A6D0D9B8 121F23F0 006BB1BB
[HUAWEI-dsa-key-code] A443130F 7CDB95D8 4A4AE2F3 D94A73D7 36FDFD5F
[HUAWEI-dsa-key-code] 411B8B73 3CDD494A 236F35AB 9BBFE19A 7336150B
[HUAWEI-dsa-key-code] 40A35DE6 2C6A82D7 5C5F2C36 67FBC275 2DF7E4C5
[HUAWEI-dsa-key-code] 1987178B 8C364D57 DD0AA24A A0C2F87F 474C7931
[HUAWEI-ecc-key-code] A9F7E8FE E0D5A1B5 092F7112 660BD153 7FB7D5B2
[HUAWEI-ecc-key-code] 171896FB 1FFC38CD
[HUAWEI-ecc-key-code] 0203
[HUAWEI-ecc-key-code] 010001
[HUAWEI-ecc-key-code] public-key-code end    //退回到公共密钥视图
[HUAWEI-ecc-public-key] peer-public-key end    //退回到系统视图
[HUAWEI] ssh user admin123 assign ecc-key key01    //为用户admin123分配一个已经存在的公钥key01
```

说明

- 使用Password-RSA认证、Password-DSA认证或Password-ECC认证时，需同时配置AAA用户信息和输入客户端公钥，即上述两种方式都需要进行。
- 使用ALL认证方式时，对于配置AAA用户信息和输入客户端公钥，可以随意选择上述两种方式其中一种方式，也可以两种方式都选择。
- 为充分保证设备安全，请定期修改密码。

步骤4 在服务器端生成本地密钥对。

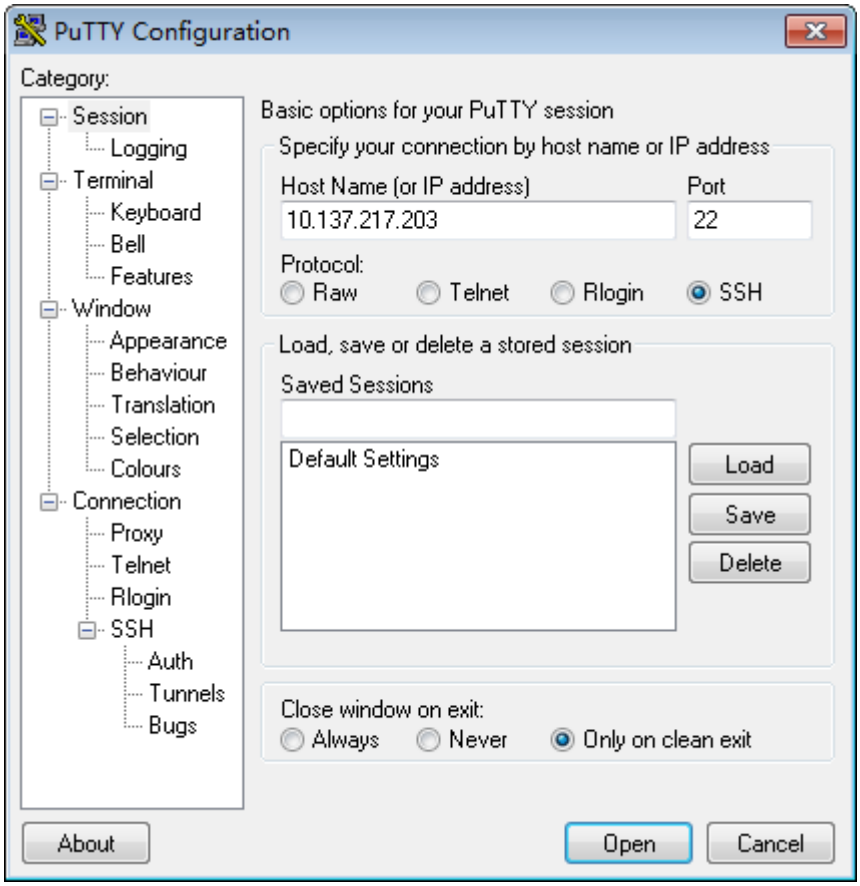
```
[HUAWEI] ecc local-key-pair create
Info: The key name will be: HUAWEI_Host_ECC.
Info: The key modulus can be any one of the following: 256, 384, 521.
Info: If the key modulus is greater than 512, it may take a few minutes.
Please input the modulus [default=521]:521
Info: Generating keys.....
Info: Succeeded in creating the ECC host keys.
```

步骤5 客户端STelnet登录设备。

PC端用Password认证方式连接SSH服务器。

通过PuTTY软件登录设备，输入设备的IP地址，选择协议类型为SSH。

图 6-1 通过 PuTTY 软件用 password 认证方式连接 SSH 服务器示意图



点击“Open”，出现如下界面，输入用户名和密码，并按Enter键，至此已登录到SSH服务器。（以下显示信息仅为示意）

```
login as: admin123
Sent username "admin123"

admin123@10.10.10.20's password:

Info: The max number of VTY users is 8, and the number
      of current VTY users on line is 5.
      The current login time is 2018-12-22 09:35:28+00:00.
<HUAWEI>
```

----结束

检查配置结果

- 执行**display ssh user-information** [*username*]命令，在SSH服务器端查看SSH用户信息。如果不指定SSH用户，则可以查看SSH服务器端所有的SSH用户信息。
- 执行**display ssh server status**命令，查看SSH服务器的全局配置信息。
- 执行**display ssh server session**命令，在SSH服务器端查看与SSH客户端连接的会话信息。

命令行功能说明

表 6-9 常用功能命令

功能	配置命令	说明
生成本地主机密钥对	**rsa local-key-pair create**、**dsa local-key-pair create**或**ecc local-key-pair create**	缺省情况，未配置任何主机密钥对。
开启STelnet服务器功能	**stelnet server enable**	缺省为去使能状态。
VTY用户界面的认证方式	**authentication-mode** { **aaa** }	缺省情况下，通过Console口登录设备时，默认认证方式为Password。 如果选择**aaa**认证，需要配置AAA本地用户相关信息。
VTY用户界面所支持的协议	**protocol inbound** { **all** | **ssh** }	缺省为SSH协议。 执行此命令后，配置结果待下次登录请求时生效。
VTY用户界面的用户级别	**user privilege level** *level*	缺省为0。 用户使用RSA、DSA或ECC认证方式时，用户的优先级由用户接入时所采用的VTY界面的优先级决定。 如果用户界面下配置的命令级别访问权限与用户名本身对应的操作权限冲突，以用户名本身对应的命令级别为准。
新建SSH用户	**ssh user** *user-name*	缺省情况，没有创建SSH用户。
SSH用户的服务方式	**ssh user** *user-name* **service-type** { **stelnet** | **all** }	缺省为空，不支持任何服务方式。

功能	配置命令	说明
SSH用户的认证方式	**ssh user** *user-name* **authentication-type** { **password** | **rsa** | **password-rsa** | **dsa** | **password-dsa** | **ecc** | **password-ecc** | **all** }	• SSH用户认证方式为**Password**时，需要在**AAA视图**下配置与SSH用户同名的本地用户、登录密码、服务方式和用户级别。包括： – **local-user** *user-name* { **password** { **cipher** | **irreversible-cipher** } *password*，创建本地用户，并配置本地用户的密码。 – **local-user** *user-name* { **privilege level** *level* }，配置本地用户的级别。 – **local-user** *user-name* **service-type** { **http** | **ssh** | **telnet** | **terminal** } *，配置本地用户的接入类型。 • SSH用户认证方式为**RSA**、**DSA**或**ECC**时，需要在**SSH服务器**上输入SSH客户端生成的密钥中的公钥部分。 • SSH用户认证方式为**Password-RSA**、**Password-DSA**或**Password-ECC**时，需要同时配置AAA用户信息和输入客户端公钥。 • SSH用户认证方式为**ALL**时，配置AAA用户信息和输入客户端公钥，可以随意选择其中一种，也可以两种方式都选择。

表 6-10 其他功能命令

功能	配置命令	说明
开启VTY终端服务	**shell**	所有VTY终端服务缺省开启。
VTY用户界面的最大个数	**user-interface maximum-vty** *number*	VTY用户界面的最大个数为15个。
VTY用户界面的登录连接超时时间	**idle-timeout** *minutes* [*seconds*]	缺省为10分钟。
VTY用户界面的终端屏显的行数	**screen-length** *screen-length*	缺省为24行。
VTY用户界面的终端屏显的列数	**screen-width** *screen-width*	缺省为80列。
VTY用户界面的历史命令缓冲区的大小	**history-command max-size** *size-value*	缺省为10条。
SSH服务器支持的密钥交换算法	**ssh server key-exchange** { **dh_group14_sha256** | **dh_group15_sha512** | **dh_group16_sha512** | **dh_group_exchange_sha256** | **ecdh_sha2_nistp256**| **ecdh_sha2_nistp384**| **ecdh_sha2_nistp521** }*	缺省为支持所有密钥交换算法。 系统软件中不包含**dh_group_exchange_sha1**、**dh_group14_sha1**和**dh_group1_sha1**参数，如需使用，需要安装WEAKEA插件，但是该算法安全性低。为了保证更好的安全性，建议使用其它算法。WEAKEA插件安装方法请参见WEAKEA插件使用指南。

功能	配置命令	说明
SSH服务器支持的加密算法	**ssh server cipher** { **aes128_ctr** | **aes256_ctr** } *	缺省情况下，不安装WEAKEA插件，SSH服务器只支持**aes128_ctr**和**aes256_ctr**算法，不可以使用**undo ssh server cipher**命令，安装WEAKEA插件后，增加支持**aes256_cbc**、**aes128_cbc**、**3des_cbc**和**des_cbc**算法，并且可以使用**undo ssh server cipher**命令。 系统软件中不包含**aes256_cbc**、**aes128_cbc**、**3des_cbc**和**des_cbc**参数，如需使用，需要安装WEAKEA插件，但是该算法安全性低。为了保证更好的安全性，建议配置**aes256_ctr**或**aes128_ctr**参数。WEAKEA插件安装方法请参见WEAKEA插件使用指南。
SSH服务器支持的校验算法	**ssh server hmac sha2_256**	缺省情况下，不安装WEAKEA插件，SSH服务器只支持**sha2_256**校验算法，不可以使用**undo ssh server hmac**命令，安装WEAKEA插件后，增加支持**sha2_256_96**、**sha1**、**sha1_96**、**md5**和**md5_96**校验算法，并且可以使用**undo ssh server hmac**命令。 系统软件中不包含**sha2_256_96**、**sha1**、**sha1_96**、**md5**和**md5_96**参数，如需使用，需要安装WEAKEA插件，但是该算法安全性低。为了保证更好的安全性，建议配置**sha2_256**参数。WEAKEA插件安装方法请参见WEAKEA插件使用指南。
SSH服务器端口号	**ssh [ipv4 | ipv6] server port** *port-number*	缺省为22。 SSH服务器配置新的端口号，可以有效防止攻击者对SSH服务标准端口的恶意访问，确保安全性。
SSH服务器的公钥算法	**ssh server publickey** { **dsa** | **ecc** | **rsa** | **rsa_sha2_256** | **rsa_sha2_512** } *	缺省为DSA、ECC、RSA、RSA_SHA2_256、RSA_SHA2_512公钥算法都开启。 使用指定的公钥算法登录服务器，同时拒绝使用其他公钥算法，从而提升设备安全性。推荐使用ECC公钥算法。

功能	配置命令	说明
SSH服务器的源接口	• **ssh server-source -i** *interface-type interface-number* • **ssh ipv6 server-source -a** *ipv6_address* [**-vpn-instance** *vpn_name*]	缺省情况下，未指定SSH服务器端的源接口。
SSH服务器密钥对更新时间	**ssh server rekey-interval** *hours*	缺省为0，永不更新。
SSH服务器协商密钥时的参数	**ssh server rekey** { **time** *rekey-time* | **data-limit** *data-limit* | **max-packet** *max-packet* } *	缺省情况下，SSH服务器触发密钥重协商的时间间隔为60分钟，重协商密钥时收发数据大小上限为1000MB，重协商密钥时收发数据包个数上限为268435456（2^28）个。
SSH认证超时时间	**ssh server timeout** *seconds*	缺省为60秒。
SSH认证重试次数	**ssh server authentication-retries** *times*	缺省为3次。

6.7 （可选）配置 ACL 限制用户通过 Telnet/STelnet 登录设备

背景信息

配置通过Telnet/STelnet登录设备时，支持配置安全策略。

操作步骤

- 限制其他设备访问本设备。
  - 方法一：
    i. 执行命令**acl** *acl-number*或**acl ipv6** *acl6-number*，创建一个访问控制列表并进入ACL或ACL6视图。

    此处*acl-number*或*acl6-number*要求配置为基本ACL范围：2000～2999。

    ii. 执行命令**rule permit source** *source-address* **0**或**rule permit source** *source-ipv6-address* **0**，配置ACL或ACL6规则，限制除设备地址为*source-address*或*source-ipv6-address*以外的设备访问本设备。

    iii. 执行命令**quit**，退出ACL或ACL6视图。

    iv. 配置可以访问本设备的访问控制列表。
    - 对于通过Telnet方式登录的设备，执行命令**telnet** [**ipv6**] **server acl** *acl-number*。

- 对于通过STelnet方式登录的设备，执行命令**ssh** [**ipv6**] **server acl** *acl-number*。

– 方法二：

i. 执行命令**acl** *acl-number*或**acl ipv6** *acl6-number*，创建一个访问控制列表并进入ACL或ACL6视图。

此处*acl-number*或*acl6-number*要求配置为基本ACL范围：2000～2999。

ii. 执行命令**rule permit source** *source-address* **0**或**rule permit source** *source-ipv6-address* **0**，配置ACL或ACL6规则，限制除设备地址为*source-address*或*source-ipv6-address*以外的设备访问本设备。

iii. 执行命令**quit**，退出ACL或ACL6视图。

iv. 执行命令**user-interface vty** *first-ui-number* [*last-ui-number*]，进入VTY用户界面视图。

v. 执行命令**acl** [**ipv6**] { *acl-number* | *acl-name* } **inbound**，配置VTY类型用户界面的基于ACL的访问限制。

- 限制本设备访问其他设备。

a. 执行命令**acl** *acl-number*或**acl ipv6** *acl6-number*，创建一个访问控制列表并进入ACL或ACL6视图。

此处*acl-number*或*acl6-number*要求配置为高级ACL范围：3000～3999。

b. 配置ACL或ACL6规则，限制本设备访问其他设备。

- 对于通过Telnet方式登录的设备，执行命令**rule deny tcp destination-port eq telnet**。
- 对于通过STelnet方式登录的设备，执行命令**rule deny tcp destination-port eq 22**。

c. 执行命令**quit**，退出ACL或ACL6视图。

d. 执行命令**user-interface vty** *first-ui-number* [*last-ui-number*]，进入VTY用户界面视图。

e. 执行命令**acl** [**ipv6**] { *acl-number* | *acl-name* } **outbound**，配置VTY类型用户界面的基于ACL的访问限制。

检查配置结果

执行命令**display acl** { *acl-number* | **name** *acl-name* | **all** }，查看ACL的配置信息。

6.8 命令行配置设备登录后的常用操作

查看在线用户

用户登录系统后可以查看每个用户界面的用户登录信息。

执行命令**display users** [**all**]，查看用户界面的使用信息。

清除在线用户

当用户需要将某个登录用户与设备连接断开时，可以清除指定的在线用户。

1. 执行命令**kill user-interface** { *ui-number* | *ui-type ui-number1* }，清除在线用户。
2. 执行命令**display users**，查看当前设备上的用户登录信息。

设置切换用户级别的密码

如果当前用户级别较低，但是需要对高于用户级别的命令进行操作，用户可以由低级别切换到高级别，并需要设置密码。

1. 执行命令**system-view**，进入系统视图。
2. 执行命令**super password** [**level** *user-level*] [**cipher** *password*]，配置切换用户级别的密码。

在对网络安全性要求较低的环境中，可以关闭低级别用户切换到高级别用户所需密码的复杂度检查功能。

1. 执行命令**system-view**，进入系统视图。
2. 执行命令**super password complexity-check disable**，关闭低级别用户切换到高级别用户所需密码的复杂度检查功能。

说明

为充分保证设备安全，请用户不要关闭密码复杂度检查功能，并定期修改密码。

切换用户级别

用户由低级别切换到高级别，需要输入设置好的密码。

1. 执行命令**super** [*level*]，切换用户级别。
2. 根据系统提示，输入切换口令。

   如果输入的口令正确，将切换到更高级别。如果连续三次输入错误的口令，将退回用户视图，仍保持现有登录级别。

说明

当以低级别登录的用户通过**super**命令切换到高级别时，系统会自动发送**trap**信息，并记录在日志中。如果切换到的级别低于当前级别，则仅记录日志。

交换机采用“用户名+密码+级别”的方式控制用户操作设备的权限。使用super命令切换用户级别后，原“用户名+密码+级别”的权限控制方式失效。任一用户只需知道高级别的super密码，即可获取高级别的操作权限，存在越权操作设备的风险。因此，不建议使用super命令切换用户级别。

锁定用户配置权限

在多用户同时登录系统进行配置时，有可能会出现配置冲突的情况。为了避免业务出现异常，可以配置权限互斥功能，保证同一时间只有一个用户可以进行配置。

1. 执行命令**configuration exclusive**，锁定配置权限给当前操作用户。

   锁定用户配置权限后，可以显式地获取独享的配置权限，其他用户无法再获取到配置权限。

   如果配置权限已经被锁定，则再次锁定会返回提示信息。

   此命令可用于所有视图。

说明

可以执行**display configuration-occupied user**命令，查看当前锁定配置级用户的信息。

2. 执行命令**system-view**，进入系统视图。
3. （可选）执行命令**configuration-occupied timeout** *timeout-value*，设置自行解锁时间间隔。

   设置锁定配置级权限用户在无配置命令下发的情况下，允许锁定的最长时间间隔，超过这个时间间隔系统就自行解锁，其他用户可以正常配置。

   缺省情况下，锁定间隔为30秒。

发送消息给其他用户界面

用户可以在当前的用户界面发送消息给其他用户界面，实现用户界面间的消息传递。

1. 执行命令**send** { **all** | *ui-number* | *ui-type ui-number1* }，设置在用户界面间传递消息。
2. 根据系统提示，输入要传递的信息。输入“Ctrl+Z”或“Enter”键结束输入，使用“Ctrl+C”终止本次操作。
3. 根据系统提示，选择是否需要发送消息。选择“Y”发送消息，选择“N”取消发送。

锁定用户界面

当用户需要暂时离开操作终端时，为防止未授权的用户操作该终端界面，可以锁定当前用户终端界面。

1. 执行命令**lock**，锁定用户界面。
2. 根据系统提示，输入锁定的密码，并确认密码。

   ```
   <HUAWEI> lock
   Please configure the login password (8-16)
   Enter Password:
   Confirm Password:
   Info: The terminal is locked.
   ```

   用户输入命令**lock**后，系统提示输入两次屏保密码，如果两次输入的密码相同，则锁定当前用户界面成功。

   缺省情况下，设备允许的显式密码最小长度是8。可以适当增加密码的长度要求，使密码复杂度增加，从而提高设备的安全性。执行命令**set password min-length** *length*，设置设备允许的显式密码最小长度。

   系统锁定后，如果想再次进入系统，必须先按“Enter”键，此时提示输入登录密码，用户输入正确的登录密码才可以解除锁定进入系统。

允许在系统视图下执行用户视图命令

对于某些命令只能在用户视图下执行，当用户需要执行该类命令时，必须退出到用户视图才能成功执行。为了便于用户执行用户视图命令，在不用切换视图的情况下，通过本配置可实现在系统视图下执行用户视图命令。

1. 执行命令**system-view**，进入系统视图。
2. 执行命令**run** *command-line*，允许在系统视图下执行用户视图命令。

   缺省情况下，系统不允许在系统视图下执行用户视图命令。

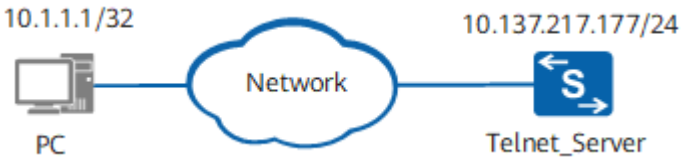
6.9 登录设备命令行的配置举例

6.9.1 配置 ACL 限制用户通过 Telnet 登录设备示例

组网需求

如图6-2所示，PC与设备之间路由可达，用户希望简单方便的配置和管理远程设备，可以在服务器端配置Telnet用户使用AAA验证登录，并配置安全策略，保证只有符合安全策略的用户才能登录设备。

图 6-2 配置通过 Telnet 登录设备组网图



配置思路

1. 配置Telnet方式登录设备，以实现远程维护网络设备。
2. 配置安全策略，保证只有符合安全策略的用户才能登录设备。
3. 配置管理员的用户名和密码。

说明

当所处环境不足够安全时，建议选择较安全的STelnet接入方式登录设备，具体配置步骤请参见**配置通过STelnet登录设备**。

配置步骤

1. 使能Telnet服务器功能

```
<HUAWEI> system-view
[HUAWEI] sysname Telnet_Server
[Telnet_Server] telnet server-source -i Vlanif 10  //假设客户端使用IP地址10.137.217.177连接服务器，该地址对应的接口为Vlanif 10
[Telnet_Server] telnet server enable
```

说明

Telnet协议本身有安全风险，建议您使用SSH v2安全协议。

2. 配置VTY用户界面的相关参数

配置VTY用户界面的最大个数。

```
[Telnet_Server] user-interface maximum-vty 15
```

配置允许用户登录设备的主机地址。

```
[Telnet_Server] acl 2001
[Telnet_Server-acl-basic-2001] rule permit source 10.1.1.1 0
[Telnet_Server-acl-basic-2001] quit
[Telnet_Server] user-interface vty 0 14
[Telnet_Server-ui-vty0-14] protocol inbound telnet
[Telnet_Server-ui-vty0-14] acl 2001 inbound
```

配置VTY用户界面的终端属性。

```
[Telnet_Server-ui-vty0-14] shell
[Telnet_Server-ui-vty0-14] idle-timeout 20
[Telnet_Server-ui-vty0-14] screen-length 0
[Telnet_Server-ui-vty0-14] history-command max-size 20
```

配置VTY用户界面的用户验证方式。

```
[Telnet_Server-ui-vty0-14] authentication-mode aaa
[Telnet_Server-ui-vty0-14] quit
```

3. 配置登录用户的相关信息

   # 配置登录验证方式。

```
[Telnet_Server] aaa
[Telnet_Server-aaa] local-user admin1234 password irreversible-cipher Helloworld@6789
[Telnet_Server-aaa] local-user admin1234 service-type telnet
[Telnet_Server-aaa] local-user admin1234 privilege level 3
[Telnet_Server-aaa] quit
```

4. 客户端登录

   # 进入管理员PC的Windows的命令行提示符，执行相关命令，通过Telnet方式登录设备。

```
C:\Documents and Settings\Administrator> telnet 10.137.217.177
```

   输入Enter键后，在登录窗口输入AAA验证方式配置的登录用户名和密码，验证通过后，出现用户视图的命令行提示符，至此用户成功登录设备。（以下显示信息仅为示意）

```
Login authentication


Username:admin1234
Password:
Info: The max number of VTY users is 15, and the number
      of current VTY users on line is 2.
      The current login time is 2019-08-06 18:33:18+00:00.
<Telnet_Server>
```

配置文件

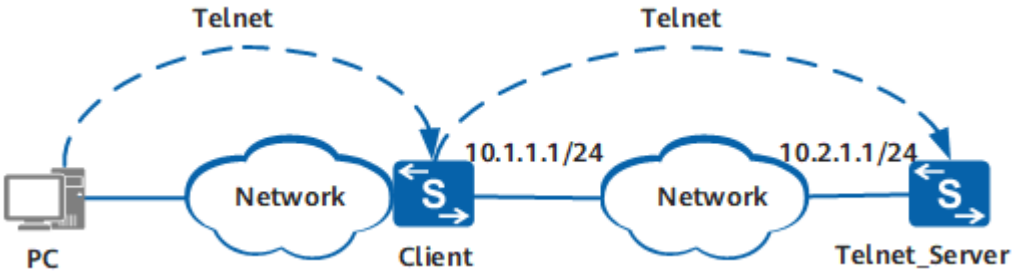
```
#
sysname Telnet_Server
#
telnet server enable
telnet server-source -i Vlanif 10
#
acl number 2001
 rule 5 permit source 10.1.1.1 0
#
aaa
 local-user admin1234 password irreversible-cipher %^%#aVW8S=aP=B<OWi1Bu'^R[=_!~oR*85r_nNY+kA(I}
[TiLiVGR-i/'DFGAI-O%^%#
 local-user admin1234 privilege level 3
 local-user admin1234 service-type telnet
#
user-interface maximum-vty 15
user-interface vty 0 14
 acl 2001 inbound
 authentication-mode aaa
 history-command max-size 20
 idle-timeout 20 0
 screen-length 0
 protocol inbound telnet
#
return
```

6.9.2 配置设备作为 Telnet 客户端登录其他设备示例

组网需求

如图6-3所示，PC与设备之间路由可达，用户希望简单方便的配置和管理远程设备，可以在服务器端配置Telnet用户使用AAA验证登录，并配置安全策略，保证只有符合安全策略的用户才能登录设备。

图 6-3 配置设备作为 Telnet 客户端登录其他设备组网图



配置思路

1. 配置Telnet方式登录设备，以实现远程维护网络设备。
2. 配置安全策略，保证只有符合安全策略的用户才能登录设备。
3. 配置管理员的用户名和密码。

说明

当所处环境不足够安全时，建议选择较安全的STelnet接入方式登录设备，具体配置案例请参见**配置设备作为STelnet客户端登录其他设备示例**。

操作步骤

1. 使能Telnet服务器功能

```
<HUAWEI> system-view
[Telnet_Server] sysname Telnet_Server
[Telnet_Server] telnet server-source -i Vlanif 10  //假设客户端使用IP地址10.2.1.1连接服务器，该地址对应的接口为Vlanif 10
[Telnet_Server] telnet server enable
```

2. 配置VTY用户界面的相关参数

   # 配置VTY用户界面的最大个数。

```
[Telnet_Server] user-interface maximum-vty 15
```

   # 配置允许用户登录设备的主机地址。

```
[Telnet_Server] acl 2001
[Telnet_Server-acl-basic-2001] rule permit source 10.1.1.1 0
[Telnet_Server-acl-basic-2001] quit
[Telnet_Server] user-interface vty 0 14
[Telnet_Server-ui-vty0-14] protocol inbound telnet
[Telnet_Server-ui-vty0-14] acl 2001 inbound
```

   # 配置VTY用户界面的终端属性。

```
[Telnet_Server-ui-vty0-14] shell
[Telnet_Server-ui-vty0-14] idle-timeout 20
[Telnet_Server-ui-vty0-14] screen-length 0
[Telnet_Server-ui-vty0-14] history-command max-size 20
```

   # 配置VTY用户界面的用户验证方式。

```
[Telnet_Server-ui-vty0-14] authentication-mode aaa
[Telnet_Server-ui-vty0-14] quit
```

3. 配置登录用户的相关信息

   # 配置登录验证方式。

   ```
   [Telnet_Server] aaa
   [Telnet_Server-aaa] local-user admin1234 password irreversible-cipher Helloworld@6789
   [Telnet_Server-aaa] local-user admin1234 service-type telnet
   [Telnet_Server-aaa] local-user admin1234 privilege level 3
   [Telnet_Server-aaa] quit
   ```

4. 客户端登录

   进入管理员PC的Windows的命令行提示符，执行相关命令，通过Telnet方式登录设备。

   ```
   C:\Documents and Settings\Administrator> telnet 10.137.217.177
   ```

   输入Enter键后，在登录窗口输入AAA验证方式配置的登录用户名和密码，验证通过后，出现用户视图的命令行提示符，至此用户成功登录设备。（以下显示信息仅为示意）

   ```
   Login authentication


   Username:admin1234
   Password:
   Info: The max number of VTY users is 8, and the number
         of current VTY users on line is 2.
         The current login time is 2019-08-06 18:33:18+00:00.
   <Telnet_Server>
   ```

配置文件

Telnet_Server的配置文件

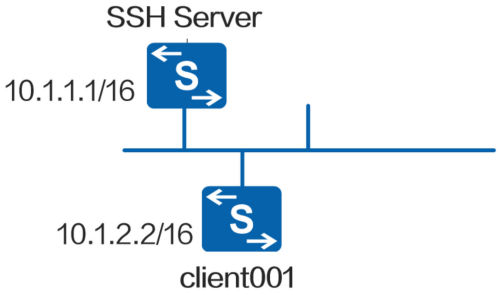
```
#
sysname Server
#
telnet server enable
telnet server-source -i Vlanif 10
#
acl number 2000
 rule 5 permit source 10.1.1.1 0
#
aaa
 local-user admin1234 password irreversible-cipher %^%#gRNl~ukoL~0.WU)C2]~2a}Cz/Y0-u8M{j@Ql6/
xHryO-Y7m{=A>kWc.-q}>*%^%#
 local-user admin1234 privilege level 3
 local-user admin1234 service-type telnet
#
user-interface maximum-vty 15
user-interface vty 0 14
 acl 2001 inbound
 authentication-mode aaa
 history-command max-size 20
 idle-timeout 20 0
 screen-length 0
 protocol inbound telnet
#
return
```

6.9.3 配置设备作为 STelnet 客户端登录其他设备示例（Password 认证）

组网需求

如图6-4所示，用户希望在服务器端和客户端进行安全的数据交互，配置一个登录用户为client001，使用password认证方式登录SSH服务器。

图 6-4 配置通过 STelnet 登录其他设备组网图



说明

使用STelnet V1协议存在安全风险，实际应用中建议使用STelnet V2登录设备。

配置思路

1. 在SSH服务器端配置SSH用户client001的认证方式为Password认证。
2. 在SSH服务器端开启STelnet服务功能。
3. 在SSH服务器端配置SSH用户client001的服务方式为STelnet。
4. 用户client001以STelnet方式实现登录SSH服务器。

说明

Password认证不安全，实际应用中建议使用AAA认证。

操作步骤

1. 在服务器端创建SSH用户。

   # 配置VTY用户界面。

   ```
   <HUAWEI> system-view
   [HUAWEI] sysname SSH Server
   [SSH Server] user-interface vty 0 4
   [SSH Server-ui-vty0-4] authentication-mode aaa
   [SSH Server-ui-vty0-4] protocol inbound ssh
   [SSH Server-ui-vty0-4] user privilege level 15
   [SSH Server-ui-vty0-4] quit
   ```

   创建SSH用户client001。

   # 新建用户名为client001的SSH用户，认证方式为password，密码是**YsHsjx_202206**。

   ```
   [SSH Server] ssh user client001
   [SSH Server] ssh user client001 authentication-type password
   [SSH Server] aaa
   [SSH Server-aaa] local-user client001 password irreversible-cipher YsHsjx_202206
   [SSH Server-aaa] local-user client001 privilege level 15
   [SSH Server-aaa] local-user client001 service-type ssh
   [SSH Server-aaa] quit
   ```

2. SSH服务器端开启STelnet服务功能。

```
[SSH Server] stelnet server enable
[SSH Server] ssh server-source -i Vlanif 10   //仅V200R020C00及之后版本需要配置这条命令。此处假设客户端使用IP地址10.1.1.1连接服务器，该地址对应的接口为Vlanif 10
```

3. 配置SSH用户client001的服务方式为STelnet。

```
[SSH Server] ssh user client001 service-type stelnet
```

4. STelnet客户端连接SSH服务器。

   # 第一次登录，需要使能SSH客户端首次认证功能。使能客户端Client001首次认证功能。

```
<HUAWEI> system-view
[HUAWEI] sysname client001
[client001] ssh client first-time enable
```

   # STelnet客户端Client001用password认证方式连接SSH服务器，输入配置的用户名和密码。

```
[client001] stelnet 10.1.1.1
Please input the username:client001
Trying 10.1.1.1 ...
Press CTRL+K to abort
Connected to 10.1.1.1 ...
The server is not authenticated. Continue to access it? [Y/N] :y
Save the server's public key? [Y/N] :y
The server's public key will be saved with the name 10.1.1.1. Please wait...

Please select public key type for user authentication [R for RSA; D for DSA; Enter for Skip publickey authentication; Ctrl_C for Can
cel], Please select [R, D, Enter or Ctrl_C]:d
Enter password:
```

   输入密码，显示登录成功信息如下：

```
<SSH Server>
```

5. 验证配置结果。

   在SSH服务器端执行**display ssh server status**命令可以查看到STelnet服务已经使能。执行**display ssh user-information**命令可以查看服务器端SSH用户信息。

   # 查看SSH状态信息。

```
[SSH Server] display ssh server status
 SSH version                     :2.0
 SSH connection timeout          :60 seconds
 SSH server key generating interval  :0 hours
 SSH authentication retries      :3 times
 SFTP server                     :Disable
 Stelnet server                  :Enable
 Scp server                      :Disable
 SSH server source               :0.0.0.0
 ACL4 number                     :0
 ACL6 number                     :0
```

   # 查看SSH用户信息。

```
[SSH Server] display ssh user-information
  User 1:
      User Name           : client001
      Authentication-type  : password
      User-public-key-name : -
      User-public-key-type : -
      Sftp-directory       : -
      Service-type         : stelnet
      Authorization-cmd    : No
```

配置文件

- SSH服务器的配置文件

```
#
system-view
```

```
#
sysname SSH Server
y
user-interface vty 0 4
y
authentication-mode aaa
y
protocol inbound ssh
y
user privilege level 15
y
quit
#
ssh user client001
y
ssh user client001 authentication-type password
y
aaa
y
local-user client001 password irreversible-cipher $1a$gRNl~ukoL~0.WU)C2]~2a}Cz/Y0-u8M{j@Ql6/
xHryO-Y7m{=A>kWc.-q}>*$
y
local-user client001 privilege level 15
y
local-user client001 service-type ssh
quit
#
stelnet server enable
y
ssh server-source -i Vlanif 10
y
#
ssh user client001 service-type stelnet
#
return
```

- SSH客户端Client001的配置文件

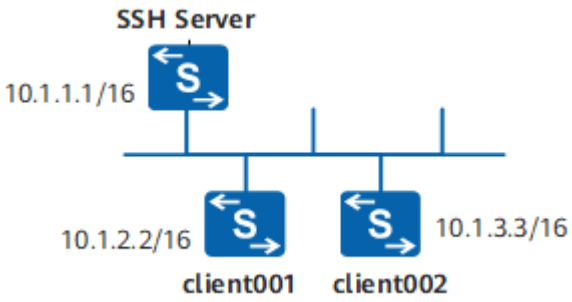
```
#
sysname client001
y
#
ssh client first-time enable
y
#
return
```

6.9.4 配置设备作为 STelnet 客户端登录其他设备示例（Password 认证+DSA 认证）

组网需求

如图6-5所示，用户希望在服务器端和客户端进行安全的数据交互，配置两个登录用户为client001和client002，分别使用password认证方式和dsa认证方式登录SSH服务器。

图 6-5 配置通过 STelnet 登录其他设备组网图



须知

使用STelnet V1协议存在安全风险，建议使用STelnet V2登录设备。

配置思路

1. 在SSH服务器端生成本地密钥对，实现在服务器端和客户端进行安全的数据交互。
2. 在SSH服务器端配置SSH用户client001和client002分别使用不同的认证方式。
3. 在SSH服务器端开启STelnet服务功能。
4. 在SSH服务器端配置SSH用户client001和client002的服务方式为STelnet。
5. 用户client001和client002分别以STelnet方式实现登录SSH服务器。

操作步骤

1. 在服务器端生成本地密钥对

```
<HUAWEI> system-view
[HUAWEI] sysname SSH Server
[SSH Server] dsa local-key-pair create
Info: The key name will be: SSH Server_Host_DSA.
Info: The DSA host key named SSH Server_Host_DSA already exists.
Info: The key modulus can be any one of the following : 1024, 2048.
Info: If the key modulus is greater than 512, it may take a few minutes.
Please input the modulus [default=2048]:
Info: Generating keys.....
Info: Succeeded in creating the DSA host keys.
```

2. 在服务器端创建SSH用户

   # 配置VTY用户界面。

```
[SSH Server] user-interface vty 0 4
[SSH Server-ui-vty0-4] authentication-mode aaa
[SSH Server-ui-vty0-4] protocol inbound ssh
[SSH Server-ui-vty0-4] quit
```

   - 创建SSH用户client001。

     # 新建用户名为client001的SSH用户，且认证方式为password。

     说明

     Password认证不安全，实际应用中建议使用AAA认证。

```
[SSH Server] aaa
[SSH Server-aaa] local-user client001 password irreversible-cipher YsHsjx_202206
[SSH Server-aaa] local-user client001 privilege level 3
```

```
[SSH Server-aaa] local-user client001 service-type ssh
[SSH Server-aaa] quit
[SSH Server] ssh user client001
[SSH Server] ssh user client001 authentication-type password
```

- 创建SSH用户client002。

  # 新建用户名为client002的SSH用户，且认证方式为dsa。

```
[SSH Server] ssh user client002
[SSH Server] ssh user client002 authentication-type dsa
```

  # 在STelnet客户端Client002生成客户端的本地密钥对。

```
<HUAWEI> system-view
[HUAWEI] sysname client002
[client002] dsa local-key-pair create
Info: The key name will be: SSH Server_Host_DSA.
Info: The DSA host key named SSH Server_Host_DSA already exists.
Info: The key modulus can be any one of the following : 1024, 2048.
Info: If the key modulus is greater than 512, it may take a few minutes.
Please input the modulus [default=2048]:
Info: Generating keys.....
Info: Succeeded in creating the DSA host keys.
```

  # 查看客户端上生成的DSA密钥对的公钥部分。

```
[client002] display dsa local-key-pair public
=====================================================
Time of Key pair created: 2014-03-03 16:51:28-05:13
Key name: client002_Host
Key modulus : 2048
Key type: DSA encryption Key
Key fingerprint: c0:52:b0:37:4c:b2:64:d1:8f:ff:a1:42:87:09:8c:6f
=====================================================
Key code:
30820109
  02820100
    CA97BCDE 697CEDE9 D9AB9475 9E004D15 C8B95116
    87B79B0C 5698C582 69A9F4D0 45ED0E53 AF2EDEC1
    A09DF4BE 459E34B6 6697B85D 2191A00E 92F3A5E7
    FB0E73E7 F0212432 E898D979 8EAA491E E2B69727
    4B51A2BE CD86A144 16748D1E 4847A814 3FE50862
    6EB1AD81 EB49A05E 64F6D186 C4E94CDB 04C53074
    B839305A 7F7BCE2C 606F6C91 EA958B6D AC46C12B
    8C2B1E03 98F1C09D 3AF2A69D 6867F930 DF992692
    9A921682 916273FC 4DD875D4 44BC371E DDBB8F6A
    C0A4CDB3 ADDAE853 DB86B9FA DB13CCA9 D8CF6EC1
    530CC2F5 697C4707 90829982 4339507F F354FAF9
    0F9CD2C2 F7D6FF3D 901D700F F0588104 856B9592
    71D773E2 E76E8EEB 431FB60D 60ABC20B
  0203
    010001

 Host public key for PEM format code:
---- BEGIN SSH2 PUBLIC KEY ----
AAAAB3NzaC1yc2EAAAADAQABAAABAQDKl7zeaXzt6dmrlHWeAE0VyLlRFoe3mwxW
mMWCaan00EXtDlOvLt7BoJ30vkWeNLZml7hdIZGgDpLzpef7DnPn8CEkMuiY2XmO
qkke4raXJ0tRor7NhqFEFnSNHkhHqBQ/5QhibrGtgetJoF5k9tGGxOlM2wTFMHS4
OTBaf3vOLGBvbJHqlYttrEbBK4wrHgOY8cCdOvKmnWhn+TDfmSaSmpIWgpFic/xN
2HXURLw3Ht27j2rApM2zrdroU9uGufrbE8yp2M9uwVMMwvVpfEcHkIKZgkM5UH/z
VPr5D5zSwvfW/z2QHXAP8FiBBIVrlZJx13Pi526O60Mftg1gq8IL
---- END SSH2 PUBLIC KEY ----

Public key code for pasting into OpenSSH authorized_keys file :
ssh-dsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDKl7zeaXzt6dmrlHWeAE0VyLlRFoe3mwxWmMWCaan0
0EXtDlOvLt7BoJ30vkWeNLZml7hdIZGgDpLzpef7DnPn8CEkMuiY2XmOqkke4raXJ0tRor7NhqFEFnS
NHkhHqBQ/
5QhibrGtgetJoF5k9tGGxOlM2wTFMHS4OTBaf3vOLGBvbJHqlYttrEbBK4wrHgOY8cCdOvKmnWhn
+TDfmSaSmpIWgpFic/
xN2HXURLw3Ht27j2rApM2zrdroU9uGufrbE8yp2M9uwVMMwvVpfEcHkIKZgkM5UH/
zVPr5D5zSwvfW/z2QHXAP8FiBBIVrlZJx13Pi526O60Mftg1gq8IL dsa-key
```


将客户端上产生的DSA公钥配置到服务器端（上面**display**命令显示信息中黑体部分即为客户端产生的DSA公钥，将其拷贝粘贴至服务器端）。

```
[SSH Server] dsa peer-public-key dsakey001 encoding-type der
[SSH Server-dsa-public-key] public-key-code begin
Info: Enter "DSA key code" view, return the last view with "public-key-code end".
[SSH Server-dsa-key-code] 30820109
[SSH Server-dsa-key-code] 2820100
[SSH Server-dsa-key-code] CA97BCDE 697CEDE9 D9AB9475 9E004D15 C8B95116
[SSH Server-dsa-key-code] 87B79B0C 5698C582 69A9F4D0 45ED0E53 AF2EDEC1
[SSH Server-dsa-key-code] A09DF4BE 459E34B6 6697B85D 2191A00E 92F3A5E7
[SSH Server-dsa-key-code] FB0E73E7 F0212432 E898D979 8EAA491E E2B69727
[SSH Server-dsa-key-code] 4B51A2BE CD86A144 16748D1E 4847A814 3FE50862
[SSH Server-dsa-key-code] 6EB1AD81 EB49A05E 64F6D186 C4E94CDB 04C53074
[SSH Server-dsa-key-code] B839305A 7F7BCE2C 606F6C91 EA958B6D AC46C12B
[SSH Server-dsa-key-code] 8C2B1E03 98F1C09D 3AF2A69D 6867F930 DF992692
[SSH Server-dsa-key-code] 9A921682 916273FC 4DD875D4 44BC371E DDBB8F6A
[SSH Server-dsa-key-code] C0A4CDB3 ADDAE853 DB86B9FA DB13CCA9 D8CF6EC1
[SSH Server-dsa-key-code] 530CC2F5 697C4707 90829982 4339507F F354FAF9
[SSH Server-dsa-key-code] 0F9CD2C2 F7D6FF3D 901D700F F0588104 856B9592
[SSH Server-dsa-key-code] 71D773E2 E76E8EEB 431FB60D 60ABC20B
[SSH Server-dsa-key-code] 203
[SSH Server-dsa-key-code] 10001
[SSH Server-dsa-key-code] public-key-code end
[SSH Server-dsa-public-key] peer-public-key end
```

在SSH服务器端为SSH用户client002绑定STelnet客户端的dsa公钥。

```
[SSH Server] ssh user client002 assign dsa-key dsakey001
```

3. SSH服务器端开启STelnet服务功能

   # 开启STelnet服务功能。

   ```
   [SSH Server] ssh server-source -i Vlanif 10   //假设客户端使用IP地址10.1.1.1连接服务器，该地址对应的接口为Vlanif 10
   [SSH Server] stelnet server enable
   ```

4. 配置SSH用户client001、client002的服务方式为STelnet

   ```
   [SSH Server] ssh user client001 service-type stelnet
   [SSH Server] ssh user client002 service-type stelnet
   ```

5. STelnet客户端连接SSH服务器

   # 第一次登录，需要使能SSH客户端首次认证功能。使能客户端Client001首次认证功能。

   ```
   <HUAWEI> system-view
   [HUAWEI] sysname client001
   [client001] ssh client first-time enable
   ```

   使能客户端Client002首次认证功能。

   ```
   [client002] ssh client first-time enable
   ```

   # STelnet客户端Client001用password认证方式连接SSH服务器，输入配置的用户名和密码。

   ```
   [client001] stelnet 10.1.1.1
   Please input the username:client001
   Trying 10.1.1.1 ...
   Press CTRL+K to abort
   Connected to 10.1.1.1 ...
   The server is not authenticated. Continue to access it? [Y/N] :y
   Save the server's public key? [Y/N] :y
   The server's public key will be saved with the name 10.1.1.1. Please wait...

   Please select public key type for user authentication [R for RSA; D for DSA; Enter for Skip publickey authentication; Ctrl_C for Can
   cel], Please select [R, D, Enter or Ctrl_C]:d
   Enter password:
   ```

   输入密码，显示登录成功信息如下：

   ```
   <SSH Server>
   ```


STelnet客户端Clent002用dsa认证方式连接SSH服务器。

```
[client002] stelnet 10.1.1.1 user-identity-key dsa
Please input the username:client002
Trying 10.1.1.1 ...
Press CTRL+K to abort
Connected to 10.1.1.1 ...
Please select public key type for user authentication [R for RSA; D for DSA; Enter for Skip publickey
authentication; Ctrl_C for Can
cel], Please select [R, D, Enter or Ctrl_C]:d
<SSH Server>
```

如果登录成功，用户将进入用户视图。如果登录失败，用户将收到**Session is disconnected**的信息。

6. 验证配置结果

在SSH服务器端执行**display ssh server status**命令可以查看到STelnet服务已经使能。执行**display ssh user-information**命令可以查看服务器端SSH用户信息。

查看SSH状态信息。

```
[SSH Server] display ssh server status
 SSH version                     :2.0
 SSH connection timeout          :60 seconds
 SSH server key generating interval  :0 hours
 SSH authentication retries      :3 times
 SFTP server                     :Disable
 Stelnet server                  :Enable
 Scp server                      :Disable
 SSH server source               :0.0.0.0
 ACL4 number                     :0
 ACL6 number                     :0
```

查看SSH用户信息。

```
[SSH Server] display ssh user-information
 User 1:
     User Name           : client001
     Authentication-type  : password
     User-public-key-name : -
     User-public-key-type : -
     Sftp-directory       : -
     Service-type         : stelnet
     Authorization-cmd    : No
 User 2:
     User Name           : client002
     Authentication-type  : dsa
     User-public-key-name : dsakey001
     User-public-key-type : dsa
     Sftp-directory       : -
     Service-type         : stelnet
     Authorization-cmd    : No
```

配置文件

- SSH服务器的配置文件

```
#
sysname SSH Server
#
dsa peer-public-key dsakey001 encoding-type der
 public-key-code begin
 30820109
   02820100
     CA97BCDE 697CEDE9 D9AB9475 9E004D15 C8B95116 87B79B0C 5698C582 69A9F4D0
     45ED0E53 AF2EDEC1 A09DF4BE 459E34B6 6697B85D 2191A00E 92F3A5E7 FB0E73E7
     F0212432 E898D979 8EAA491E E2B69727 4B51A2BE CD86A144 16748D1E 4847A814
     3FE50862 6EB1AD81 EB49A05E 64F6D186 C4E94CDB 04C53074 B839305A 7F7BCE2C
     606F6C91 EA958B6D AC46C12B 8C2B1E03 98F1C09D 3AF2A69D 6867F930 DF992692
     9A921682 916273FC 4DD875D4 44BC371E DDBB8F6A C0A4CDB3 ADDAE853 DB86B9FA
     DB13CCA9 D8CF6EC1 530CC2F5 697C4707 90829982 4339507F F354FAF9 0F9CD2C2
```



```
    F7D6FF3D 901D700F F0588104 856B9592 71D773E2 E76E8EEB 431FB60D 60ABC20B
   0203
    010001
 public-key-code end
peer-public-key end
#
aaa
 local-user client001 password irreversible-cipher $1a$gRNl~ukoL~0.WU)C2]~2a}Cz/Y0-u8M{j@Ql6/
xHryO-Y7m{=A>kWc.-q}>*$
 local-user client001 privilege level 3
 local-user client001 service-type ssh
#
stelnet server enable
ssh user client001
ssh user client001 authentication-type password
ssh user client001 service-type stelnet
ssh user client002
ssh user client002 authentication-type dsa
ssh user client002 assign dsa-key dsakey001
ssh user client002 service-type stelnet
ssh server-source -i Vlanif 10
#
user-interface vty 0 4
 authentication-mode aaa
#
return
```

- SSH客户端Client001的配置文件

```
#
sysname client001
#
ssh client first-time enable
#
return
```

- SSH客户端Client002的配置文件

```
#
sysname client002
#
ssh client first-time enable
#
return
```

6.10 登录设备命令行界面失败处理办法

6.10.1 通过 Console 口登录设备失败

故障现象

通过Console口登录设备失败。

操作步骤

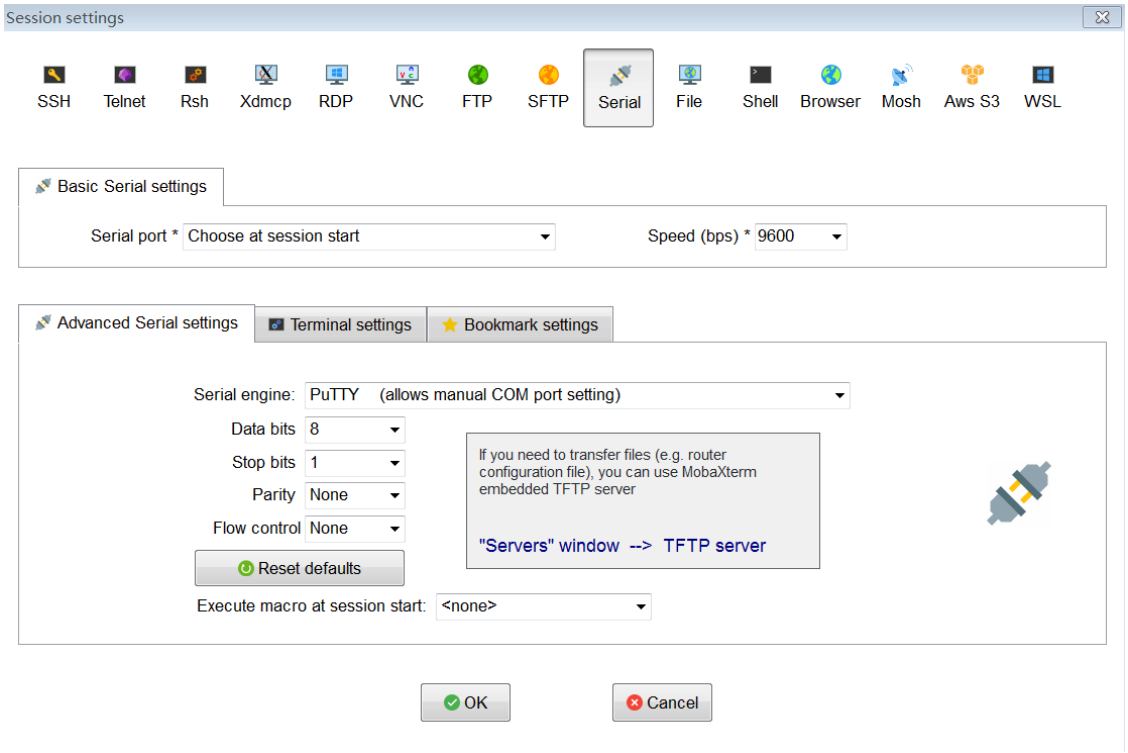
步骤1 核对通信参数，确认是否配置正确。（此处使用第三方软件MobaXterm为例进行介绍）

确认设置的连接端口是否正确。有些PC上会有多个串口，每个串口都有对应的编号，在设置连接端口时，需要选择连接的端口对应的编号。

确认PC的串口物理属性是否与设备的Console口属性保持一致，如图6-6所示。在设备Console口属性没有改变的情况下，属性参数为：

- 波特率：9600
- 数据位：8
- 奇偶校验位：无
- 停止位：1
- 流控：无

图 6-6 设置连接的接口以及通信参数



步骤2 确认串口线缆连接是否牢固且能正常使用。可以考虑更换一根确定之前使用没有问题的串口线缆。

步骤3 如果能登录到认证界面，但输入正确的用户名和密码后提示认证失败，此时可能是Console用户界面的认证方式配置有误。请通过其他方式登录设备（例如Telnet），确认在AAA视图下是否执行了**local-user** *user-name* **service-type terminal**命令为Console登录的用户配置接入类型；如果Telnet等远程方式无法登录，则需要通过BootLoad清除Console口的登录信息，具体操作方式请参见“BootLoad菜单操作”中的“清除Console登录密码”。

----结束

6.10.2 通过 Telnet 登录设备失败

故障现象

通过Telnet方式登录设备失败。

操作步骤

步骤1 查看设备是否配置了Telnet服务器端的源接口或源地址。

从Console口登录到设备，执行命令**display current-configuration | include telnet**，查看是否配置**telnet server-source**或**telnet ipv6 server-source**。如果没有此配置，可以执行命令行**telnet server-source**或**telnet ipv6 server-source**配置Telnet服务器端的源接口或IPv6源地址。

步骤2 查看登录设备的用户数是否到达了上限。

从Console口登录到设备，执行命令**display users**，查看当前的VTY通道是否全部被占用。缺省情况下，VTY通道允许的最大用户数是5个，可以先执行命令**display user-interface maximum-vty**，查看当前VTY通道允许的最大用户数。

如果当前的用户数已经达到上限，可以执行命令**user-interface maximum-vty** 15，将VTY通道允许的最大用户数扩展到15个。然后在扩展后的VTY用户界面配置支持的协议类型、认证方式和用户级别。

步骤3 查看设备上VTY类型用户界面视图下是否配置了ACL。（以Telnet IPv4为例）

在Telnet服务器端上执行命令**user-interface vty**进入用户界面视图，执行命令**display this**，查看VTY用户界面是否配置了ACL限制，如果配置了ACL限制，请记录该ACL编号。

在Telnet服务器端上执行命令**display acl** *acl-number*，查看该访问控制列表中是否**deny**了Telnet客户端的地址。如果**deny**客户端的IP地址，则在ACL视图下，执行命令**undo rule** *rule-id*，删除**deny**规则，再执行相应的命令修改访问控制列表，允许客户端的IP地址访问。

步骤4 查看VTY类型用户界面视图下允许接入的协议配置是否正确。

在Telnet服务器端上执行命令**user-interface vty**进入用户界面视图，执行命令**display this**，查看VTY用户界面的protocol inbound是否为telnet或者all（缺省情况下，系统支持协议SSH）。如果不是，执行命令**protocol inbound** { **telnet** | **all** }修改配置，允许telnet类型用户接入设备。

步骤5 查看用户界面视图下是否设置登录认证。

在VTY用户界面视图执行**display this**查看登录认证方式。

- 如果使用命令**authentication-mode password**配置了VTY通道下的登录认证方式为**password**，则必须在登录时输入此密码。
- 如果使用命令**authentication-mode aaa**设置认证方式为**aaa**，则必须使用命令**local-user**创建AAA本地用户。

----结束

6.10.3 通过 STelnet 登录设备失败

故障现象

通过STelnet方式登录设备失败。

操作步骤

步骤1 查看设备是否配置SSH服务器端的源接口或源地址。

通过Console口或Telnet方式登录SSH服务器端，执行命令**display current-configuration | include ssh**，查看是否配置**ssh server-source**或**ssh ipv6 server-source**。如果没有此配置，可以执行命令行**ssh server-source**或**ssh ipv6 server-source**配置SSH服务器端的源接口或IPv6源地址。

步骤2 查看设备的SSH服务是否启动。

通过Console口或Telnet方式登录SSH服务器端，执行命令**display ssh server status**，查看SSH服务器端配置信息。

如果STelnet没有使能，执行如下命令**stelnet [ipv4 | ipv6] server enable**，使能SSH服务器端的STelnet服务。

步骤3 在SSH服务器端上查看VTY类型用户界面视图下允许接入的协议配置是否正确。

在SSH服务器端上执行命令**user-interface vty**进入用户界面视图，执行命令**display this**，查看VTY用户界面的protocol inbound是否为ssh或者all。如果不是，执行命令**protocol inbound** { **ssh** | **all** }修改配置，允许STelnet类型用户接入设备。

步骤4 查看在SSH服务器端是否配置了RSA、DSA或ECC公钥。

设备作为SSH服务器时，必须配置本地密钥对。

在SSH服务器端上执行命令**display rsa local-key-pair public**、**display dsa local-key-pair public**或**display ecc local-key-pair public**查看当前服务器端密钥对信息。如果显示信息为空，则表明没有配置服务器端密钥对，执行命令**rsa local-key-pair create**、**dsa local-key-pair create**或**ecc local-key-pair create**创建。

步骤5 查看SSH服务器端上是否配置了SSH用户。

执行命令**display ssh user-information**，查看SSH用户的配置信息。如果不存在配置信息，请在系统视图下执行命令**ssh user**、**ssh user authentication-type**和**ssh user service-type**，新建SSH用户并配置SSH用户的认证方式和SSH用户的服务方式。

步骤6 查看登录SSH服务器端的用户数是否到达了上限。

从Console口登录到设备，执行命令**display users**，查看当前的VTY通道是否全部被占用。缺省情况下，VTY通道允许的最大用户数是5个，可以先执行命令**display user-interface maximum-vty**，查看当前VTY通道允许的最大用户数。

如果当前的用户数已经达到上限，可以执行命令**user-interface maximum-vty** 15，将VTY通道允许的最大用户数扩展到15个。

步骤7 查看SSH服务器端上VTY类型用户界面下是否绑定了ACL。

在SSH服务器端上执行命令**user-interface vty**进入SSH用户会使用的界面视图，执行命令**display this**，查看VTY用户界面是否配置了ACL限制，如果配置了ACL限制，请记录该ACL编号。

在SSH服务器端上执行命令**display acl** *acl-number*，查看该访问控制列表中是否**deny**了STelnet客户端的地址。如果**deny**客户端的IP地址，则在ACL视图下，执行命令**undo rule** *rule-id*，删除**deny**规则，再执行相应的命令修改访问控制列表，允许客户端的IP地址访问。

步骤8 查看SSH客户端和服务器上SSH版本信息。

在SSH服务器上执行命令**display ssh server status**，查看SSH版本信息。

步骤9 查看SSH客户端是否使能了首次认证功能。

在系统视图下执行命令**display this**，查看是否使能SSH客户端首次认证功能。

如果没有使能SSH客户端首次认证功能，则STelnet客户端第一次登录SSH服务器时，由于对SSH服务器的公钥有效性检查失败，而导致登录服务器失败。执行命令**ssh client first-time enable**使能SSH客户端首次认证功能。

步骤10 查看SSH服务器上是否配置了攻击溯源。

在SSH服务器上执行命令**display auto-defend configuration**，查看攻击溯源的配置信息。

缺省情况下，SSH服务器上使能了攻击溯源功能。如果指定攻击溯源的惩罚措施为丢弃，端口收到的可防范协议报文的速率超过端口防攻击检查阈值时，可能导致用户登录异常。可执行命令**undo auto-defend enable**去使能攻击溯源功能，或者执行命令**undo auto-defend action**去使能攻击溯源的惩罚功能。

----结束

6.11 登录设备 FAQ

6.11.1 为什么 SSH 方式登录设备慢?

当使用SSH方式登录设备时，因DH秘钥交换算法耗时较长，因此登录设备很慢，建议使用ECDH秘钥交换算法。可通过**ssh server key-exchange**配置SSH服务器端的密码交换算法列表。

7 登录设备 Web 网管界面

7.1 通过Web网管登录设备简介
7.2 Web网管登录使用注意事项
7.3 配置通过Web网管登录设备
7.4 登录设备Web界面失败处理办法
7.5 通过Web网管登录设备的FAQ

7.1 通过 Web 网管登录设备简介

定义

Web网管是一种对设备的管理方式，它利用设备内置的Web服务器，为用户提供图形化的操作界面。用户需要从终端通过HTTPS登录到设备，才能利用Web网管对设备进行管理和维护。

目的

用户对设备的管理方式有命令行方式和Web网管方式两种。命令行方式需要用户使用设备提供的命令行对设备进行管理与维护，此方式可实现对设备的精细化管理，但是要求用户熟悉命令行；Web网管方式通过图形化的操作界面，实现对设备直观方便地管理与维护，但是此方式仅可实现对设备部分功能的管理与维护。用户可以根据实际需求，合理选择管理方式。

如果选择命令行方式，用户需要通过Console口、Telnet或STelnet方式登录设备；如果选择Web网管方式，用户需要通过HTTPS登录到设备。

通过Console口、Telnet或STelnet方式登录设备的详细配置，请参见**6 登录设备命令行界面**。

相关概念

在配置通过Web网管登录设备之前，需要了解以下相关概念：

- **HTTP**

  HTTP是Hypertext Transfer Protocol（超文本传输协议）的简称，它用来在Internet上传递Web网页文件信息。HTTP位于TCP/IP协议栈的应用层，传输层采

用面向连接的TCP。HTTP存在安全风险，目前设备仅支持通过安全HTTP（即HTTPS）登录Web网管，不支持通过HTTP登录Web网管。

- **HTTPS**

  HTTPS是Secure HTTP的简称，即安全HTTP。HTTPS通过安全套接层协议SSL（Secure Sockets Layer），使客户端与设备之间交互的数据经过加密处理，并为设备制定基于证书属性的访问控制策略，提高了数据传输的安全性和完整性，保证合法客户端可以安全地访问设备，禁止非法的客户端访问设备，从而实现了对设备的安全管理。

- **SSL策略**

  在配置HTTPS之前，需要在设备上部署SSL策略，并加载相应的数字证书。SSL策略是指设备启动时使用的SSL参数。只有与应用层协议（如HTTP协议）关联后，SSL策略才能生效。

- **数字证书**

  数字证书是由CA签发的一个声明，证明证书主体（证书申请者拥有了证书后即成为证书主体）与证书中所包含的公钥的惟一对应关系。数字证书中包括证书申请者的名称及相关信息、申请者的公钥、签发数字证书的CA的数字签名及数字证书的有效期等内容。数字证书使网上通信双方的身份得到了互相验证，提高了通信的可靠性。

  设备可以加载PEM、ASN1和PFX三种格式的数字证书文件。不同格式的数字证书文件的内容是一样的。

  - PEM是最常用的一种数字证书格式，文件的扩展名是.pem，适用于系统之间的文本模式传输。
  - ASN1是通用的数字证书格式之一，文件的扩展名是.der，是大多数浏览器的默认格式。
  - PFX是通用的数字证书格式之一，文件的扩展名是.pfx，是可移植的二进制格式，可以转换为PEM或ASN1格式。

- **CA（Certificate Authority）**

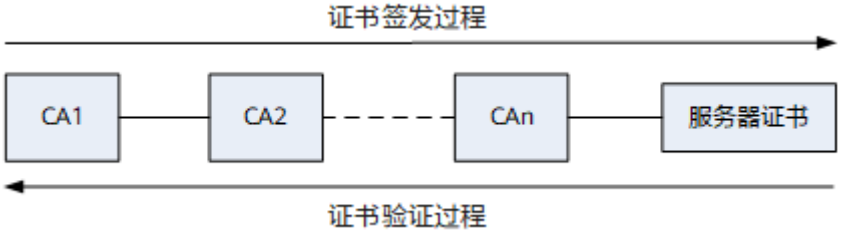
  CA是发放、管理、废除数字证书的机构。CA的作用是检查数字证书持有者身份的合法性，并签发数字证书（在证书上签字），以防证书被伪造或篡改，以及对证书和密钥进行管理。国际上被广泛信任的CA，被称之为根CA。根CA可授权其它CA为其下级CA。CA的身份也需要证明，证明信息在信任证书机构文件中描述。

  例如：CA1作为最上级CA也叫根证书，签发下一级CA2证书，CA2又可以给它的下一级CA3签发证书，以此下去，最终由CAn签发服务器的证书。

  如果服务器端的证书由CA3签发，则在客户端验证证书的过程从服务器端的证书有效性验证开始。客户端先由CA3证书验证服务器端证书的有效性，如果通过则再由CA2证书验证CA3证书的有效性，最后由最上级CA1证书验证CA2证书的有效性。只有通过最上级CA证书即根证书的验证，服务器证书才会验证成功。

  证书签发过程与证书验证过程如图7-1所示。

图 7-1 证书签发过程与证书验证过程示意图



- **证书撤销列表CRL（Certificate Revocation List）**

  CRL由CA发布，它指定了一套证书发布者认为无效的证书。

  数字证书的寿命是有限的，但CA可通过证书撤销过程缩短证书的寿命。CRL指定的寿命通常比数字证书指定的寿命要短。由CA撤销数字证书，意味着CA在数字证书正常到期之前撤销允许使用密钥对的有关声明。在撤销证书到期后，CRL中的有关数据被删除，以缩短CRL列表的大小。

在PC上可以加载验证服务器数字证书以上的各级证书（也称信任证书）及CRL，也可以不加载。如果未加载，在连接建立时浏览器会提示用户是否信任对方，如果点击信任则连接建立成功，不信任则连接无法建立。此时客户端无法对服务器端的数字证书进行验证，但是可以保证双方数据传输的私密性。为了确保访问的是合法的Web服务器，可以在PC上加载信任证书和CRL，加载方法请参考PC操作系统中的帮助信息。

7.2 Web 网管登录使用注意事项

对于当前版本，Web网管登录使用注意事项如下：

- 登录Web网管要求操作系统为Windows7.0、Windows8.0、Windows8.1、Windows10.0或IOS操作系统。
- 登录Web网管要求浏览器为Microsoft Edge、IE10.0、IE11.0、Firefox97.0～Firefox101.0或Chrome93.0～Chrome102.0。如果浏览器版本或浏览器补丁版本不在上述范围内，可能会出现Web页面显示异常，请及时更新浏览器和浏览器补丁。同时，登录Web网管要求浏览器支持Javascript。
- 在使用IE浏览器登录Web网管时，请确保没有禁用IE浏览器安全选项中活动脚本，否则Web网管登录可能会出现异常。
- 登录Web网管的显示器最佳分辨率为1316px，分辨率小于1280px时，系统会给出提示信息。
- 设备的SSL策略默认采用的最低SSL版本为TLS1.2。在通过Web网管登录时，请确保当前浏览器支持的SSL版本与设备当前支持的SSL版本一致，否则Web网管登录可能会出现异常。建议根据弹出页面提示升级浏览器，或者修改SSL的设置。以IE浏览器为例，用户可在“Internet选项”中选择“高级”页签，查看并选择SSL版本。
- Web网管是根据设备电子标签中的Item值来识别设备信息的，而设备硬件驱动通过判断BarCode值来选择是否启动设备。由于BarCode字段值与Item值无法保证一致，所以可能会出现Web网管无法读取并显示设备信息的情况。
- Web系统不支持浏览器自带的后退、前进、刷新等按钮，使用这些按钮可能会导致Web页面直接回退到登录界面。
- 用同一个浏览器的多个窗口登录同一个IP地址的网管时，只保留最后一次登录的会话。如果IP地址和端口号均相同，即同一个Web网管，所有窗口刷新后，先登录的网管使用的账号均会变为最后一次登录时使用的账号；如果IP地址相同，端口号不同，所有窗口刷新后，先登录的网管会提示超时。
- 当设备的软件版本发生变化（例如对软件版本进行了升级或者回退操作），使用Web网管前，建议清除浏览器缓存，否则可能出现Web页面显示异常。
- V200R020C00及之后版本配置Web网管登录时，
  - 对于HTTP IPv4服务，设备默认使能该功能，同时默认将管理IP地址192.168.1.253配置在管理网口或VLANIF1接口下，且将该接口设置为HTTP服务器端的源接口。

  - 对于HTTP IPv6服务，设备默认未使能该功能，用户需通过**http ipv6 server enable**命令使能HTTP IPv6服务功能，并通过**http ipv6 server-source**命令配置HTTP服务器端的IPv6源地址。
- 对于S300、S500，如果设备通过Wi-Fi开局在华为坤灵上线，上线过程中会统一设置登录密码。后续如果需要登录设备Web网管页面，登录密码即为该密码，用户名为admin。

7.3 配置通过 Web 网管登录设备

Web网管方式通过图形化的操作界面，实现对设备直观方便地管理与维护。配置通过Web网管登录设备前，需要确保终端PC和设备之间路由可达。

说明

V200R020C00版本开始，当需要授权客户从非管理接口登录服务器时，需要执行命令指定HTTP服务器端的源接口。

配置通过 Web 网管登录设备的常用功能

增加新的Web用户或者修改用户信息时，配置步骤如下：

1. 开启HTTP服务。
2. 创建Web用户及其登录密码。
3. 配置Web用户的接入类型和用户级别。

操作步骤

1. 开启HTTP服务。

   说明

   HTTP协议存在安全风险，建议您使用HTTPS安全协议

   ```
   <HUAWEI> system-view
   [HUAWEI] http server enable    //缺省情况下，设备的HTTP IPv4服务功能已开启，HTTP IPv6服务功能为关闭状态
   [HUAWEI] http server-source -i MEth0/0/1    //缺省情况下，设备默认将管理IP地址192.168.1.253配置在管理网口或VLANIF1接口下，并将该接口设置为HTTP服务器端的源接口，且设备默认未指定HTTP服务器端的IPv6源地址。
   Warning: The operation will reboot the HTTP server. Continue? [Y/
   N]:y
   Info: Succeeded in setting the source interface of the HTTP server to
   MEth0/0/1.
   Info: Succeeded in starting the HTTP secure
   server.
   Warning: HTTP is not a secure protocol, and it is recommended to use
   HTTPS.
   Info: Succeeded in starting the HTTP server.
   [HUAWEI] quit
   ```

2. 创建Web用户及其登录密码。

   ```
   [HUAWEI] aaa
   [HUAWEI-aaa] local-user admin123 password irreversible-cipher YsHsjx_202206    //创建本地用户admin123，登录密码为YsHsjx_202206
   ```

3. 配置Web用户的接入类型和用户级别。

   ```
   [HUAWEI-aaa] local-user admin123 privilege level 15    //配置本地用户admin123的级别为15
   Warning: This operation may affect online users, are you sure to change the user privilege level ?[Y/
   N]y
   [HUAWEI-aaa] local-user admin123 service-type http    //配置本地用户admin123的接入类型为HTTP
   [HUAWEI-aaa] quit
   ```

4. 查看HTTPS服务器信息。

```
[HUAWEI] display http server
  HTTP Server Status             : enabled
  HTTP Server Port               : 80(80)
  HTTP Timeout Interval          : 20
  Current Online Users           : 3
  Maximum Users Allowed          : 5
  HTTP Secure-server Status      : enabled
  HTTP Secure-server Port        : 443(443)
  HTTP SSL Policy                : ssl_server
  HTTP IPv6 Server Status        : disabled
  HTTP IPv6 Server Port          : 80(80)
  HTTP IPv6 Secure-server Status : disabled
  HTTP IPv6 Secure-server Port   : 443(443)
  HTTP server source interface   : MEth0/0/1
```

说明

缺省情况下，HTTP采用随机生成的自签名证书支持HTTPS。由于自签名证书存在安全风险，因此建议用户替换为官方授信的数字证书，替换方法请参见**加载数字证书文件和绑定SSL策略**。

5. 通过Web登录设备。

完成Web登录设备的常用功能配置后，在用户终端PC上打开浏览器，在地址栏中输入“https://*IP address*”，按回车键后将进入Web网管登录界面。如**图7-2**所示，输入之前配置的Web用户名和密码，并选择Web网管系统的语言。

图 7-2 Web 网管登录界面

说明

- 第一次登录Web网管的账号，在登录过程中会跳转到密码修改界面，必须修改密码。
- 用户密码即将过期或者已经过期时，网管页面也会跳转到密码修改界面。此时用户必须修改密码，才能进入Web网管系统主页面。
- 为提升密码安全性，密码至少同时包含小写字母、大写字母、数字、特殊符号（例如“!”、“$”、“#”和“%”等）这四种形式中的两种，并且不能包括空格和单引号。

配置通过 Web 网管登录设备的其他功能

- 加载Web网页文件

  设备的系统软件中已经集成了Web网页文件并完成了加载，一般不需要单独再操作。如果用户需要对Web网页文件进行升级，可以登录华为公司的官方网站下载独立的Web网页文件，上传到设备并进行加载。

a. 上传Web网页文件到设备。

说明

Web网页文件获取路径：请先登录华为公司企业业务支持网站（**http://support.huawei.com/enterprise**）根据产品型号和版本名称，在“VR版本公共补丁”中点击某一补丁版本，下载所需的Web网页文件，名称为“产品-软件版本号.Web网管文件版本号.web.7z”。

每个Web网页文件对应一个签名文件，签名文件和Web网页文件下载方法相同。

上传必要文件到设备的配置方式，请参见**文件管理**。

b. 加载Web网页文件。

```
<HUAWEI> system-view
[HUAWEI] http server load web.7z
```

c. 开启HTTPS服务。

```
[HUAWEI] http secure-server enable    //缺省情况下，设备的HTTPS IPv4服务功能已开启，HTTPS IPv6服务功能为关闭状态
```

- 加载数字证书文件和绑定SSL策略

a. 上传服务器数字证书、私钥文件到设备。证书中的Subject: CN字段需要与登录设备的域名信息匹配。

说明

可通过SFTP等方式上传服务器数字证书文件和私钥文件，且要保存至security目录。如果设备上没有security目录，可以通过命令**mkdir security**创建。文件上传的具体操作过程请参见**文件管理**。

上传完成后，请在用户视图下执行命令**dir**，对比上传到设备的服务器数字证书文件和私钥文件大小是否与文件服务器上的一致。如果不一致，可能是在文件上传过程中出现异常，请重新上传。

b. 创建SSL策略，并加载数字证书，此处以加载PEM格式证书为例。

```
[HUAWEI] ssl policy http_server
[HUAWEI-ssl-policy-http_server] certificate load pem-cert 1_servercert_pem_dsa.pem key-pair dsa key-file 1_serverkey_pem_dsa.pem auth-code cipher YsHsjx_202206
[HTTPS-Server-ssl-policy-http_server] quit
```

c. 绑定SSL策略并开启HTTPS服务。

```
[HUAWEI] http secure-server ssl-policy http_server
[HUAWEI] http secure-server enable
```

d. 查看加载的数字证书详细信息。

```
[HUAWEI] display ssl policy

    SSL Policy Name: http_server
  Policy Applicants: Config-Webs
      Key-pair Type: DSA
Certificate File Type: PEM
   Certificate Type: certificate
Certificate Filename: 1_servercert_pem_dsa.pem
  Key-file Filename: 1_serverkey_pem_dsa.pem
        Auth-code: ******
              MAC:
         CRL File:
    Trusted-CA File:
       Issuer Name:
 Validity Not Before:
  Validity Not After:
```

命令行功能说明

详细的命令行功能说明请参见《命令参考》手册。

表 7-1 常用功能命令

功能	配置命令	说明
新增AAA本地用户名和密码	**local-user** *user-name* **password irreversible-cipher** *password*	缺省情况下，没有创建本地用户。
配置AAA本地用户的接入类型	**local-user** *user-name* **service-type http**	缺省情况下，本地用户关闭所有的接入类型。
配置本地用户的级别	**local-user** *user-name* **privilege level** *level*	缺省情况下，本地用户的级别为0。
加载Web网页文件	**http server load** { *file-name* | **default** }	缺省情况下，设备已加载系统软件中集成的Web网页文件。
创建SSL策略并进入SSL策略视图	**ssl policy** *policy-name*	缺省为未创建SSL策略。
设备绑定SSL策略	**http secure-server ssl-policy** *policy-name*	缺省情况下，HTTP服务器已配置默认的SSL策略。
开启HTTPS服务	**http** [**ipv6**] **secure-server enable**	缺省情况下，设备的HTTPS IPv4服务功能是开启的，HTTPS IPv6服务功能是关闭的。
指定HTTP服务器端的源接口或IPv6源地址	• **http server-source -i** *interface-type interface-number* • **http ipv6 server-source -a** *ipv6_address* [**-vpn-instance** *vpn_name*]	缺省情况下，HTTP服务器端的源接口为管理网口或VLANIF1，未指定HTTP服务器端的IPv6源地址。

表 7-2 其他功能命令

功能	配置命令	说明
对Web网页文件合法性进行校验	**check file-integrity** *filename signature-filename*	校验失败的文件不能作为系统软件、补丁软件、Web文件或mod文件使用。
HTTPS服务器的端口号	**http** [**ipv6**] **secure-server port** *port-number*	缺省为443。
HTTPS会话的超时时间	**http timeout** *timeout*	缺省为20分钟。
创建SSL算法套定制策略	**ssl cipher-suite-list** *customization-policy-name*	缺省为安全算法。 设备也支持算法套定制功能，通过该命令定制算法套。

功能	配置命令	说明
在SSL算法套定制策略视图定制策略中支持的算法套	**set cipher-suite** { **tls12_ck_dss_aes_128_gcm_sha256** | **tls12_ck_dss_aes_256_gcm_sha384** | **tls12_ck_rsa_aes_128_gcm_sha256** | **tls12_ck_rsa_aes_256_gcm_sha384** }	缺省为没有配置算法套。 系统软件中不包含**tls12_ck_rsa_aes_256_cbc_sha256**、**tls1_ck_dhe_dss_with_aes_128_sha**、**tls1_ck_dhe_dss_with_aes_256_sha**、**tls1_ck_dhe_rsa_with_aes_128_sha**、**tls1_ck_dhe_rsa_with_aes_256_sha**、**tls1_ck_rsa_with_aes_128_sha**和**tls1_ck_rsa_with_aes_256_sha**参数，如需使用，需要安装WEAKEA插件，但是该算法安全性低。为了保证更好的安全性，建议使用其它算法。WEAKEA插件安装方法请参见WEAKEA插件使用指南。
设置SSL策略所采用的最低SSL版本	**ssl minimum version** { **tls1.1** | **tls1.2** | **tls1.3** }	缺省为TLS1.2。 系统软件中不包含**tls1.0**参数，如需使用，需要安装WEAKEA插件，但是该算法安全性低。为了保证更好的安全性，建议配置**tls1.2**参数。WEAKEA插件安装方法请参见WEAKEA插件使用指南。
SSL策略中绑定指定的SSL算法套定制策略	**binding cipher-suite-customization** *customization-policy-name*	缺省为默认的算法套。 绑定的SSL算法套定制策略中如果仅有一种类型的算法（RSA或DSS），SSL策略需要加载对应类型的证书，确保SSL协商时能成功。
加载PEM格式的数字证书/证书链并指定私钥文件	1. **certificate load pem-cert** *cert-filename* **key-pair** { **dsa** | **rsa** } **key-file** *key-filename* **auth-code cipher** *auth-code* 2. **certificate load pem-chain** *cert-filename* **key-pair** { **dsa** | **rsa** } **key-file** *key-filename* **auth-code cipher** *auth-code*	一个SSL策略只能加载一个证书或者证书链（证书链是指从终端实体证书到根证书的一系列可信任证书构成的证书序列）。如果已经加载了证书或者证书链，加载新证书或者证书链之前必须先执行命令**undo certificate load**卸载旧证书或者证书

功能	配置命令	说明
加载ASN1格式的数字证书并指定私钥文件	**certificate load asn1-cert** *cert-filename* **key-pair** { **dsa** | **rsa** } **key-file** *key-filename*	链。请根据证书类型，选择相应的配置。 加载PEM格式的数字证书或证书链时，根据从CA处获取的是数字证书还是证书链，两条命令选择一条执行。 命令1为加载PEM格式的数字证书并指定私钥文件。 命令2为加载PEM格式的证书链并指定私钥文件。
加载PFX格式的数字证书并指定私钥文件	**certificate load pfx-cert** *cert-filename* **key-pair** { **dsa** | **rsa** } { **mac cipher** *mac-code* | **key-file** *key-filename* } **auth-code cipher** *auth-code*	
强制指定的Web用户下线	**free http user-id** *user-id*	设备最多只支持5个Web用户同时在线。
设置Web网管欢迎语	**web welcome-message** *message*	_
查看当前在线Web用户信息	**display http user** [**username** *username*]	_

7.4 登录设备 Web 界面失败处理办法

故障现象

设备与客户端之间可以ping通，但是Web网管无法登录。

操作步骤

步骤1 检查HTTPS服务是否开启。

- 对于HTTPS IPv4

  缺省情况下，HTTPS IPv4服务功能是开启的。在系统视图下执行命令**display this**，查看是否有**undo http secure-server enable**的配置。如果有，说明HTTPS IPv4服务被人为关闭。

  用户可以在系统视图下执行命令**http secure-server enable**，开启HTTPS IPv4服务。

- 对于HTTPS IPv6

  缺省情况下，HTTPS IPv6服务功能是关闭的。用户可以在系统视图下执行命令**http ipv6 secure-server enable**，开启HTTPS IPv6服务。

步骤2 检查设备上是否配置了HTTP服务器端的源接口或IPv6源地址。

- 对于HTTPS IPv4

  在系统视图下执行命令**display this**，查看是否有**http server-source**的配置。如果没有，可以在系统视图下执行命令**http server-source**，配置HTTP服务器端的源接口。

- 对于HTTPS IPv6

在系统视图下执行命令**display this**，查看是否有**http ipv6 server-source**的配置。如果没有，可以在系统视图下执行命令**http ipv6 server-source**，配置HTTP服务器端的IPv6源地址。

步骤3 检查在线Web用户是否已经达到上限。

在设备上执行命令**display http user**，查看当前在线的Web用户是否已经达到5个。

目前，设备只支持5个Web用户同时在线。如果长时间无操作的用户占用了Web通道资源，可能导致其它用户无法登录。管理员可以执行命令**free http user-id** *user-id*，强制长时间无操作的Web用户下线。

步骤4 检查设备上是否配置了对Web用户进行访问控制。

- 对于HTTPS IPv4

  在系统视图下执行命令**display this**，查看是否有**http acl** *acl-number*的配置。如果有，请记录该*acl-number*。

  在任意视图下执行命令**display acl** *acl-number*，查看该访问控制列表中是否deny了Web用户客户端的IPv4地址。如果是，则在ACL视图下执行命令**undo rule** *rule-id*，删除deny规则，再执行相应的命令修改访问控制列表，允许Web用户客户端的IPv4地址通过。

- 对于HTTPS IPv6

  在系统视图下执行命令**display this**，查看是否有**http ipv6 acl** *acl6-number*的配置。如果有，请记录该*acl6-number*。

  在任意视图下执行命令**display acl ipv6** *acl6-number*，查看该访问控制列表中是否deny了Web用户客户端的IPv6地址。如果是，则在ACL6视图下执行命令**undo rule** *rule-id*，删除deny规则，再执行相应的命令修改访问控制列表，允许Web用户客户端的IPv6地址通过。

步骤5 检查Web用户的接入类型是否正确。

在AAA视图下执行命令**display this**，查看Web用户的接入类型是否为HTTP。如果配置中存在**local-user** *user-name* **service-type http**，则说明用户名为*user-name*的用户接入类型为HTTP；如果没有该配置，请在AAA视图下执行命令**local-user** *user-name* **service-type http**，配置Web用户的接入类型为HTTP。

----结束

7.5 通过 Web 网管登录设备的 FAQ

7.5.1 Web 网管功能对环境有什么要求?

使用Web网管功能，只需要在用户终端PC上打开浏览器，在地址栏中输入“https://*IP address*”，按回车键后即可进入Web网管登录界面。

但不同版本的Web网管功能，对操作系统、浏览器的版本会有一定的要求，具体要求请看对应版本“**Web网管登录使用注意事项**”页面中的说明。

7.5.2 如何获取 Web 网页文件?

如果设备的系统软件中已经集成了Web网页文件并完成了加载，则无需再获取Web网页文件。如果设备的系统软件中未集成或者用户需要对Web网页文件进行升级，可以登录华为公司的官方网站下载独立的Web网页文件，上传到设备并进行加载。

Web网页文件获取路径：请先登录华为公司企业业务支持网站（**http://support.huawei.com/enterprise**）根据产品型号和版本名称，在“VR版本公共补丁”中点击某一补丁版本，下载所需的Web网页文件，名称为“产品-软件版本号.Web网管文件版本号.web.7z”。

下载完成后，请对比下载的Web网页文件大小是否与网站上一致。如果不一致，可能是在文件下载过程中出现异常，请重新下载。

7.5.3 为什么登录 Web 网管后只有几个操作选项?

Web用户的级别为3级以下时为监控用户，监控用户只有ping和tracert的操作权限；Web用户的级别为3级或3级以上时为管理用户，管理用户有所有Web页面的操作权限。

可以在AAA视图下执行命令**local-user** *user-name* **privilege level** *level*，配置Web用户的级别为3级或3级以上，即可具备所有Web页面的操作权限。

7.5.4 如何修改 Web 登录密码?

如果忘记了Web登录密码或者希望修改Web登录密码，用户可以通过Console口、STelnet或Telnet等方式登录交换机后设置新的Web登录密码。

须知

使用Telnet协议存在安全风险，建议使用Console口或STelnet V2登录设备。

以用户名为**admin123**，新密码为YsHsjx_202206为例，配置如下。

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] local-user admin123 password irreversible-cipher YsHsjx_202206
[HUAWEI-aaa] local-user admin123 service-type http
[HUAWEI-aaa] local-user admin123 privilege level 15
Warning: This operation may affect online users, are you sure to change the user privilege level ?[Y/N]y
[HUAWEI-aaa] return
<HUAWEI> save
```

7.5.5 Web 和 HTTP 什么区别?

HTTP是Hypertext Transfer Protocol（超文本传输协议）的简称，它用来在Internet上传递Web网页文件信息。HTTP位于TCP/IP协议栈的应用层，传输层采用面向连接的TCP。

综上所述，HTTP是一种协议，Web是一种对设备的管理方式。通过Web网管对设备进行管理与维护依赖于HTTP协议。

8 文件管理

8.1 文件系统简介
8.2 设备支持的文件管理方式
8.3 管理本地文件
8.4 访问其他设备的文件
8.5 文件管理的配置举例
8.6 文件管理的常见配置错误
8.7 文件管理FAQ

8.1 文件系统简介

文件系统

文件系统是指对存储器中文件、目录的管理，包括创建、删除、修改文件和目录，以及显示文件的内容等。

存储器

设备支持的存储器为Flash。

文件的命名规则

字符串形式，不支持空格，不区分大小写。文件名有两种表示方式：文件名、路径+文件名。

- 文件名

  如果直接使用文件名，则表示当前工作路径下的文件。文件名的长度范围是1～64。
- 路径+文件名

  格式为**drive + path + filename**，使用这种命名方式可以唯一的标识指定路径下的文件。文件名的长度范围是1～64，路径+文件名的总长度范围是1～160。

  drive是设备中的存储器，命名为**flash:**。

如果设备在堆叠情况下，**drive**的命名如下：

- flash：堆叠系统中主交换机Flash存储器根目录。
- 堆叠ID#flash：堆叠系统中某设备的Flash存储器根目录。

  例如：**slot2#flash:**是指堆叠ID为2的Flash卡。

path是指存储器中目录以及子目录，即路径。目录名使用的字符不可以是空格、“~”、“*”、“/”、“\”、“:”、“'”和“"”等字符，不区分大小写。

设备支持的路径可以是绝对路径也可以是相对路径。指定根目录（指定**drive**）的路径是绝对路径，相对路径有相对于根目录（即当前的存储器目录）的路径和相对于当前工作路径的路径，路径以“/”开头，则表示相对于根目录的路径。

- 若路径为“flash:/my/test/”，这是绝对路径。
- 若路径为“/selftest/”，表示根目录下的selftest目录，这是相对于根目录的相对路径。
- 若路径为“selftest/”，表示当前工作路径下的selftest目录，这是相对于当前工作路径的相对路径。

例如：**dir flash:/my/test/mytest.txt**，查看**flash:/my/test/**路径下的**mytest.txt**文件的信息，这是一种绝对路径。

如果用相对于根目录的路径，则可以使用命令：**dir /my/test/mytest.txt**。

如果用相对于当前工作路径的路径（若当前工作路径是**flash:/my/**），则使用命令**dir test/mytest.txt**。

说明

- 文件名在文件操作命令格式中统一用**filename**表示。
- 目录在文件操作命令中统一用**directory**表示，目录的格式即为**drive + path**。

8.2 设备支持的文件管理方式

设备在进行文件管理的过程中，可以分别充当服务器和客户端的角色：

- 设备作为服务器：可以从终端访问设备，实现对本设备文件的管理，以及与终端间的文件传输操作。
- 设备作为客户端访问其他设备（服务器）：可以实现管理其他设备上的文件，以及与其他设备间进行文件传输操作。

对于TFTP方式，设备只支持客户端功能；对于FTP、SFTP、SCP以及FTPS方式，设备均支持服务器与客户端功能。

各种文件管理方式的应用场景，优缺点如表8-1所示，用户可以根据需求选择其中一种方式。

表 8-1 文件管理方式

文件管理方式	应用场景	优点	缺点
直接登录系统	通过Console口、Telnet或STelnet方式登录设备，对存储器、目录和文件进行管理。特别是对存储器的操作需要通过此种方式。	对存储器、目录和文件的管理直接通过登录设备完成，方便快捷。	只是对本设备进行文件操作，无法进行文件的传输。
FTP（File Transfer Protocol）	适用于对网络安全性要求不是很高的文件传输场景中，广泛用于版本升级等业务中。	• 配置较简单，支持文件传输以及文件目录的操作。 • FTP可以在两个不同文件系统主机之间传输文件。 • 具有授权和认证功能。	明文传输数据，存在安全隐患。
TFTP（Trivial File Transfer Protocol）	在网络条件良好的实验室局域网中，可以使用TFTP进行版本的在线加载和升级。适用于客户端和服务器之间，不需要复杂交互的环境。	TFTP所占的内存要比FTP小。	• 设备只支持TFTP客户端功能。 • TFTP只支持文件传输，不支持交互。 • TFTP没有授权和认证，且是明文传输数据，存在安全隐患，易于网络病毒传输以及被黑客攻击。
SFTP（Secure File Transfer Protocol）	适用于网络安全性要求高的场景，目前被广泛用于日志下载、配置文件备份等业务中。	• 数据进行了严格加密和完整性保护，安全性高。 • 支持文件传输及文件目录的操作。 • 在设备上可以同时配置SFTP功能和普通FTP功能。（这一点与FTPS方式相比：FTPS是不可以同时提供FTPS和普通FTP功能的。）	配置较复杂。

文件管理方式	应用场景	优点	缺点
SCP（Secure Copy Protocol）	适用于网络安全性要求高，且文件上传下载效率高的场景。	• 数据进行了严格加密和完整性保护，安全性高。 • 客户端与服务器连接的同时完成文件的上传下载操作（即连接和拷贝操作使用一条命令完成），效率较高。	配置较复杂（与SFTP方式的配置非常类似），且不支持交互。
FTPS（FTP over SSL（Secure Sockets Layer））	适用于网络安全性要求高，且不提供普通FTP功能的场景。	利用数据加密、身份验证和消息完整性验证机制，为基于TCP可靠连接的应用层协议提供安全性保证。	• 配置较复杂，需要预先从CA处获得一套证书。 • 若配置FTPS服务，则普通的FTP服务功能必须关闭。

直接登录系统、FTP、TFTP方式，理解和配置都比较简单，下面主要介绍下另外几种文件管理方式。

SFTP 方式

SFTP是SSH协议的一部分，利用SSH协议提供的安全通道，使得远程用户可以安全地登录设备进行文件管理和文件传输等操作，为数据传输提供了更高的安全保障。同时，设备支持客户端的功能，用户可以从本地设备安全登录到远程SSH服务器上，进行文件的安全传输。

SSH提供的安全性主要有：

- 密文传输：在SSH连接建立初期，双方会通过协商的方式得出双方通信的加密算法和会话密钥，此后双方的通信就是以密文的方式进行，这样非法用户就很难窃取到合法用户的帐户信息。
- 支持基于公钥的认证：设备支持RSA、DSA和ECC三种公钥认证方式。
- 支持对服务器的认证：SSH协议可以通过验证服务器端公钥的方式来对服务器的身份进行认证，从而可以避免“伪服务器”方式的攻击。
- 支持对交互数据的校验：SSH协议支持对数据的完整性和真实性的校验，使用的校验方法是CRC(SSH1.5版本)和基于MD5的MAC算法(SSH2.0版本)。这样可以有效地防止类似于“中间人”的攻击。

SSH连接的建立过程：

1. 协商SSH版本号

   客户端与服务器通过发送的标识版本的字符串选择相互通讯所用的SSH协议版本。
2. 算法协商

   服务器和客户端进行密钥交换算法、加密算法、MAC算法协商的一个交互过程，用于后续的通讯过程。

3. 密钥交换

   根据前面算法协商过程中确定的密钥交换算法，服务器和客户端通过计算获得相同的会话密钥和会话ID。

4. 验证用户身份

   客户端向服务器发送用户身份信息。客户端将采用在服务器端配置的用户验证方式向服务器提出验证请求，直到验证通过或连接超时断开。

   服务器提供公钥认证和密码认证。

   - 在公钥（RSA、DSA和ECC三种）认证方式下，客户端必须生成RSA、DSA和ECC三种密钥对（包含公钥和私钥），并将公钥发送给服务器端。用户发起认证请求时，客户端随机生成一段由私钥加密的密文并发送给服务器，服务器利用客户端的公钥对其进行解密，解密成功就认为用户是可信的，对用户授予相应的访问权限。否则，中断连接。
   - 密码认证依靠AAA实现，与Telnet和FTP类似，支持本地数据库和远程RADIUS服务器验证，服务器对来自客户端的用户名与密码和预先配置的用户名与密码进行比较，如果完全匹配则验证通过。

5. 请求会话

   认证完成后，客户端向服务器提交会话请求。服务器则进行等待，处理客户端的请求。

6. 交互会话

   会话申请成功后，连接进入交互会话模式。在这个模式下，数据在两个方向上双向传送。

说明

在进行SSH连接建立前，需要在服务器端生成本地密钥对（RSA密钥对、DSA密钥对和ECC密钥对），这个密钥对不仅用于生成会话密钥和会话ID，还用于客户端验证服务器身份，同时这也是配置SSH服务器的关键步骤。

SCP 方式

SCP也是SSH协议的一部分，是基于SSH协议的远程文件拷贝技术，实现文件的拷贝，包括上传和下载。SCP文件拷贝命令简单易用，提高了网络维护的效率。

FTPS 方式

FTPS将FTP和SSL（Secure Sockets Layer，安全套接层）结合，又称安全FTP。通过SSL对客户端身份和服务器进行验证，对传输的数据进行加密，SSL为普通FTP服务器提供了安全连接，从而很大程度上改善了普通FTP服务器安全性问题，实现了对设备上文件的安全管理。

配置此方式必须要了解的几个概念：

- CA（Certificate Authority）

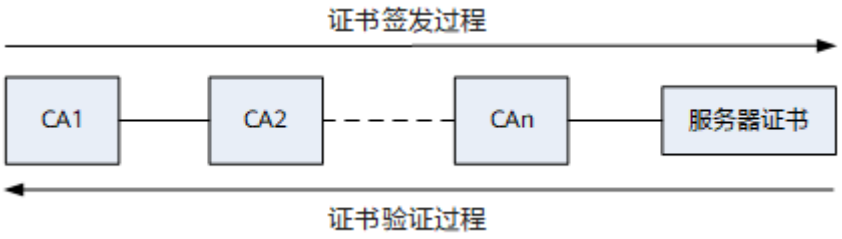
  CA是发放、管理、废除数字证书的机构。CA的作用是检查数字证书持有者身份的合法性，并签发数字证书（在证书上签字），以防证书被伪造或篡改，以及对证书和密钥进行管理。国际上被广泛信任的CA，被称之为根CA。根CA可授权其它CA为其下级CA。CA的身份也需要证明，而证明信息在信任证书机构文件中描述。

  例如：CA1作为最上级CA也叫根证书，签发下一级CA2证书，CA2又可以给它的下一级CA3签发证书，以此下去，最终由CAn签发服务器的证书。

如果服务器端的证书由CA3签发，则在客户端验证证书的过程从服务器端的证书有效性验证开始。先由CA3证书验证服务器端证书的有效性，如果通过则再由CA2证书验证CA3证书的有效性，最后由最上级CA1证书验证CA2证书的有效性。只有通过最上级CA证书即根证书的验证，服务器证书才会验证成功。

证书签发过程与证书验证过程如图8-1所示。

图 8-1 证书签发过程与证书验证过程示意图



- 数字证书

  数字证书实际上是存于计算机上的一个记录，是由CA签发的一个声明，证明证书主体（证书申请者拥有了证书后即成为证书主体）与证书中所包含的公钥的惟一对应关系。数字证书中包括证书申请者的名称及相关信息、申请者的公钥、签发数字证书的CA的数字签名及数字证书的有效期等内容。数字证书的作用使网上通信双方的身份得到了互相验证，提高了通信的可靠性。

  用户必须事先获取信息发送者的公钥证书，以便对信息进行解码认证，同时还需要CA发送给发送者的证书，以便用户验证发送者的身份。

- 证书撤销列表CRL（Certificate Revocation List）

  CRL由CA发布，它指定了一套证书发布者认为无效的证书。

  数字证书的寿命是有限的，但CA可通过证书撤销过程缩短证书的寿命。CRL指定的寿命通常比数字证书指定的寿命要短。由CA撤销数字证书，意味着CA在数字证书正常到期之前撤销允许使用密钥对的有关声明。在撤销证书到期后，CRL中的有关数据被删除，以缩短CRL列表的大小。

设备分别作为服务器和客户端的实现方式：

- 从用户终端访问作为FTP服务器的设备

  在作为FTP服务器的设备上部署SSL策略，加载数字证书并使能安全FTP服务器功能后，用户在终端通过支持SSL的FTP客户端软件访问安全FTP服务器，在终端与服务器之间实现文件的安全管理操作。

- 设备作为客户端访问FTP服务器

  在作为FTP客户端的设备上部署SSL策略并加载信任证书机构文件，检查证书持有者身份的合法性，以防证书被伪造或篡改。

8.3 管理本地文件

背景信息

须知

在对设备进行版本文件下载等文件操作过程中，请保持设备的正常供电。否则可能会引起文件损坏或文件系统损坏，从而造成设备存储介质损坏或设备不能正常启动等问题。

8.3.1 通过登录系统进行文件操作

前置任务

在配置通过登录系统进行文件操作之前，需完成以下任务：

- 终端与设备之间路由可达。
- 已从终端登录到设备。

配置流程

用户从终端登录到设备后，可以对存储器、目录及文件进行一系列操作。

以下各操作没有严格顺序，可根据需求选择一种或多种操作项目。

操作步骤

- **对目录进行操作**

表 8-2 目录操作

操作项目	命令	说明
查看当前所处的目录	**pwd**	-
改变当前所处的目录	**cd** *directory*	-
显示目录中的文件和子目录的列表	**dir** [**/all**] [*filename* | *directory* | **/all-filesystems**]	-
创建目录	**mkdir** *directory*	-

操作项目	命令	说明
删除目录	**rmdir** *directory*	• 被删除的目录必须为空目录。 • 目录被删除后，无法从回收站中恢复，原目录下被删除的文件也彻底从回收站中删除。

- **对文件进行操作**

表 8-3 文件操作

操作项目	命令	说明
显示文件的内容	**more** *filename* [*offset*] [**all**]	-
拷贝文件	**copy** *source-filename destination-filename*	• 在拷贝文件前，确保存储器有足够的空间。 • 若目标文件名与已经存在的文件名重名，将提示是否覆盖。
从HTTP服务器下载文件或上传文件到HTTP服务器	**copy** { *source-http-urlname destination-filename* | *source-filename destination-http-urlname* } [**username** *user-name* **password** *password*]	V200R013C00SPC500及之后版本支持。
从HTTPS服务器下载文件或上传文件到HTTPS服务器	**copy** { *source-https-urlname destination-filename* | *source-filename destination-https-urlname* } [**username** *user-name* **password** *password*] **ssl-policy** *ssl-policy*	V200R013C00SPC500及之后版本支持。
移动文件	**move** *source-filename destination-filename*	若目标文件名与已经存在的文件名重名，将提示是否覆盖。
重新命名文件	**rename** *old-name new-name*	-
压缩文件	**zip** *source-filename destination-filename*	-
解压缩文件	**unzip** *source-filename destination-filename*	-

操作项目	命令	说明
删除文件	**delete** [**/unreserved**] [**/quiet**] { *filename* | *devicename* }	此命令不能删除目录。 **须知** 如果使用参数**/unreserved**，则删除后的文件不可恢复。
恢复删除的文件	**undelete** { *filename* | *devicename* }	执行**delete**命令（不带**/unreserved**参数）后，文件将被放入回收站中。可以执行此命令恢复回收站中被删除的文件。
彻底删除回收站中的文件	**reset recycle-bin** [*filename* | *devicename*]	需要永久删除回收站中的文件时，可进行此操作。
进入系统视图	**system-view**	-
运行批处理文件	**execute** *batch-filename*	一次进行多项处理时，可进行此操作。编辑好的批处理文件要预先保存在设备的存储器中。

说明

当对文件执行操作命令时，若出现错误提示信息“Cannot xxx, because it may be locked or no lock available.”，请等待一段时间后再执行该命令。若多次执行命令后仍出现该提示，请联系技术支持人员处理。

- **对存储器进行操作**

当某存储器上的文件系统出现异常时，终端会给出提示信息，建议修复异常。

当文件系统的异常无法修复或者确认不再需要存储器上的所有数据时，可格式化存储器。格式化会清空存储器中的所有文件和目录。

须知

格式化存储器，会导致数据无法恢复，请慎用。

表 8-4 存储器的操作

操作项目	命令	说明
修复文件系统异常的存储器	**fixdisk** *drive*	执行此命令后，如果仍然收到系统建议修复的信息，则表示存储器可能已经损坏。
格式化存储器	**format** *drive*	如果执行此命令后，存储器仍然不可用，则可能是物理原因导致的存储器不可用。

- **配置文件系统提示方式**

  当在设备上进行操作时，系统可以给予提示或警示信息（特别是对于可能导致数据丢失或破坏的操作）。如果需要修改系统对文件操作的提醒方式时，可以进行配置文件系统提示方式的操作。

  表 8-5 配置文件系统提示方式

操作步骤	命令	说明
进入系统视图	**system-view**	-
配置文件系统提示方式	**file prompt { alert | quiet }**	缺省情况下，提示方式为**alert**。 **须知** 如果将文件操作的提醒方式设置为**quiet**，则对由于用户误操作（比如删除文件操作）而导致数据丢失的情况不作提示，请慎用。

----结束

8.3.2 通过 FTP 进行文件操作

前置任务

在通过FTP进行文件操作之前，需完成以下任务：

- 终端与设备之间路由可达。
- 终端支持FTP客户端软件。

配置流程

须知

使用FTP协议存在安全风险，建议使用SFTP V2、SCP或FTPS方式进行文件操作。

从V200R020C00版本开始，当需要授权客户可以登录服务器时，必须执行命令指定服务器端的源接口或源地址。

通过FTP进行文件操作的配置流程如表8-6所示。

表 8-6 通过 FTP 进行文件操作的配置流程

序号	配置任务名称	配置任务说明	配置流程说明
1	配置FTP服务器功能及参数	包括FTP服务器的使能及参数配置：端口号、源地址、超时断连时间。	序号1、2、3之间没有严格的配置顺序。

序号	配置任务名称	配置任务说明	配置流程说明
2	配置FTP本地用户	包括配置本地用户的服务类型、用户级别及FTP用户的授权目录等。	
3	（可选）配置FTP访问控制	包括配置ACL规则及FTP基本访问控制列表，提高FTP访问的安全性。	
4	用户通过FTP访问设备	从终端通过FTP访问设备。	-

缺省配置

表 8-7 缺省配置

参数	缺省值
FTP服务器功能	关闭
端口号	21
FTP用户	没有创建本地用户

操作步骤

- **配置FTP服务器功能及参数**

  表 8-8 配置 FTP 服务器功能及参数

操作步骤	命令	说明
进入系统视图	**system-view**	-
（可选）指定FTP服务器端口号	**ftp** [**ipv6**] **server port** *port-number*	缺省情况下，FTP服务器端口号是21。 如果配置了新的端口号，FTP服务器端先断开当前已经建立的所有FTP连接，然后使用新的端口号开始尝试连接。这样可以有效防止攻击者对FTP服务标准端口的访问。

操作步骤	命令	说明
指定FTP服务器的源地址	• **ftp server-source** { **-a** *source-ip-address* | **-i** *interface-type interface-number* } • **ftp ipv6 server-source -a** *ipv6_address* [**vpn-instance** *vpn_name*]	缺省情况下，未指定FTP服务器的源地址。 配置了服务器的源地址后，登录服务器时，所输入的服务器地址必须与该命令中配置的一致，否则无法成功登录。
使能FTP服务器	**ftp** [**ipv6**] **server enable**	缺省情况下，设备的FTP服务器功能是关闭的。
（可选）配置FTP连接空闲时间	**ftp** [**ipv6**] **timeout** *minutes*	缺省情况下，连接空闲时间为10分钟。 在设定的时间内，如果FTP连接始终处于空闲状态时，系统将自动断开FTP连接。
（可选）设置FTP服务器支持的最大会话数	**ftp** [**ipv6**] **server max-sessions** *max-sessions-number*	缺省情况下，FTP服务器支持的最大会话数是5。

说明

- 如果变更端口号前FTP服务已经启动，则不能变更成功。需执行**undo ftp** [**ipv6**] **server**命令关闭FTP服务，再进行端口号变更。
- 当客户端与设备之间的文件操作结束后，请执行**undo ftp** [**ipv6**] **server**命令，及时关闭FTP服务器功能，从而保证设备的安全。

- **配置FTP本地用户**

当用户通过FTP进行文件操作时，需要在作为FTP服务器的设备上配置本地用户名及口令、指定用户的服务类型以及可以访问的目录，否则用户将无法通过FTP访问设备。

表 8-9 配置 FTP 本地用户

操作步骤	命令	说明
进入系统视图	**system-view**	-
进入AAA视图	**aaa**	-
配置本地用户名和密码	**local-user** *user-name* **password irreversible-cipher** *password*	-
配置本地用户级别	**local-user** *user-name* **privilege level** *level*	**说明** 必须将用户级别配置在3级或3级以上，否则FTP连接将无法成功。

操作步骤	命令	说明
配置本地用户的服务类型为FTP	**local-user** *user-name* **service-type ftp**	缺省情况下，本地用户可以使用所有的接入类型。
配置FTP用户的授权目录	**local-user** *user-name* **ftp-directory** *directory*	缺省情况下，本地用户的FTP目录为空。 当有多个FTP用户且有相同的授权目录时，可以执行**set default ftp-directory** *directory*命令，为FTP用户配置缺省工作目录。此时，不需要通过**local-user** *user-name* **ftp-directory** *directory*命令为每个用户配置授权目录。
配置本地用户的FTP权限	**local-user** *user-name* **ftp-privilege** [*directoryfilename*] { **read** | **write** | **execute** }*	缺省情况下，本地用户的FTP权限为读、写和执行权限。

- **（可选）配置FTP访问控制**

  ACL是一系列有顺序的规则组的集合，这些规则根据数据包的源地址、目的地址、端口号等来描述。ACL通过规则对数据包进行分类，这些规则应用到路由设备，路由设备根据这些规则判断哪些数据包可以接收，哪些数据包需要拒绝。

  用户可以配置FTP访问控制列表，实现只允许指定的客户端登录到设备，以提高安全性。

  ACL规则：

  - 当ACL的rule配置为**permit**时，则允许匹配该rule规则的其他设备与本设备建立FTP连接。
  - 当ACL的rule配置为**deny**时，则拒绝匹配该rule规则的其他设备与本设备建立FTP连接。
  - 当ACL配置了rule，但来自其他设备的报文没有匹配该rule规则时，则拒绝其他设备与本设备建立FTP连接。
  - 当ACL未配置rule时，则允许任何其他设备与本设备建立FTP连接。

  表 8-10 （可选）配置 FTP 访问控制

操作步骤	命令	说明
进入系统视图	**system-view**	-
进入ACL视图	**acl** [**number**] *acl-number*	-

操作步骤	命令	说明
配置ACL规则	**rule** [*rule-id*] { **deny** | **permit** } [**source** { *source-address source-wildcard* | **any** } | **fragment** | **logging** | **time-range** *time-name* | { **vpn-instance** *vpn-instance-name* | **public** }] *	-
退回到系统视图	**quit**	-
配置FTP基本访问控制列表	**ftp** [**ipv6**] **acl** *acl-number*	-

- **用户通过FTP访问设备**

  从终端通过FTP访问设备，可以选择使用Windows命令行提示符或第三方软件。此处以Windows命令行提示符为例进行配置。

  – 执行Windows命令**ftp** *ip-address*，通过FTP方式访问设备。

    此处输入的IP地址为设备上配置的IP地址，且与用户终端IP地址路由可达。

  – 根据提示输入用户名和口令，按Enter键，当出现FTP客户端视图的命令行提示符，如ftp>，此时用户进入了FTP服务器的工作目录。（以下显示信息仅为示意）

```
C:\Documents and Settings\Administrator> ftp 192.168.150.208
连接到 192.168.150.208。
220 FTP service ready.
用户(192.168.150.208:(none)):huawei
331 Password required for huawei.
密码:
230 User logged in.
ftp>
```

- **通过FTP命令进行文件操作**

  用户访问FTP服务器后，可以通过FTP命令进行文件操作，包括目录操作、文件操作、配置文件传输方式、查看FTP命令在线帮助等。

  说明

  用户的操作权限受限于服务器上对该用户的权限设置。

  由于文件系统对根目录下的文件个数有限制，当根目录中文件个数大于50个时，继续在根目录中创建文件可能会失败。

  以下各操作没有严格顺序，可根据需求选择一种或多种操作项目。

表 8-11 通过 FTP 命令进行文件操作

操作项目	命令	说明
改变服务器上的工作路径	**cd** *remote-directory*	-

操作项目	命令	说明
改变服务器的工作路径到上一级目录	**cdup**	-
显示服务器工作路径	**pwd**	-
显示或者改变客户端的工作路径	**lcd** [*local-directory*]	与**pwd**不同的是，**lcd**命令执行后显示的是客户端的本地工作路径，而**pwd**显示的则是远端服务器的工作路径。
在服务器上创建目录	**mkdir** *remote-directory*	创建的目录可以为字母和数字等的组合，但不可以为<、>、？ 、\、： 等特殊字符。
在服务器上删除目录	**rmdir** *remote-directory*	-
显示服务器上指定目录或文件的信息	**dir/ls** [*remote-filename* [*local-filename*]]	• **ls**命令只能显示出目录/文件的名称，而**dir**命令可以查看目录/文件的详细信息，如大小，创建日期等。 • 如果指定远程文件时没有指定路径名称，那么系统将在用户的授权目录下搜索指定的文件。
删除服务器上指定文件	**delete** *remote-filename*	-
上传单个或多个文件	**put** *local-filename* [*remote-filename*] 或 **mput** *local-filenames*	• **put**命令是上传单个文件。 • **mput**命令是上传多个文件。
下载单个或多个文件	**get** *remote-filename* [*local-filename*] 或 **mget** *remote-filenames*	• **get**命令是下载单个文件。 • **mget**命令是下载多个文件。
配置传输文件的数据类型为ASCII模式或二进制模式	**ascii** 或 **binary**	二选一 • 缺省情况下，文件传输方式为ASCII模式。 • 传输文本文件使用ASCII方式，传输程序、系统软件、数据库文件等使用二进制模式。

操作项目	命令	说明
配置文件传输方式为被动方式或主动方式	**passive** 或 **undo passive**	二选一 缺省情况下，数据传输方式是主动方式。
查看FTP命令的在线帮助	**remotehelp** [*command*]	-
使能系统的提示功能	**prompt**	缺省情况下，不使能信息提示。
打开verbose开关	**verbose**	如果打开verbose开关，将显示所有FTP响应，包括FTP协议信息，以及FTP服务器返回的详细信息。

- **（可选）更改登录用户**

  设备可以在不退出FTP客户端视图的情况下，以其他的用户名登录到FTP服务器。所建立的FTP连接，与执行**ftp**命令建立的FTP连接完全相同。

操作步骤	命令	说明
FTP客户端视图下，更改当前的登录用户	**user** *user-name* [*password*]	更改当前的登录用户后，原用户与服务器的连接将断开。

- **断开与FTP服务器的连接**

  用户可以在FTP客户端视图中选择不同的命令断开与FTP服务器的连接。

操作步骤	命令	说明
终止与服务器的连接，并退回到用户视图	**bye** 或 **quit**	二选一。
终止与服务器的连接，并退回到FTP客户端视图	**close** 或 **disconnect**	

----结束

检查配置结果

- 使用**display** [**ipv6**] **ftp-server**命令，查看FTP服务器的配置和状态信息。
- 使用**display ftp-users**命令，查看登录的FTP用户信息。

8.3.3 通过 SFTP 进行文件操作

前置任务

在配置通过SFTP进行文件操作之前，需完成以下任务：

- 终端与设备之间有可达路由。
- 终端上已安装SSH客户端软件。

配置流程

说明

使用SFTP V1协议存在安全风险，建议使用SFTP V2或FTPS方式进行文件操作。

从V200R020C00版本开始，当需要授权客户可以登录服务器时，必须执行命令指定服务器端的源接口或源地址。

通过SFTP进行文件操作的配置流程如表8-12所示。

表 8-12 通过 SFTP 进行文件操作的配置流程

序号	配置任务名称	配置任务说明	配置流程说明
1	配置SFTP服务器功能及参数	包括服务器本地密钥对生成、SFTP服务器功能的使能及服务器参数的配置：端口号、源地址、密钥对更新时间、SSH认证超时时间、SSH验证重试次数等。	序号1、2、3之间没有严格的配置顺序。
2	配置SSH用户登录的用户界面	包括VTY用户界面的用户验证方式、VTY用户界面支持SSH协议及其它基本属性。	
3	配置SSH用户	包括SSH用户的创建、认证方式、服务方式、SFTP服务授权目录等。	
4	用户通过SFTP协议访问设备	从终端通过SSH客户端软件访问设备。	-

缺省配置

表 8-13 缺省配置

参数	缺省值
SFTP服务器功能	关闭
端口号	22

参数	缺省值
服务器密钥对更新时间	0，表示永不更新
SSH认证超时时间	60秒
SSH验证重试次数	3
SSH用户	没有创建
SSH用户的服务方式	空，即不支持任何服务方式
SSH用户的SFTP服务授权目录	flash:

操作步骤

- **配置SFTP服务器功能及参数**

  表 8-14 配置 SFTP 服务器功能及参数

操作步骤	命令	说明
进入系统视图	**system-view**	-
生成本地密钥对	**rsa local-key-pair create**、**dsa local-key-pair create**或**ecc local-key-pair create**	根据生成的密钥类型，三选一。 密钥对生成后，可以执行**display rsa local-key-pair public**、**display dsa local-key-pair public**或**display ecc local-key-pair public**命令查看本地密钥对中的公钥信息。 **说明** 密钥对长度越大，密钥对安全性就越好，建议使用最大的密钥对长度。
指定SSH服务器端的源地址	• **ssh server-source -i** *interface-type interface-number* • **ssh ipv6 server-source -a** *ipv6_address* [**-vpn-instance** *vpn_name*]	缺省情况下，未指定SSH服务器端的源地址。
使能SFTP服务器功能	**sftp [ipv4 | ipv6] server enable**	缺省情况下，SFTP服务为关闭状态。

操作步骤	命令	说明
（可选）配置SSH服务器端的密钥交换算法列表	**ssh server key-exchange** { **dh_group14_sha256** | **dh_group15_sha512** | **dh_group16_sha512** | **dh_group_exchange_sha256** | **ecdh_sha2_nistp256**| **ecdh_sha2_nistp384**| **ecdh_sha2_nistp521**}*	缺省情况下，SSH服务器支持所有的密钥交换算法。 系统软件中不包含**dh_group_exchange_sha1**、**dh_group14_sha1和dh_group1_sha1**参数，如需使用，需要安装WEAKEA插件，但是该算法安全性低。为了保证更好的安全性，建议使用其它算法。WEAKEA插件安装方法请参见WEAKEA插件使用指南。
（可选）配置SSH服务器端的加密算法列表	**ssh server cipher** { **aes128_ctr** | **aes256_ctr** } *	缺省情况下，不安装WEAKEA插件，SSH服务器只支持**aes128_ctr**和**aes256_ctr**算法，不可以使用**undo ssh server cipher**命令，安装WEAKEA插件后，增加支持**aes256_cbc**、**aes128_cbc**、**3des_cbc**和**des_cbc**算法，并且可以使用**undo ssh server cipher**命令。 系统软件中不包含**aes256_cbc**、**aes128_cbc**、**3des_cbc**和**des_cbc**参数，如需使用，需要安装WEAKEA插件，但是该算法安全性低。为了保证更好的安全性，建议配置**aes256_ctr**或**aes128_ctr**参数。WEAKEA插件安装方法请参见WEAKEA插件使用指南。

操作步骤	命令	说明
（可选）配置SSH服务器上的校验算法列表	**ssh server hmac** {**sha2_256** }	缺省情况下，不安装WEAKEA插件，SSH服务器只支持**sha2_256**校验算法，不可以使用**undo ssh server hmac**命令，安装WEAKEA插件后，增加支持**sha2_256_96**、**sha1**、**sha1_96**、**md5**和**md5_96**校验算法，并且可以使用**undo ssh server hmac**命令。 系统软件中不包含**sha2_256_96**、**sha1**、**sha1_96**、**md5**和**md5_96**参数，如需使用，需要安装WEAKEA插件，但是该算法安全性低。为了保证更好的安全性，建议配置**sha2_256**参数。WEAKEA插件安装方法请参见WEAKEA插件使用指南。
（可选）配置与SSH客户端进行Diffie-hellman-group-exchange密钥交换时，支持的最小密钥长度	**ssh server dh-exchange min-len** *min-len*	缺省情况下，SSH服务器与客户端进行Diffie-hellman-group-exchange密钥交换时，支持的最小密钥长度为1024字节。
（可选）端口号	**ssh [ipv4 | ipv6] server port** *port-number*	缺省情况下，SSH服务器的端口号是22。 如果配置了新的端口号，SSH服务器端先断开当前已经建立的所有SSH连接，然后使用新的端口号开始尝试连接。这样可以有效防止攻击者对SSH服务标准端口的访问，确保安全性。

操作步骤	命令	说明
（可选）服务器密钥对更新时间	**ssh server rekey-interval** *hours*	缺省情况下，SSH服务器密钥对的更新时间间隔为0，表示永不更新。 配置服务器密钥对更新时间，使得当SSH服务器的更新周期到达时，自动更新服务器密钥对，从而可以保证安全性。 该命令只在SSH1.X版本生效。SSH1.X的安全性较低，不推荐使用。
（可选）配置SSH服务器重协商密钥时的参数	**ssh server rekey** { **time** *rekey-time* | **data-limit** *data-limit* | **max-packet** *max-packet* } *	缺省情况下，SSH服务器触发密钥重协商的时间间隔为60分钟，重协商密钥时收发数据大小上限为1000MB，重协商密钥时收发数据包个数上限为268435456（2^28）个。
（可选）指定SSH服务器的公钥算法	**ssh server publickey** { **dsa** | **ecc** | **rsa** | **rsa_sha2_256** | **rsa_sha2_512** } *	缺省情况下，DSA、ECC、RSA、RSA_SHA2_256、RSA_SHA2_512公钥算法都是开启的。
（可选）SSH认证超时时间	**ssh server timeout** *seconds*	缺省情况下，SSH连接认证超时时间为60秒。
（可选）SSH验证重试次数	**ssh server authentication-retries** *times*	缺省情况下，SSH连接的验证重试次数为3。
（可选）配置访问控制列表	**ssh** [**ipv6**] **server acl** *acl-number*	缺省情况下，没有配置访问控制列表。 配置了访问控制列表，可控制哪些客户端能以SSH方式访问本设备。

- 生成本地RSA密钥对时，将同时生成两个密钥对：服务器密钥对和主机密钥对，二者分别包括一个公钥和一个私钥。服务器密钥对和主机密钥对的长度均为2048位。
- 生成本地DSA密钥对时，只生成一个主机密钥对，长度可为1024、2048。缺省情况下，密钥对的长度为2048位。
- 生成本地ECC密钥对时，只生成一个主机密钥对，长度可为256、384、521。缺省情况下，密钥对的长度为521位。

- **配置SSH用户登录的用户界面**

  使用SFTP协议，用户将通过VTY用户界面登录设备，所以需要配置VTY用户界面的相关属性

表 8-15 配置 SSH 用户登录的用户界面

操作步骤	命令	说明
进入系统视图	**system-view**	-
进入VTY用户界面视图	**user-interface vty** *first-ui-number* [*last-ui-number*]	-
配置VTY用户界面的验证方式为AAA	**authentication-mode aaa**	缺省情况下，VTY用户界面没有验证方式。 必须配置VTY用户界面验证方式为AAA验证，否则**protocol inbound ssh**不能配置成功，用户也将无法登录设备。
配置VTY用户界面支持SSH协议	**protocol inbound ssh**	缺省情况下，用户界面支持的协议是SSH。 如果不配置某个或某几个VTY用户界面支持SSH协议，则SSH用户不能登录设备。
配置VTY用户界面的用户优先级	**user privilege level** *level*	必须将用户级别配置为3级及3级以上，否则连接不成功。 如果是password认证用户，还可以执行**local-user** *user-name* **privilege level** *level*命令配置本地用户的用户级别为3级及3级以上。
（可选）VTY用户界面其他属性	-	除配置VTY用户界面的验证方式和用户优先级外，VTY用户界面的其他属性包括： ● VTY用户界面的最大个数 ● VTY用户界面的呼入呼出限制 ● VTY用户界面的终端属性 请参见**6.6 配置通过STelnet登录设备**–其他功能命令。

- **配置SSH用户**

配置SSH用户包括配置SSH用户的验证方式，设备支持的认证方式包括RSA、password、password-rsa、DSA、password-dsa、ECC、password-ecc和all。其中：

- password-rsa认证需要同时满足password认证和RSA认证。
- password-dsa认证需要同时满足password认证和DSA认证。
- password-ecc认证需要同时满足password认证和ECC认证。
- all认证是指password认证、RSA、DSA或ECC认证方式满足其中一种即可。

表 8-16 配置 SSH 用户

操作步骤	命令	说明
进入系统视图	**system-view**	-
创建SSH用户	**ssh user** *user-name*	-
配置SSH用户的认证方式	**ssh user** *user-name* **authentication-type** { **password** | **rsa** | **password-rsa** | **dsa** | **password-dsa** | **ecc** | **password-ecc** | **all** }	如果没有使用**ssh user**命令配置相应的SSH用户，则可以直接执行**ssh authentication-type default password**命令为用户配置SSH认证缺省采用密码认证，在用户数量比较多时，对用户使用缺省密码认证方式可以简化配置，此时只需再配置AAA用户即可。 **说明** 当认证方式为all认证时，用户的优先级需根据接入用户选择的认证方式来决定： • 如果接入用户选择的认证方式为password认证，则用户优先级为AAA中设置的用户优先级。 • 如果接入用户选择的认证方式为RSA、DSA或ECC认证，则用户的优先级由用户接入时所采用的VTY界面的优先级决定。 如果SSH用户认证方式为all认证，且存在一个同名AAA用户，那通过这两种方式接入时用户优先级可能不同，请根据需要进行部署。
配置SSH用户的服务方式为SFTP或all	**ssh user** *username* **service-type** { **sftp** | **stelnet** | **all** }	缺省情况下，SSH用户的服务方式是空，即不支持任何服务方式。
配置SSH用户的SFTP服务授权目录	**ssh user** *username* **sftp-directory** *directoryname*	缺省情况下，SSH用户的SFTP服务授权目录是flash:。

- password认证依靠AAA实现，当用户使用password、password-rsa、password-dsa或password-ecc认证方式登录设备时，需要在AAA视图下创建同名的本地用户。
- 如果SSH用户使用password认证，则只需要在SSH服务器端生成本地RSA、DSA或ECC密钥。如果SSH用户使用RSA、DSA或ECC认证，则在服务器端和客户端都需要生成本地RSA、DSA或ECC密钥对，并且服务器端和客户端都需要将对方的公钥配置到本地。

根据上面配置的认证方式，进行选择配置：

- 若对SSH用户进行password认证，请根据**表8-17**进行配置。
- 若对SSH用户进行RSA、DSA或ECC认证，请根据**表8-18**进行配置。
- 若对SSH用户进行password-rsa、password-dsa或password-ecc认证，则AAA用户和RSA、DSA或ECC公共密钥都需要进行配置，即同时配置**表8-17**和**表8-18**。

表 8-17 配置对 SSH 用户进行 password、password-rsa、password-dsa 或 password-ecc 认证

操作步骤	命令	说明
进入系统视图	**system-view**	-
进入AAA视图	**aaa**	-
配置本地用户名和密码	**local-user** *user-name* **password irreversible-cipher** *password*	-
配置本地用户的服务方式	**local-user** *user-name* **service-type ssh**	-
配置本地用户的级别	**local-user** *user-name* **privilege level** *level*	-
退回到系统视图	**quit**	-

表 8-18 配置对 SSH 用户进行 dsa、rsa、ecc、password-dsa、password-rsa 或 password-ecc 认证

操作步骤	命令	说明
进入系统视图	**system-view**	-

操作步骤	命令	说明
进入RSA、DSA或ECC公共密钥视图	**rsa peer-public-key** *key-name* [**encoding-type** { **der** | **openssh** | **pem** }] 、 **dsa peer-public-key** *key-name* **encoding-type** { **der** | **openssh** | **pem** } 或 **ecc peer-public-key** *key-name* **encoding-type** { **der** | **openssh** | **pem** }	-
进入公共密钥编辑视图	**public-key-code begin**	-
编辑公共密钥	*hex-data*	• 键入的公共密钥必须是按公钥格式编码的十六进制字符串，由支持SSH的客户端软件生成。具体操作参见相应的SSH客户端软件的帮助文档。 • 请将RSA、DSA或ECC公钥输入到作为SSH服务器的设备上。
退出公共密钥编辑视图	**public-key-code end**	• 如果未输入合法的密钥编码hex-data，执行本步骤后，将无法生成密钥。 • 如果指定的密钥*key-name*已经在别的窗口下被删除，再执行本步骤时，系统会提示：密钥已经不存在，此时直接退到系统视图。
退出公共密钥视图，回到系统视图	**peer-public-key end**	-
为SSH用户分配RSA、DSA或ECC公钥	**ssh user** *user-name* **assign** { **rsa-key** | **dsa-key** | **ecc-key** } *key-name*	-

- **用户通过SFTP协议访问设备**

从终端通过SFTP访问设备，需要在终端上安装SSH客户端软件。此处以使用第三方软件OpenSSH和Windows命令行提示符为例进行配置。

- OpenSSH软件的安装请参考该软件的安装说明。
- 使用OpenSSH软件从终端访问设备时，需要使用OpenSSH的命令，命令的使用可以参见该软件的帮助文档。
- 只有安装了OpenSSH软件后，Windows命令行提示符才能识别OpenSSH相关命令。

进入Windows的命令行提示符，执行OpenSSH命令，通过SFTP方式访问设备。

当出现SFTP客户端视图的命令行提示符，如sftp>，此时用户进入了SFTP服务器的工作目录。（以下显示信息仅为示意）

```
C:\Documents and Settings\Administrator> sftp sftpuser@10.136.23.5
Connecting to 10.136.23.5...
The authenticity of host '10.136.23.5 (10.136.23.5)' can't be established.
DSA key fingerprint is 46:b2:8a:52:88:42:41:d4:af:8f:4a:41:d9:b8:4f:ee.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.136.23.5' (DSA) to the list of known hosts.

User Authentication
Password:
sftp>
```

- **通过SFTP命令进行文件操作**

  当SFTP客户端登录到SSH服务器之后，用户可以在SFTP客户端进行如表8-19所示的操作。

  以下各操作没有严格顺序，可根据需求选择一种或多种操作项目。

  说明

  在SFTP客户端视图下，文件操作命令不支持联想功能，必须手动输入完整的命令，否则会提示是不支持的命令。

  由于文件系统对根目录下的文件个数有限制，当根目录中文件个数大于50个时，继续在根目录中创建文件可能会失败。

表 8-19 通过 SFTP 文件操作命令进行文件操作

操作项目	命令	说明
改变用户的当前工作目录	**cd** [*remote-directory*]	-
改变用户的工作目录为当前工作目录的上一级目录	**cdup**	-
显示用户的当前工作目录	**pwd**	-
显示指定目录下的文件列表	**dir/ls** [**-l** | **-a**] [*remote-directory*]	**dir**与**ls**执行的效果是一样的。

操作项目	命令	说明
删除服务器上目录	**rmdir** *remote-directory* &<1-10>	一次最多可以删除十个目录。 使用该命令删除目录时，目录中不能有文件，否则会删除失败。
在服务器上创建新目录	**mkdir** *remote-directory*	-
改变服务器上指定的文件的名字	**rename** *old-name new-name*	-
下载远程服务器上的文件	**get** *remote-filename* [*local-filename*]	-
上传本地文件到远程服务器	**put** *local-filename* [*remote-filename*]	-
删除服务器上文件	**remove** *remote-filename* &<1-10>	一次最多可以删除十个文件。
SFTP客户端命令帮助	**help** [**all** | *command-name*]	-

用户也可以在系统视图下执行如下命令下载服务器上的文件或者上传本地文件到远程服务器中:

- IPv4地址：**sftp client-transfile** { **get** | **put** } [**-a** *source-address* | **-i** *interface-type interface-number*] **host-ip** *host-ipv4* [*port*] [[**public-net** | **-vpn-instance** *vpn-instance-name*] | **prefer_kex** *prefer_key-exchange* | **identity-key** { **rsa** | **dsa** | **ecc** } | **prefer_ctos_cipher** *prefer_ctos_cipher* | **prefer_stoc_cipher** *prefer_stoc_cipher* | **prefer_ctos_hmac** *prefer_ctos_hmac* | **prefer_stoc_hmac** *prefer_stoc_hmac* | **-ki** *aliveinterval* | **-kc** *alivecountmax*] * **username** *user-name* **password** *password* **sourcefile** *source-file* [**destination** *destination*]
- IPv6地址：**sftp client-transfile** { **get** | **put** } **ipv6** [**-a** *source-address*] **host-ip** *host-ipv6* [**-oi** *interface-type interface-number*] [*port*] [**-vpn-instance** *vpn-instance-name* | **prefer_kex** *prefer_key-exchange* | **identity-key** { **rsa** | **dsa** | **ecc** } | **prefer_ctos_cipher** *prefer_ctos_cipher* | **prefer_stoc_cipher** *prefer_stoc_cipher* | **prefer_ctos_hmac** *prefer_ctos_hmac* | **prefer_stoc_hmac** *prefer_stoc_hmac* | **-ki** *aliveinterval* | **-kc** *alivecountmax*] * **username** *user-name* **password** *password* **sourcefile** *source-file* [**destination** *destination*]

- **断开与SFTP服务器的连接**

操作步骤	命令	说明
断开与SFTP服务器的连接	**quit**	-

----结束

检查配置结果

- 使用**display ssh user-information** [*username*]命令，在SSH服务器端查看SSH用户信息。
- 使用**display ssh server status**命令，查看SSH服务器的全局配置信息。
- 使用**display ssh server session**命令，在SSH服务器端查看SSH客户端连接会话信息。

8.3.4 通过 SCP 进行文件操作

前置任务

配置通过SCP进行文件操作之前，需完成以下任务：

- 终端与设备之间路由可达。
- 终端上已安装支持SCP的SSH客户端软件。

配置流程

通过SCP进行文件操作的配置流程如表8-20所示。

说明

从V200R020C00版本开始，当需要授权客户可以登录服务器时，必须执行命令指定服务器端的源接口或源地址。

表 8-20 通过 SCP 进行文件操作的配置流程

序号	配置任务名称	配置任务说明	配置流程说明
1	配置SCP服务器功能及参数	包括服务器本地密钥对生成、SCP服务器功能的使能及服务器参数的配置：端口号、源地址、密钥对更新时间、SSH认证超时时间、SSH验证重试次数等。	序号1、2、3之间没有严格的配置顺序。
2	配置SSH用户登录的用户界面	包括VTY用户界面的用户验证方式、VTY用户界面支持SSH协议及其它基本属性。	
3	配置SSH用户	包括SSH用户的创建、认证方式、服务方式等。	
4	用户通过SCP进行文件操作	从终端通过SCP客户端软件实现上传或下载文件的操作。	—

缺省配置

表 8-21 缺省配置

参数	缺省值
SCP服务器功能	关闭
端口号	22
服务器密钥对更新时间	0，表示永不更新
SSH认证超时时间	60秒
SSH验证重试次数	3
SSH用户	没有创建
SSH用户的服务方式	空，即不支持任何服务方式

操作步骤

- **配置SCP服务器功能及参数**

表 8-22 配置 SCP 服务器功能及参数

操作步骤	命令	说明
进入系统视图	**system-view**	-
生成本地密钥对	**rsa local-key-pair create**、**dsa local-key-pair create**或**ecc local-key-pair create**	根据生成的密钥类型，三选一。 密钥对生成后，可以执行**display rsa local-key-pair public**、**display dsa local-key-pair public**或**display ecc local-key-pair public**命令查看本地密钥对中的公钥信息。 **说明** 密钥对长度越大，密钥对安全性就越好，建议使用最大的密钥对长度。
指定SSH服务器端的源地址	• **ssh server-source -i** *interface-type interface-number* • **ssh ipv6 server-source -a** *ipv6_address* [**-vpn-instance** *vpn_name*]	缺省情况下，未指定SSH服务器端的源地址。
使能SCP服务器功能	**scp [ipv4 | ipv6] server enable**	缺省情况下，SCP服务为关闭状态。

操作步骤	命令	说明
（可选）配置SSH服务器端的密钥交换算法列表	**ssh server key-exchange** { **dh_group14_sha256** | **dh_group15_sha512** | **dh_group16_sha512** | **dh_group_exchange_sha256** | **ecdh_sha2_nistp256**| **ecdh_sha2_nistp384**| **ecdh_sha2_nistp521** }*	缺省情况下，SSH服务器支持所有的密钥交换算法。 系统软件中不包含**dh_group_exchange_sha1**、**dh_group14_sha1**和**dh_group1_sha1**参数，如需使用，需要安装WEAKEA插件，但是该算法安全性低。为了保证更好的安全性，建议使用其它算法。WEAKEA插件安装方法请参见WEAKEA插件使用指南。
（可选）配置SSH服务器端的加密算法列表	**ssh server cipher** { **aes128_ctr** | **aes256_ctr** } *	缺省情况下，不安装WEAKEA插件，SSH服务器只支持**aes128_ctr**和**aes256_ctr**算法，不可以使用**undo ssh server cipher**命令，安装WEAKEA插件后，增加支持**aes256_cbc**、**aes128_cbc**、**3des_cbc**和**des_cbc**算法，并且可以使用**undo ssh server cipher**命令。 系统软件中不包含**aes256_cbc**、**aes128_cbc**、**3des_cbc**和**des_cbc**参数，如需使用，需要安装WEAKEA插件，但是该算法安全性低。为了保证更好的安全性，建议配置**aes256_ctr**或**aes128_ctr**参数。WEAKEA插件安装方法请参见WEAKEA插件使用指南。
（可选）配置SSH服务器上的校验算法列表	**ssh server hmac sha2_256**	缺省情况下，不安装WEAKEA插件，SSH服务器只支持**sha2_256**校验算法，不可以使用**undo ssh server hmac**命令，安装WEAKEA插件后，增加支持**sha2_256_96**、**sha1**、**sha1_96**、**md5**和**md5_96**校验算法，并且可以使用**undo ssh server hmac**命令。 系统软件中不包含**sha2_256_96**、**sha1**、**sha1_96**、**md5**和**md5_96**参数，如需使用，需要安装WEAKEA插件，但是该算法安全性低。为了保证更好的安全性，建议配置**sha2_256**参数。WEAKEA插件安装方法请参见WEAKEA插件使用指南。

操作步骤	命令	说明
（可选）配置与SSH客户端进行Diffie-hellman-group-exchange密钥交换时，支持的最小密钥长度	**ssh server dh-exchange min-len** *min-len*	缺省情况下，SSH服务器与客户端进行Diffie-hellman-group-exchange密钥交换时，支持的最小密钥长度为1024字节。
（可选）端口号	**ssh [ipv4 | ipv6] server port** *port-number*	缺省情况下，SSH服务器的端口号是22。 如果配置了新的端口号，SSH服务器端先断开当前已经建立的所有SSH连接，然后使用新的端口号开始尝试连接。这样可以有效防止攻击者对SSH服务标准端口的访问，确保安全性。
（可选）服务器密钥对更新时间	**ssh server rekey-interval** *hours*	缺省情况下，SSH服务器密钥对的更新时间间隔为0，表示永不更新。 配置服务器密钥对更新时间，使得当SSH服务器的更新周期到达时，自动更新服务器密钥对，从而可以保证安全性。 该命令只在SSH1.X版本生效。SSH1.X的安全性较低，不推荐使用。
（可选）配置SSH服务器重协商密钥时的参数	**ssh server rekey** { **time** *rekey-time* | **data-limit** *data-limit* | **max-packet** *max-packet* } *	缺省情况下，SSH服务器触发密钥重协商的时间间隔为60分钟，重协商密钥时收发数据大小上限为1000MB，重协商密钥时收发数据包个数上限为268435456（2^28）个。
（可选）指定SSH服务器的公钥算法	**ssh server publickey** { **dsa** | **ecc** | **rsa** | **rsa_sha2_256** | **rsa_sha2_512** } *	缺省情况下，DSA、ECC、RSA、RSA_SHA2_256、RSA_SHA2_512公钥算法都是开启的。
（可选）SSH认证超时时间	**ssh server timeout** *seconds*	缺省情况下，SSH连接认证超时时间为60秒。
（可选）SSH验证重试次数	**ssh server authentication-retries** *times*	缺省情况下，SSH连接的验证重试次数为3。
（可选）配置访问控制列表	**ssh** [**ipv6**] **server acl** *acl-number*	缺省情况下，没有配置访问控制列表。 配置了访问控制列表，可控制哪些客户端能以SSH方式访问本设备。

- 生成本地RSA密钥对时，将同时生成两个密钥对：服务器密钥对和主机密钥对，二者分别包括一个公钥和一个私钥。服务器密钥对和主机密钥对的长度均为2048位。
- 生成本地DSA密钥对时，只生成一个主机密钥对，长度可为1024、2048。缺省情况下，密钥对的长度为2048位。
- 生成本地ECC密钥对时，只生成一个主机密钥对，长度可为256、384、521。缺省情况下，密钥对的长度为521位。

- **配置SSH用户登录的用户界面**

  使用SCP协议，用户将通过VTY用户界面登录设备，所以需要配置VTY用户界面的相关属性。

  表 8-23 配置 SSH 用户登录的用户界面

操作步骤	命令	说明
进入系统视图	**system-view**	-
进入VTY用户界面视图	**user-interface vty** *first-ui-number* [*last-ui-number*]	-
配置VTY用户界面的验证方式为AAA	**authentication-mode aaa**	缺省情况下，VTY用户界面没有验证方式。 必须配置VTY用户界面验证方式为AAA验证，否则**protocol inbound ssh**不能配置成功，用户也将无法登录设备。
配置VTY用户界面支持SSH协议	**protocol inbound ssh**	缺省情况下，用户界面支持的协议是SSH。 如果不配置某个或某几个VTY用户界面支持SSH协议，则SSH用户不能登录设备。
配置VTY用户界面的用户优先级	**user privilege level** *level*	必须将用户级别配置为3级及3级以上，否则连接不成功。 如果是password认证用户，还可以执行**local-user** *user-name* **privilege level** *level*命令配置本地用户的用户级别为3级及3级以上。

操作步骤	命令	说明
（可选）VTY用户界面其他属性	-	除配置VTY用户界面的验证方式和用户优先级外，VTY用户界面的其他属性包括： ● VTY用户界面的最大个数 ● VTY用户界面的呼入呼出限制 ● VTY用户界面的终端属性 请参见**6.6 配置通过STelnet登录设备**–其他功能命令。

- **配置SSH用户**

  配置SSH用户包括配置SSH用户的验证方式，设备支持的认证方式包括RSA、password、password-rsa、DSA、password-dsa、ECC、password-ecc和all。其中：

  – password-rsa认证需要同时满足password认证和RSA认证。
  – password-dsa认证需要同时满足password认证和DSA认证。
  – password-ecc认证需要同时满足password认证和ECC认证。
  – all认证是指password认证、RSA、DSA或ECC认证方式满足其中一种即可。

  表 8-24 配置 SSH 用户

操作步骤	命令	说明
进入系统视图	**system-view**	-
创建SSH用户	**ssh user** *user-name*	-

操作步骤	命令	说明
配置SSH用户的认证方式	**ssh user** *user-name* **authentication-type** { **password** | **rsa** | **password-rsa** | **dsa** | **password-dsa** | **ecc** | **password-ecc** | **all** }	如果没有使用**ssh user**命令配置相应的SSH用户，则可以直接执行**ssh authentication-type default password**命令为用户配置SSH认证缺省采用密码认证，在用户数量比较多时，对用户使用缺省密码认证方式可以简化配置，此时只需再配置AAA用户即可。 **说明** 当认证方式为all认证时，用户的优先级需根据接入用户选择的认证方式来决定： • 如果接入用户选择的认证方式为password认证，则用户优先级为AAA中设置的用户优先级。 • 如果接入用户选择的认证方式为RSA、DSA或ECC认证，则用户的优先级由用户接入时所采用的VTY界面的优先级决定。 如果SSH用户认证方式为all认证，且存在一个同名AAA用户，那通过这两种方式接入时用户优先级可能不同，请根据需要进行部署。
配置SSH用户的服务方式为all	**ssh user** *username* **service-type all**	缺省情况下，SSH用户的服务方式是空，即不支持任何服务方式。

- password认证依靠AAA实现，当用户使用password、password-rsa、password-dsa或password-ecc认证方式登录设备时，需要在AAA视图下创建同名的本地用户。
- 如果SSH用户使用password认证，则只需要在SSH服务器端生成本地RSA、DSA或ECC密钥。如果SSH用户使用RSA、DSA或ECC认证，则在服务器端和客户端都需要生成本地RSA、DSA或ECC密钥对，并且服务器端和客户端都需要将对方的公钥配置到本地。

根据上面配置的认证方式，进行选择配置：

- 若对SSH用户进行password认证，请根据**表8-25**进行配置。
- 若对SSH用户进行RSA、DSA或ECC认证，请根据**表8-26**进行配置。
- 若对SSH用户进行password-rsa、password-dsa或password-ecc认证，则AAA用户和RSA、DSA或ECC公共密钥都需要进行配置。即同时配置**表8-25**和**表8-26**。

表 8-25 配置对 SSH 用户进行 password、password-rsa、password-dsa 或 password-ecc 认证

操作步骤	命令	说明
进入系统视图	**system-view**	-
进入AAA视图	**aaa**	-
配置本地用户名和密码	**local-user** *user-name* **password irreversible-cipher** *password*	-
配置本地用户的服务方式	**local-user** *user-name* **service-type ssh**	-
配置本地用户的级别	**local-user** *user-name* **privilege level** *level*	-
退回到系统视图	**quit**	-

表 8-26 配置对 SSH 用户进行 dsa、rsa、ecc、password-dsa、password-rsa 或 password-ecc 认证

操作步骤	命令	说明
进入系统视图	**system-view**	-
进入RSA、DSA或ECC公共密钥视图	**rsa peer-public-key** *key-name* [**encoding-type** { **der** | **openssh** | **pem** }] 、 **dsa peer-public-key** *key-name* **encoding-type** { **der** | **openssh** | **pem** } 或 **ecc peer-public-key** *key-name* **encoding-type** { **der** | **openssh** | **pem** }	-
进入公共密钥编辑视图	**public-key-code begin**	-

操作步骤	命令	说明
编辑公共密钥	*hex-data*	• 键入的公共密钥必须是按公钥格式编码的十六进制字符串，由支持SSH的客户端软件生成。具体操作参见相应的SSH客户端软件的帮助文档。 • 请将RSA、DSA或ECC公钥输入到作为SSH服务器的设备上。
退出公共密钥编辑视图	**public-key-code end**	• 如果未输入合法的密钥编码hex-data，执行本步骤后，将无法生成密钥。 • 如果指定的密钥*key-name*已经在别的窗口下被删除，再执行本步骤时，系统会提示：密钥已经不存在，此时直接退到系统视图。
退出公共密钥视图，回到系统视图	**peer-public-key end**	-
为SSH用户分配RSA、DSA或ECC公钥	**ssh user** *user-name* **assign** { **rsa-key** | **dsa-key** | **ecc-key** } *key-name*	-

- **用户通过SCP进行文件操作**

  从终端通过SCP方式上传或下载文件，需要在终端上安装支持SCP的SSH客户端软件。此处以使用第三方软件OpenSSH和Windows命令行提示符为例进行配置。

  – OpenSSH软件的安装请参考该软件的安装说明。
  – 使用OpenSSH软件从终端访问设备时，需要使用OpenSSH的命令，命令的使用可以参见该软件的帮助文档。
  – 只有安装了OpenSSH软件后，Windows命令行提示符才能识别OpenSSH相关命令。

  进入Windows的命令行提示符，执行OpenSSH命令，通过SCP方式进行文件操作。(以下显示信息仅为示意)

```
C:\Documents and Settings\Administrator> scp scpuser@10.136.23.5:flash:/vrpcfg.zip vrpcfg-backup.zip
The authenticity of host '10.136.23.5 (10.136.23.5)' can't be established.
DSA key fingerprint is 46:b2:8a:52:88:42:41:d4:af:8f:4a:41:d9:b8:4f:ee.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.136.23.5' (DSA) to the list of known hosts.

User Authentication
Password:
```

```
vrpcfg.zip                                100% 1257     1.2KByte(s)/sec   00:00
Received disconnect from 10.136.23.5: 2: The connection is closed by SSH server


C:\Documents and Settings\Administrator>
```

可以看到，用户终端通过SCP方式，在与远端设备建立连接的同时完成了文件上传或下载的操作，最后又回到了用户本地路径。

说明

由于文件系统对根目录下的文件个数有限制，当根目录中文件个数大于50个时，继续在根目录中创建文件可能会失败。

----结束

检查配置结果

- 使用**display ssh user-information** [*username*]命令，在SSH服务器端查看SSH用户信息。
- 使用**display ssh server status**命令，查看SSH服务器的全局配置信息。
- 使用**display ssh server session**命令，在SSH服务器端查看SSH客户端连接会话信息。

8.3.5 通过 FTPS 进行文件操作

前置任务

在配置通过FTPS进行文件操作之前，需完成以下任务：

- 终端与设备之间路由可达。
- 终端上已经安装支持SSL的FTP客户端软件。

配置流程

通过FTPS进行文件操作的配置流程如表8-27所示。

说明

从V200R020C00版本开始，当需要授权客户可以登录服务器时，必须执行命令指定服务器端的源接口或源地址。

表 8-27 通过 FTPS 进行文件操作的配置流程

序号	配置任务名称	配置任务说明	配置流程说明
1	上传服务器数字证书文件及私钥文件	通过其他文件上传方式将数字证书文件和私钥文件上传至设备。	序号1、2、3、4配置任务中，加载数字证书（序号2）前必须先上传数字证书（序号1），其他无严格配置顺序。
2	配置SSL策略并加载数字证书	包括配置SSL策略及在服务器上加载数字证书。	

序号	配置任务名称	配置任务说明	配置流程说明
3	配置FTPS服务器功能及FTP服务参数	包括为FTPS服务器配置SSL策略、源地址、FTPS服务器的使能及FTP服务参数的配置：端口号、超时断连时间。	
4	配置FTP本地用户	包括配置本地用户的服务类型及FTP用户的授权目录。	
5	用户通过FTPS访问设备	从终端通过FTPS访问设备。	-

缺省配置

表 8-28 缺省配置

参数	缺省值
SSL策略	没有为FTPS服务创建SSL策略
FTPS服务器功能	关闭
端口号	21
FTP用户	没有创建本地用户

操作步骤

- **上传服务器数字证书文件及私钥文件**

  可使用SFTP或SCP方式将服务器数字证书文件和私钥文件上传至设备，且要保存至security中，如设备无此目录，可执行命令**mkdir** *directory*创建。

  服务器需要从证书颁发中心CA（Certificate Authority）获得数字证书文件（包括私钥文件），访问服务器的客户端也需要从CA得到CA证书，用来验证服务器数字证书的有效性。

  说明

  CA是负责发放和管理数字证书的权威机构，当前FTPS服务器上加载的数字证书必须向CA申请。

  证书格式分为PEM格式、ASN1格式和PFX格式。虽然证书的格式不相同，但是证书的内容一样。

  - PEM格式的证书是最常用的一种数字证书格式，文件的扩展名是.pem，适用于系统之间的文本模式传输。
  - ASN1是通用的数字证书格式之一，文件的扩展名是.der，是大多数浏览器的默认格式。

- PFX是通用的数字证书格式之一，文件的扩展名是.pfx，是可移植的二进制格式。

具体的操作步骤请参考手册中其他文件上传方式的介绍。

- **配置SSL策略并加载数字证书文件**

  加载数字证书文件的同时指定私钥文件。

  表 8-29 配置 SSL 策略并加载数字证书

操作步骤	命令	说明
进入系统视图	**system-view**	-
（可选）定制SSL算法套	**ssl cipher-suite-list** *customization-policy-name*	创建SSL算法套定制策略并进入定制策略视图。 缺省情况下，没有配置SSL算法套定制策略。

操作步骤	命令	说明
	set cipher-suite { **tls12_ck_dss_aes_128_gcm_sha256** | **tls12_ck_dss_aes_256_gcm_sha384** | **tls12_ck_rsa_aes_128_gcm_sha256** | **tls12_ck_rsa_aes_256_gcm_sha384** | }	配置SSL算法套定制策略中支持的算法套。 缺省情况下，SSL算法套定制策略中没有配置算法套。 配置算法套定制策略中支持的算法套后，SSL协商时将使用定制策略中配置的策略进行协商。 如果算法套定制策略已经被SSL策略引用，可以对算法套进行增加、修改和部分删除，但不能将算法套定制策略中的算法套全部删除。 系统软件中不包含**tls12_ck_rsa_aes_256_cbc_sha256**、**tls1_ck_dhe_dss_with_aes_128_sha**、**tls1_ck_dhe_dss_with_aes_256_sha**、**tls1_ck_dhe_rsa_with_aes_128_sha**、**tls1_ck_dhe_rsa_with_aes_256_sha**、**tls1_ck_rsa_with_aes_128_sha**和**tls1_ck_rsa_with_aes_256_sha**参数，如需使用，需要安装WEAKEA插件，但是该算法安全性低。为了保证更好的安全性，建议使用其它算法。WEAKEA插件安装方法请参见WEAKEA插件使用指南。
	quit	返回系统视图。
配置SSL策略并进入SSL策略视图	**ssl policy** *policy-name*	-
（可选）设置SSL策略所采用的最低SSL版本	**ssl minimum version** { **tls1.1** | **tls1.2** | **tls1.3** }	缺省情况下，SSL策略所采用的最低SSL版本为TLS1.2。 系统软件中不包含**tls1.0**参数，如需使用，需要安装WEAKEA插件，但是该算法安全性低。为了保证更好的安全性，建议配置**tls1.2**参数。WEAKEA插件安装方法请参见WEAKEA插件使用指南。

操作步骤	命令	说明
（可选）在SSL策略中绑定指定的SSL算法套定制策略	**binding cipher-suite-customization** *customization-policy-name*	缺省情况下，SSL策略未绑定算法套定制策略，使用默认的算法套。SSL策略默认支持如下算法套： ● tls1_ck_rsa_with_aes_256_sha ● tls1_ck_rsa_with_aes_128_sha ● tls1_ck_dhe_rsa_with_aes_256_sha ● tls1_ck_dhe_dss_with_aes_256_sha ● tls1_ck_dhe_rsa_with_aes_128_sha ● tls1_ck_dhe_dss_with_aes_128_sha ● tls12_ck_rsa_aes_256_cbc_sha256 绑定的SSL算法套定制策略中如果仅有一种类型的算法（RSA或DSS），SSL策略需要加载对应类型的证书，确保SSL协商时能成功。
加载PEM格式的证书	**certificate load pem-cert** *cert-filename* **key-pair** { **dsa** | **rsa** } **key-file** *key-filename* **auth-code cipher** *auth-code*	根据证书类型，选其一。 **说明** ● 一个SSL策略只能加载一个证书或者证书链。如果已经加载了证书或者证书链，加载新证书或者证书链之前必须先卸载旧证书或者证书链。 ● 配置SSL策略加载证书或证书链时，证书或证书链中密钥对长度最大为2048位。如果该长度超过2048位，证书文件或证书链文件将无法上传到设备中使用。 ● 从V200R008C00及之后版本降级至以前版本时，需要先备份当前配置中加载的SSL私钥文件。
加载ASN1格式的证书	**certificate load asn1-cert** *cert-filename* **key-pair** { **dsa** | **rsa** } **key-file** *key-filename*	
加载PFX格式的证书	**certificate load pfx-cert** *cert-filename* **key-pair** { **dsa** | **rsa** } { **mac cipher** *mac-code* | **key-file** *key-filename* } **auth-code cipher** *auth-code*	
加载PEM格式的证书链	**certificate load pem-chain** *cert-filename* **key-pair** { **dsa** | **rsa** } **key-file** *key-filename* **auth-code cipher** *auth-code*	

- **配置FTPS服务器功能及FTP服务参数**

  基于FTP协议的FTPS，除了配置FTPS服务器功能外，还可以对FTP服务参数进行配置。

  表 8-30 配置 FTPS 服务器功能及 FTP 服务参数

操作步骤	命令	说明
进入系统视图	**system-view**	-
（可选）指定FTP服务器端口号	**ftp** [**ipv6**] **server port** *port-number*	缺省情况下，FTP服务器端口号是21。 如果配置了新的端口号，FTP服务器端先断开当前已经建立的所有FTP连接，然后使用新的端口号开始尝试连接。这样可以有效防止攻击者对FTP服务标准端口的访问。
为FTPS服务器配置SSL策略	**ftp secure-server ssl-policy** *policy-name*	此处配置的SSL策略即为上个操作步骤中创建的SSL策略。
指定FTP服务器的源地址	• **ftp server-source** { **-a** *source-ip-address* | **-i** *interface-type interface-number* } • **ftp ipv6 server-source -a** *ipv6_address* [**vpn-instance** *vpn_name*]	缺省情况下，未指定FTP服务器的源地址。 配置了服务器的源地址后，登录服务器时，所输入的服务器地址必须与该命令中配置的一致，否则无法成功登录。
使能FTPS服务器功能	**ftp** [**ipv6**] **secure-server enable**	缺省情况下，未使能FTPS服务器。 **说明** 使能FTPS服务功能前，必须去使能FTP服务器功能。
（可选）配置FTP连接空闲时间	**ftp** [**ipv6**] **timeout** *minutes*	缺省情况下，连接空闲时间为10分钟。 在设定的时间内，如果FTP连接始终处于空闲状态时，系统将自动断开FTP连接。
（可选）设置FTP服务器支持的最大会话数	**ftp** [**ipv6**] **server max-sessions** *max-sessions-number*	缺省情况下，FTP服务器支持的最大会话数是5。

说明

- 如果变更端口号前FTPS服务已经启动，则不能变更成功。需执行**undo ftp** [**ipv6**] **secure-server**命令关闭FTPS服务，再进行端口号变更。
- 当客户端与设备之间的文件操作结束后，请执行**undo ftp** [**ipv6**] **secure-server**命令，及时关闭FTPS服务器功能，从而保证设备的安全。

- **配置FTP本地用户**

  当用户通过FTPS进行文件操作时，需要在作为FTPS服务器的设备上配置本地用户名及口令，指定用户的服务类型以及可以访问的目录。否则用户将无法访问设备。

  表 8-31 配置 FTP 本地用户

操作步骤	命令	说明
进入系统视图	**system-view**	-
进入AAA视图	**aaa**	-
配置本地用户名和密码	**local-user** *user-name* **password irreversible-cipher** *password*	-
配置本地用户级别	**local-user** *user-name* **privilege level** *level*	**说明** 必须将用户级别配置在3级或3级以上，否则FTP连接将无法成功。
配置本地用户的服务类型为FTP	**local-user** *user-name* **service-type ftp**	缺省情况下，本地用户可以使用所有的接入类型。
配置FTP用户的授权目录	**local-user** *user-name* **ftp-directory** *directory*	缺省情况下，本地用户的FTP目录为空。 当有多个FTP用户且有相同的授权目录时，可以执行**set default ftp-directory** *directory*命令，为FTP用户配置缺省工作目录。此时，不需要通过**local-user** *user-name* **ftp-directory** *directory*命令为每个用户配置授权目录。
配置本地用户的FTP权限	**local-user** *user-name* **ftp-privilege** [*directoryfilename*] { **read** | **write** | **execute** }*	缺省情况下，本地用户的FTP权限为读、写和执行权限。

- **用户通过FTPS访问设备**

  需要在用户终端安装支持SSL的FTP客户端软件，通过第三方软件从用户终端登录FTPS服务器，实现对FTPS服务器进行文件的安全管理。

说明

由于文件系统对根目录下的文件个数有限制，当根目录中文件个数大于50个时，继续在根目录中创建文件可能会失败。

----结束

检查配置结果

- 使用**display ssl policy**命令，查看配置的SSL策略及加载的数字证书。
- 使用**display [ipv6] ftp-server**命令，查看FTPS服务器的状态。
- 使用**display ftp-users**命令，查看登录的FTP用户信息。

8.4 访问其他设备的文件

8.4.1 配置设备作为 TFTP 客户端访问其他设备的文件

前置任务

在配置通过TFTP访问其他设备的文件之前，需完成以下任务：

- 当前设备和TFTP服务器路由可达。
- 已获取TFTP服务器的主机名或IP地址以及下载或上传文件所在的目录。

配置流程

说明

使用TFTP协议存在安全风险，建议使用SFTP V2、SCP或FTPS方式进行文件操作。

通过TFTP访问其他设备文件的配置流程如**表8-32**所示。

表 8-32 配置设备作为 TFTP 客户端访问其他设备文件的配置流程

序号	配置任务名称	配置任务说明	配置流程说明
1	（可选）配置TFTP客户端源地址	客户端源地址可以配置为源接口或源IP，达到安全校验的目的。	在执行任务3前，任务1、2之间没有严格的配置顺序。
2	（可选）配置TFTP访问限制	包括配置ACL（Access Control List）规则及TFTP基本访问控制列表，提高TFTP访问的安全性。	
3	使用TFTP命令向其他设备上传或下载文件	包括文件的上传和下载操作。	

操作步骤

- **（可选）配置TFTP客户端源地址**

  配置源地址需要选择设备上状态稳定的接口，如LoopBack接口。该配置简化了ACL规则和安全策略的配置，只要将ACL规则的源地址或目的地址指定为该地址，就可以屏蔽接口IP地址的差异以及接口状态的影响，实现对设备进出报文的过滤。

  表 8-33 （可选）配置 TFTP 客户端源地址

操作步骤	命令	说明
进入系统视图	**system-view**	-
配置TFTP客户端的源地址信息	**tftp client-source** { **-a** *source-ip-address* | **-i** *interface-type interface-number* }	源地址可以是源IP或源接口，如果是源接口，必须要为该接口配置IP地址，否则会导致TFTP连接建立失败。 缺省情况下，TFTP客户端发送报文的源地址为与TFTP服务器通信的出接口的IP地址，显示为0.0.0.0。

- **（可选）配置TFTP访问限制**

  ACL是一系列有顺序的规则组的集合，这些规则根据数据包的源地址、目的地址、端口号等来描述。ACL通过规则对数据包进行分类，这些规则应用到路由设备，路由设备根据这些规则判断哪些数据包可以接收，哪些数据包需要拒绝。

  每个ACL中可以定义多个规则，根据规则的功能分为基本ACL规则、高级ACL规则和二层ACL规则等。

  TFTP只支持基本访问控制列表（编号范围为2000～2999）。

  ACL规则：

  - 当ACL的rule配置为**permit**时，则允许本设备与匹配该rule规则的其他设备建立TFTP连接。
  - 当ACL的rule配置为**deny**时，则拒绝本设备与匹配该rule规则的其他设备建立TFTP连接。

  表 8-34 （可选）配置 TFTP 访问限制

操作步骤	命令	说明
进入系统视图	**system-view**	-
创建一个ACL访问控制列表，并进入ACL视图	**acl** [**number**] *acl-number*	缺省情况下，未创建ACL访问控制列表。

操作步骤	命令	说明
配置ACL规则	**rule** [*rule-id*] { **deny** | **permit** } [**source** { *source-address source-wildcard* | **any** } | **fragment** | **logging** | **time-range** *time-name* | { **vpn-instance** *vpn-instance-name* | **public** }] *	缺省情况下，ACL视图下没有配置规则。 **说明** 仅S5720I-SI、S5735-S、S5735S-S、S5735-S-I、S5735S-H、S5736-S、S5731-H-K、S5731-H、S5731-S、S5731S-H、S5731S-S、S5732-H、S5732-H-K、S6735-S、S6720-EI、S6720S-EI、S6720S-S、S6730-H-K、S6730-H、S6730S-H、S6730-S和S6730S-S应用为软件ACL时才支持**vpn-instance**和**public**参数。软件ACL的应用场景请参见《S300, S500, S2700, S5700, S6700 V200R022C00 配置指南-安全》ACL配置 - ACL的基本原理中的“**ACL的实现方式**”。
退回到系统视图	**quit**	-
配置TFTP访问限制	**tftp-server** [**ipv6**] **acl** *acl-number*	-

- **使用TFTP命令向其他设备上传文件或从其他设备下载文件**

操作步骤	命令	说明
IPv4地址	**tftp** [**-a** *source-ip-address* | **-i** *interface-type interface-number*] *tftp-server* [**public-net** | **vpn-instance** *vpn-instance-name*] { **get** | **put** } *source-filename* [*destination-filename*]	• **get**表示从其他设备下载文件操作。 • **put**表示向其他设备上传文件操作。
IPv6地址	**tftp ipv6** [**-a** *source-ip-address*] *tftp-server-ipv6* [**-oi** *interface-type interface-number*] { **get** | **put** } *source-filename* [*destination-filename*]	

说明

由于文件系统对根目录下的文件个数有限制，当根目录中文件个数大于50个时，继续在根目录中创建文件可能会失败。

此命令中指定的源地址或者接口优先级高于**tftp client-source**命令中指定的源地址或者接口。如果执行命令**tftp client-source**指定了源地址或者接口，又在**tftp**命令中指定了源地址或者接口，则采用**tftp**命令中指定的源地址或者接口进行通信。**tftp client-source**命令指定的源地址或者接口对所有的TFTP连接都有效，**tftp**命令指定的源地址或者接口只对当前的TFTP连接有效。

----结束

检查配置结果

- 执行**display tftp-client**命令，查看设备作为TFTP客户端时的源地址。
- 执行**display acl** { *acl-number* | **all** }命令，查看TFTP客户端配置的ACL规则。

8.4.2 配置设备作为 FTP 客户端访问其他设备的文件

前置任务

在配置通过FTP访问其他设备的文件之前，需完成以下任务：

- 当前设备和FTP服务器路由可达。
- 已获取FTP服务器的主机名或IP地址、FTP用户名及密码。
- 如果服务器不是使用标准的端口号，则还需获取服务器端设置的端口号。

配置流程

须知

使用FTP协议存在安全风险，建议使用SFTP V2、SCP或FTPS方式进行文件操作。

从V200R020C00版本开始，缺省情况下FTP服务器端不接收来自任何接口登录连接的IPv4和IPv6请求，当需要授权客户可以登录服务器时，必须执行命令指定服务器端的源接口或源地址。

通过FTP访问其他设备文件的配置流程如表8-35所示。

表 8-35 配置设备作为 FTP 客户端访问其他设备的文件配置流程

序号	配置任务名称	配置任务说明	配置流程说明
1	（可选）配置FTP客户端源地址	客户端源地址可以配置为源接口或源IP，达到安全校验的目的。	序号1、2有序操作，FTP连接建立后，序号3、4无操作顺序，序号5（断开连接操作）为最后一步。
2	使用FTP连接其他设备	-	

序号	配置任务名称	配置任务说明	配置流程说明
3	通过FTP文件操作命令进行文件操作	包括目录操作、文件操作、配置文件传输方式、查看FTP命令在线帮助等。	
4	（可选）更改登录用户	-	
5	断开与FTP服务器的连接	-	

操作步骤

- **（可选）配置FTP客户端源地址**

  配置源地址需要选择设备上状态稳定的接口，如LoopBack接口。该配置简化了ACL规则和安全策略的配置，只要将ACL规则的源地址或目的地址指定为该地址，就可以屏蔽接口IP地址的差异以及接口状态的影响，实现对设备进出报文的过滤。

  FTP客户端配置的源地址必须为LoopBack地址或LoopBack接口。

  表 8-36 配置 FTP 客户端源地址

操作步骤	命令	说明
进入系统视图	**system-view**	-
配置FTP客户端的源地址信息	**ftp client-source** { **-a** *source-ip-address* | **-i** *interface-type interface-number* }	建议使用Loopback接口的地址。 当配置为LoopBack接口时，一定要为此接口配置IP地址，否则会导致FTP连接建立失败。

- **使用FTP连接其他设备**

  在用户视图和FTP客户端视图下，用户均可以使用相应命令访问FTP服务器。

  根据服务器端IP地址类型不同，进行如下操作。

  表 8-37 使用 FTP 命令连接其他设备（服务器端 IPv4 地址类型）

操作步骤	命令	说明
用户视图下直接建立与IPv4 FTP服务器的连接	**ftp** [**-a** *source-ip-address* | **-i** *interface-type interface-number*] *host-ip* [*port-number*] [**public-net** | **vpn-instance** *vpn-instance-name*]	二选一 FTP客户端视图下建立与FTP服务器的连接时需要先使用**ftp**命令进入FTP客户端视图。

操作步骤	命令	说明
FTP客户端视图下建立与IPv4 FTP服务器的连接	**ftp**	
	open [**-a** *source-ip-address* | **-i** *interface-type interface-number*] *host-ip* [*port-number*] [**public-net** | **vpn-instance** *vpn-instance-name*]	

说明

- 在访问FTP服务器之前，可以执行命令**set net-manager vpn-instance**，设置默认的VPN实例。执行该命令后，进行FTP操作时所使用的VPN实例即用户配置的默认VPN实例。
- 基于IPV4网络中，**ftp**命令中指定的源地址优先级高于**ftp client-source**命令中指定源地址的优先级。如果执行命令**ftp client-source**指定了源地址后，又在**ftp**命令中指定了源地址，则采用**ftp**命令中指定的源地址进行通信。**ftp client-source**命令指定的源地址对所有的FTP连接都有效，**ftp**命令指定的源地址只对当前的FTP连接有效。

表 8-38 使用 FTP 命令连接其他设备（服务器端 IPv6 地址类型）

操作步骤	命令	说明
用户视图下直接建立与IPv6 FTP服务器的连接	**ftp ipv6** *host-ipv6* [*port-number*]	二选一 FTP客户端视图下建立与FTP服务器的连接时需要先使用**ftp**命令进入FTP客户端视图。
FTP客户端视图下建立与IPv6 FTP服务器的连接	**ftp**	
	open ipv6 *host-ipv6* [*port-number*]	

用户访问服务器时，需要经过验证，输入正确的用户名和密码后，方可访问服务器。

- **通过FTP命令进行文件操作**

  用户访问FTP服务器后，可以通过FTP命令进行文件操作，包括目录操作、文件操作、配置文件传输方式、查看FTP命令在线帮助等。

  说明

  用户的操作权限受限于服务器上对该用户的权限设置。

  由于文件系统对根目录下的文件个数有限制，当根目录中文件个数大于50个时，继续在根目录中创建文件可能会失败。

  以下各操作没有严格顺序，可根据需求选择一种或多种操作项目。

表 8-39 通过 FTP 命令进行文件操作

操作项目	命令	说明
改变服务器上的工作路径	**cd** *remote-directory*	-
改变服务器的工作路径到上一级目录	**cdup**	-
显示服务器工作路径	**pwd**	-
显示或者改变客户端的工作路径	**lcd** [*local-directory*]	与**pwd**不同的是，**lcd**命令执行后显示的是客户端的本地工作路径，而**pwd**显示的则是远端服务器的工作路径。
在服务器上创建目录	**mkdir** *remote-directory*	创建的目录可以为字母和数字等的组合，但不可以为<、>、？ 、\、： 等特殊字符。
在服务器上删除目录	**rmdir** *remote-directory*	-
显示服务器上指定目录或文件的信息	**dir/ls** [*remote-filename* [*local-filename*]]	• **ls**命令只能显示出目录/文件的名称，而**dir**命令可以查看目录/文件的详细信息，如大小，创建日期等。 • 如果指定远程文件时没有指定路径名称，那么系统将在用户的授权目录下搜索指定的文件。
删除服务器上指定文件	**delete** *remote-filename*	-
上传单个或多个文件	**put** *local-filename* [*remote-filename*] 或 **mput** *local-filenames*	• **put**命令是上传单个文件。 • **mput**命令是上传多个文件。
下载单个或多个文件	**get** *remote-filename* [*local-filename*] 或 **mget** *remote-filenames*	• **get**命令是下载单个文件。 • **mget**命令是下载多个文件。

操作项目	命令	说明
配置传输文件的数据类型为ASCII模式或二进制模式	**ascii** 或 **binary**	二选一 • 缺省情况下，文件传输方式为ASCII模式。 • 传输文本文件使用ASCII方式，传输程序、系统软件、数据库文件等使用二进制模式。
配置文件传输方式为被动方式或主动方式	**passive** 或 **undo passive**	二选一 缺省情况下，数据传输方式是主动方式。
查看FTP命令的在线帮助	**remotehelp** [*command*]	-
使能系统的提示功能	**prompt**	缺省情况下，不使能信息提示。
打开verbose开关	**verbose**	如果打开verbose开关，将显示所有FTP响应，包括FTP协议信息，以及FTP服务器返回的详细信息。

- **（可选）更改登录用户**

  设备可以在不退出FTP客户端视图的情况下，以其他的用户名登录到FTP服务器。所建立的FTP连接，与执行**ftp**命令建立的FTP连接完全相同。

操作步骤	命令	说明
FTP客户端视图下，更改当前的登录用户	**user** *user-name* [*password*]	更改当前的登录用户后，原用户与服务器的连接将断开。

- **断开与FTP服务器的连接**

  用户可以在FTP客户端视图中选择不同的命令断开与FTP服务器的连接。

操作步骤	命令	说明
终止与服务器的连接，并退回到用户视图	**bye** 或 **quit**	二选一。
终止与服务器的连接，并退回到FTP客户端视图	**close** 或 **disconnect**	

----结束

检查配置结果

- 使用**display ftp-client**命令，查看设备作为FTP客户端时的源参数。

8.4.3 配置设备作为 SFTP 客户端访问其他设备的文件

前置任务

在配置通过SFTP访问其他设备的文件之前，需完成以下任务：

- 当前设备和SSH服务器路由可达。
- 已获取SSH服务器的主机名或IP地址以及SSH用户信息。
- 如果服务器不是使用标准的端口号，则还需获取服务器端设置的端口号。

配置流程

须知

从V200R020C00版本开始，缺省情况下SFTP服务器端不接收来自任何接口登录连接的IPv4和IPv6请求，当需要授权客户可以登录服务器时，必须执行命令指定服务器端的源接口或源地址。

通过SFTP访问其他设备文件的配置流程如**表8-40**所示。

表 8-40 配置设备作为 SFTP 客户端访问其他设备文件的配置流程

序号	配置任务名称	配置任务说明	配置流程说明
1	（可选）配置SFTP客户端源地址	客户端源地址可以配置为源接口或源IP，达到安全校验的目的。	序号1、2、3无序操作，SFTP连接（序号4）建立后，可执行序号5的操作，最后断开连接（序号6）。
2	生成本地密钥对	生成本地密钥对，然后将公钥配置到SSH服务器上。 本步骤仅在设备以RSA、DSA或ECC方式登录SSH服务器的时候执行，password方式登录SSH服务器则无需执行。	
3	配置设备首次连接SSH服务器的方式	有两种配置方式：使能SSH客户端首次认证功能方式和SSH客户端为SSH服务器分配公钥方式，用户可选择其一进行配置。	

序号	配置任务名称	配置任务说明	配置流程说明
4	使用SFTP命令连接其他设备	-	
5	通过SFTP文件操作命令进行文件操作	用户可以通过SFTP客户端管理SSH服务器上的目录和文件，以及查看SFTP客户端命令帮助。	
6	断开与SFTP服务器的连接	-	

操作步骤

- **（可选）配置SFTP客户端源地址**

  配置源地址需要选择设备上状态稳定的接口，如LoopBack接口。该配置简化了ACL规则和安全策略的配置，只要将ACL规则的源地址或目的地址指定为该地址，就可以屏蔽接口IP地址的差异以及接口状态的影响，实现对设备进出报文的过滤。

  SFTP客户端配置的源地址必须为LoopBack地址或LoopBack接口。

  表 8-41 配置 SFTP 客户端源地址

操作步骤	命令	说明
进入系统视图	**system-view**	-
配置SFTP客户端的源地址信息	**sftp client-source** { **-a** *source-ip-address* | **-i** *interface-type interface-number* }	缺省情况下，源地址为0.0.0.0。 配置的源地址为设备的LoopBack地址或LoopBack接口。

- **生成本地密钥对**

  说明

  此步骤仅在设备以RSA、DSA或ECC方式登录SSH服务器的时候执行，设备以password方式登录SSH服务器，则无需执行。

  表 8-42 生成本地密钥对

操作步骤	命令	说明
进入系统视图	**system-view**	-

操作步骤	命令	说明
生成本地密钥对	**rsa local-key-pair create**、**dsa local-key-pair create**或**ecc local-key-pair create**	根据对端密钥的类型，三选一。 密钥对生成后，可以执行**display rsa local-key-pair public**、**display dsa local-key-pair public**或**display ecc local-key-pair public**命令查看RSA本地密钥对、DSA本地密钥对或ECC密钥对中的公钥部分信息，然后将公钥配置到SSH服务器上。

- **配置设备首次连接SSH服务器的方式**

  作为客户端的设备首次连接SSH服务器时，因为客户端还没有保存过SSH服务器的公钥，无法对SSH服务器有效性进行检查，这样会导致连接不成功。可以通过下面两种方式来解决：

  - 使能SSH客户端首次认证功能方式：不对SSH服务器的公钥进行有效性检查，确保首次连接成功。成功连接后，系统将自动分配并保存公钥，为下次连接时认证使用。具体配置见**表8-43**。此种方式配置简单。
  - SSH客户端配置服务器公钥方式：将服务器端产生的公钥直接保存至客户端，保证在首次连接时SSH服务器有效性检查能够通过。具体配置见**表8-44**。此种方式配置较复杂，但比上面那种方式安全性更高。

表 8-43 使能 SSH 客户端首次认证功能

操作步骤	命令	说明
进入系统视图	**system-view**	-
使能SSH客户端首次认证功能	**ssh client first-time enable**	缺省情况下，SSH客户端首次认证功能是关闭的。

表 8-44 SSH 客户端为 SSH 服务器分配 RSA、DSA 或 ECC 公钥方式

操作步骤	命令	说明
进入系统视图	**system-view**	-

操作步骤	命令	说明
进入RSA、DSA或ECC公共密钥视图	**rsa peer-public-key** *key-name* [**encoding-type** { **der** | **openssh** | **pem** }] 、 **dsa peer-public-key** *key-name* **encoding-type** { **der** | **openssh** | **pem** } 或 **ecc peer-public-key** *key-name* **encoding-type** { **der** | **openssh** | **pem** }	根据生成的密钥类型，三选一。
进入公共密钥编辑视图	**public-key-code begin**	-
编辑公共密钥	*hex-data*	● 键入的公共密钥必须是按公钥格式编码的十六进制字符串，由SSH服务器随机生成。 ● 进入公共密钥编辑视图后，即可将服务器上产生的RSA、DSA或ECC公钥输入到客户端。
退出公共密钥编辑视图	**public-key-code end**	● 如果输入的密钥编码hex-data不合法，执行本步骤后，将无法生成密钥。 ● 如果指定的密钥key-name已经被删除，再执行本步骤时，系统会提示：密钥已经不存在，此时直接退到系统视图。
退出公共密钥视图，回到系统视图	**peer-public-key end**	-
为SSH服务器绑定RSA、DSA或ECC公钥	**ssh client** *servername* **assign** { **rsa-key** | **dsa-key** | **ecc-key** } *keyname*	如果SSH客户端保存的SSH服务器公钥失效，执行命令**undo ssh client** *servername* **assign** { **rsa-key** | **dsa-key** | **ecc-key** }，取消SSH服务器与RSA、DSA或ECC公钥的绑定关系，再执行本命令，为SSH服务器重新分配RSA、DSA或ECC公钥。

- **使用SFTP命令连接其他设备**

SFTP客户端连接命令跟STelnet客户端连接命令很相似，支持访问SSH服务器时携带源地址，选择密钥交换算法、加密算法和HMAC算法，以及设置keepalive功能。

表 8-45 使用 SFTP 命令连接其他设备

操作步骤	命令	说明
进入系统视图	**system-view**	-
（可选）配置SSH客户端的密钥交换算法列表	**ssh client key-exchange** { **dh_group14_sha256** | **dh_group15_sha512** | **dh_group16_sha512** | **dh_group_exchange_sha256** | **ecdh_sha2_nistp256**| **ecdh_sha2_nistp384**| **ecdh_sha2_nistp521**}*	缺省情况下，SSH客户端支持所有的密钥交换算法。 系统软件中不包含**dh_group_exchange_sha1**、**dh_group14_sha1和dh_group1_sha1**参数，如需使用，需要安装WEAKEA插件，但是该算法安全性低。为了保证更好的安全性，建议使用其它算法。WEAKEA插件安装方法请参见WEAKEA插件使用指南。
（可选）配置SSH客户端的加密算法列表	**ssh client cipher** { **aes128_ctr** | **aes256_ctr** } *	缺省情况下，不安装WEAKEA插件，SSH客户端只支持**aes128_ctr**和**aes256_ctr**算法，不可以使用**undo ssh client cipher**命令，安装WEAKEA插件后，增加支持**aes256_cbc**、**aes128_cbc**、**3des_cbc**和**des_cbc**算法，并且可以使用**undo ssh client cipher**命令。 系统软件中不包含**aes256_cbc**、**aes128_cbc**、**3des_cbc**和**des_cbc**参数，如需使用，需要安装WEAKEA插件，但是该算法安全性低。为了保证更好的安全性，建议配置**aes256_ctr**或**aes128_ctr**参数。WEAKEA插件安装方法请参见WEAKEA插件使用指南。

操作步骤	命令	说明
（可选）配置SSH客户端上的校验算法列表	**ssh client hmac** { **sha2_256** }	缺省情况下，不安装WEAKEA插件，SSH客户端只支持**sha2_256**校验算法，不可以使用**undo ssh client hmac**命令，安装WEAKEA插件后，增加支持**sha2_256_96**、**sha1**、**sha1_96**、**md5**和**md5_96**校验算法，并且可以使用**undo ssh client hmac**命令。 系统软件中不包含**sha2_256_96**、**sha1**、**sha1_96**、**md5**和**md5_96**参数，如需使用，需要安装WEAKEA插件，但是该算法安全性低。为了保证更好的安全性，建议配置**sha2_256**参数。WEAKEA插件安装方法请参见WEAKEA插件使用指南。
（可选）配置SSH客户端重协商密钥时的参数	**ssh client rekey** { **time** *rekey-time* | **data-limit** *data-limit* | **max-packet** *max-packet* } *	缺省情况下，SSH客户端触发密钥重协商的时间间隔为60分钟，重协商密钥收发数据大小上限为1000MB，重协商密钥收发数据包个数上限为268435456（2^28）个。
IPv4地址	**sftp** [**-a** *source-address* | **-i** *interface-type interface-number*] *host-ip* [*port*] [[**public-net** | **-vpn-instance** *vpn-instance-name*] | **identity-key** { **dsa** | **rsa** | **ecc** | **rsa_sha2_256** | **rsa_sha2_512** } | **user-identity-key** { **rsa** | **dsa** | **ecc** } | **prefer_kex** *prefer_key-exchange* | **prefer_ctos_cipher** *prefer_ctos_cipher* | **prefer_stoc_cipher** *prefer_stoc_cipher* | **prefer_ctos_hmac** *prefer_ctos_hmac* | **prefer_stoc_hmac** *prefer_stoc_hmac*| **-ki** *aliveinterval*] | [**-kc** *alivecountmax*] *	根据地址类型选其一。 大多数情况下，该命令可以只指定IP地址，而不需要指定其他可选项。 **说明** 为了保证更好的安全性，建议您使用更安全的aes128或aes256算法作为客户端到服务器端的认证算法。

操作步骤	命令	说明
IPv6地址	**sftp ipv6** [**-a** *source-address*] *host-ipv6* [**-oi** *interface-type interface-number*] [*port*] [**identity-key** { **dsa** | **rsa** | **ecc** | **rsa_sha2_256** | **rsa_sha2_512** } | **user-identity-key** { **rsa** | **dsa** | **ecc** } | **-vpn-instance** *vpn-instance-name* | **prefer_kex** *prefer_key-exchange* | **prefer_ctos_cipher** *prefer_ctos_cipher* | **prefer_stoc_cipher** *prefer_stoc_cipher* | **prefer_ctos_hmac** *prefer_ctos_hmac* | **prefer_stoc_hmac** *prefer_stoc_hmac* | **-ki** *aliveinterval* | **-kc** *alivecountmax*] *	

例如：

```
[HUAWEI] sftp 10.137.217.201
```

连接成功后，屏幕会显示**sftp-client>**，此时已经进入了SFTP客户端视图。

- **通过SFTP命令进行文件操作**

  当SFTP客户端登录到SSH服务器之后，用户可以在SFTP客户端进行如表8-46所示的操作。

  以下各操作没有严格顺序，可根据需求选择一种或多种操作项目。

  说明

  在SFTP客户端视图下，文件操作命令不支持联想功能，必须手动输入完整的命令，否则会提示是不支持的命令。

  由于文件系统对根目录下的文件个数有限制，当根目录中文件个数大于50个时，继续在根目录中创建文件可能会失败。

表 8-46 通过 SFTP 文件操作命令进行文件操作

操作项目	命令	说明
改变用户的当前工作目录	**cd** [*remote-directory*]	-
改变用户的工作目录为当前工作目录的上一级目录	**cdup**	-
显示用户的当前工作目录	**pwd**	-

操作项目	命令	说明
显示指定目录下的文件列表	**dir/ls** [**-l** | **-a**] [*remote-directory*]	**dir**与**ls**执行的效果是一样的。
删除服务器上目录	**rmdir** *remote-directory* &<1-10>	一次最多可以删除十个目录。 使用该命令删除目录时，目录中不能有文件，否则会删除失败。
在服务器上创建新目录	**mkdir** *remote-directory*	-
改变服务器上指定的文件的名字	**rename** *old-name new-name*	-
下载远程服务器上的文件	**get** *remote-filename* [*local-filename*]	-
上传本地文件到远程服务器	**put** *local-filename* [*remote-filename*]	-
删除服务器上文件	**remove** *remote-filename* &<1-10>	一次最多可以删除十个文件。
SFTP客户端命令帮助	**help** [**all** | *command-name*]	-

用户也可以在系统视图下执行如下命令下载服务器上的文件或者上传本地文件到远程服务器中:

- IPv4地址：**sftp client-transfile** { **get** | **put** } [**-a** *source-address* | **-i** *interface-type interface-number*] **host-ip** *host-ipv4* [*port*] [[**public-net** | **-vpn-instance** *vpn-instance-name*] | **prefer_kex** *prefer_key-exchange* | **identity-key** { **rsa** | **dsa** | **ecc** } | **prefer_ctos_cipher** *prefer_ctos_cipher* | **prefer_stoc_cipher** *prefer_stoc_cipher* | **prefer_ctos_hmac** *prefer_ctos_hmac* | **prefer_stoc_hmac** *prefer_stoc_hmac* | **-ki** *aliveinterval* | **-kc** *alivecountmax*] * **username** *user-name* **password** *password* **sourcefile** *source-file* [**destination** *destination*]
- IPv6地址：**sftp client-transfile** { **get** | **put** } **ipv6** [**-a** *source-address*] **host-ip** *host-ipv6* [**-oi** *interface-type interface-number*] [*port*] [**-vpn-instance** *vpn-instance-name* | **prefer_kex** *prefer_key-exchange* | **identity-key** { **rsa** | **dsa** | **ecc** } | **prefer_ctos_cipher** *prefer_ctos_cipher* | **prefer_stoc_cipher** *prefer_stoc_cipher* | **prefer_ctos_hmac** *prefer_ctos_hmac* | **prefer_stoc_hmac** *prefer_stoc_hmac* | **-ki** *aliveinterval* | **-kc** *alivecountmax*] * **username** *user-name* **password** *password* **sourcefile** *source-file* [**destination** *destination*]

- **断开与SFTP服务器的连接**

操作步骤	命令	说明
断开与SFTP服务器的连接	**quit**	-

----结束

检查配置结果

- 使用**display sftp-client**命令，查看设备作为SFTP客户端时的源参数地址。
- 使用**display ssh server-info**命令，查看客户端所有的SSH服务器与公钥之间的对应关系。

8.4.4 配置设备作为 SCP 客户端访问其他设备的文件

前置任务

在配置通过SCP访问其他设备的文件之前，需完成以下任务：

- 当前设备和SSH服务器路由可达。
- 已获取SSH服务器的主机名或IP地址以及SSH用户信息。
- 如果服务器不是使用标准的端口号，则还需获取服务器端设置的端口号。

配置流程

须知

从V200R020C00版本开始，缺省情况下SCP服务器端不接收来自任何接口登录连接的IPv4和IPv6请求，当需要授权客户可以登录服务器时，必须执行命令指定服务器端的源接口或源地址。

通过SCP访问其他设备文件的配置流程如表8-47所示。

表 8-47 配置设备作为 SCP 客户端访问其他设备文件的配置流程

序号	配置任务名称	配置任务说明	配置流程说明
1	（可选）配置SCP客户端源地址	客户端源地址可以配置为源接口或源IP，达到安全校验的目的。	序号1、2、3之间没有严格的配置顺序。

序号	配置任务名称	配置任务说明	配置流程说明
2	生成本地密钥对	生成本地密钥对，然后将公钥配置到SSH服务器上。 本步骤仅在设备以RSA、DSA或ECC方式登录SSH服务器的时候执行，password方式登录SSH服务器则无需执行。	
3	配置设备首次连接SSH服务器的方式	有两种配置方式：使能SSH客户端首次认证功能方式和SSH客户端为SSH服务器分配公钥方式，用户可选择其一进行配置。	
4	使用SCP命令连接其他设备	-	

操作步骤

- **（可选）配置SCP客户端源地址**

表 8-48 （可选）配置 SCP 客户端源地址

操作步骤	命令	说明
进入系统视图	**system-view**	-
配置SCP客户端的源地址信息	**scp client-source** { **-a** *source-ip-address* | **-i** *interface-type interface-number* }	缺省情况下，没有配置源地址。

- **生成本地密钥对**

说明

此步骤仅在设备以RSA、DSA或ECC方式登录SSH服务器的时候执行，设备以password方式登录SSH服务器，则无需执行。

表 8-49 生成本地密钥对

操作步骤	命令	说明
进入系统视图	**system-view**	-

操作步骤	命令	说明
生成本地密钥对	**rsa local-key-pair create**、**dsa local-key-pair create**或**ecc local-key-pair create**	根据对端密钥的类型，三选一。 密钥对生成后，可以执行**display rsa local-key-pair public**、**display dsa local-key-pair public**或**display ecc local-key-pair public**命令查看RSA本地密钥对、DSA本地密钥对或ECC密钥对中的公钥部分信息，然后将公钥配置到SSH服务器上。

- **配置设备首次连接SSH服务器的方式**

  作为客户端的设备首次连接SSH服务器时，因为客户端还没有保存过SSH服务器的公钥，无法对SSH服务器有效性进行检查，这样会导致连接不成功。可以通过下面两种方式来解决：

  - 使能SSH客户端首次认证功能方式：不对SSH服务器的公钥进行有效性检查，确保首次连接成功。成功连接后，系统将自动分配并保存公钥，为下次连接时认证使用。具体配置见表8-43。此种方式配置简单。
  - SSH客户端配置服务器公钥方式：将服务器端产生的公钥直接保存至客户端，保证在首次连接时SSH服务器有效性检查能够通过。具体配置见表8-44。此种方式配置较复杂，但比上面那种方式安全性更高。

表 8-50 使能 SSH 客户端首次认证功能

操作步骤	命令	说明
进入系统视图	**system-view**	-
使能SSH客户端首次认证功能	**ssh client first-time enable**	缺省情况下，SSH客户端首次认证功能是关闭的。

表 8-51 SSH 客户端为 SSH 服务器分配 RSA、DSA 或 ECC 公钥方式

操作步骤	命令	说明
进入系统视图	**system-view**	-

操作步骤	命令	说明
进入RSA、DSA或ECC公共密钥视图	**rsa peer-public-key** *key-name* [**encoding-type** { **der** | **openssh** | **pem** }] 、 **dsa peer-public-key** *key-name* **encoding-type** { **der** | **openssh** | **pem** } 或 **ecc peer-public-key** *key-name* **encoding-type** { **der** | **openssh** | **pem** }	根据生成的密钥类型，三选一。
进入公共密钥编辑视图	**public-key-code begin**	-
编辑公共密钥	*hex-data*	● 键入的公共密钥必须是按公钥格式编码的十六进制字符串，由SSH服务器随机生成。 ● 进入公共密钥编辑视图后，即可将服务器上产生的RSA、DSA或ECC公钥输入到客户端。
退出公共密钥编辑视图	**public-key-code end**	● 如果输入的密钥编码hex-data不合法，执行本步骤后，将无法生成密钥。 ● 如果指定的密钥key-name已经被删除，再执行本步骤时，系统会提示：密钥已经不存在，此时直接退到系统视图。
退出公共密钥视图，回到系统视图	**peer-public-key end**	-
为SSH服务器绑定RSA、DSA或ECC公钥	**ssh client** *servername* **assign** { **rsa-key** | **dsa-key** | **ecc-key** } *keyname*	如果SSH客户端保存的SSH服务器公钥失效，执行命令**undo ssh client** *servername* **assign** { **rsa-key** | **dsa-key** | **ecc-key** }，取消SSH服务器与RSA、DSA或ECC公钥的绑定关系，再执行本命令，为SSH服务器重新分配RSA、DSA或ECC公钥。

- **使用SCP命令连接其他设备**

SCP与SFTP方式不同，当SCP命令执行后，与服务器建立安全连接，客户端可以直接上传文件至服务器或从服务器下载文件至本地。

表 8-52 使用 SCP 命令连接其他设备

操作步骤	命令	说明
进入系统视图	**system-view**	-
（可选）配置SSH客户端的密钥交换算法列表	**ssh client key-exchange** { **dh_group14_sha256** | **dh_group15_sha512** | **dh_group16_sha512** | **dh_group_exchange_sha256** | **ecdh_sha2_nistp256**| **ecdh_sha2_nistp384**| **ecdh_sha2_nistp521** }*	缺省情况下，SSH客户端支持所有的密钥交换算法。 系统软件中不包含**dh_group_exchange_sha1**、**dh_group14_sha1和dh_group1_sha1**参数，如需使用，需要安装WEAKEA插件，但是该算法安全性低。为了保证更好的安全性，建议使用其它算法。WEAKEA插件安装方法请参见WEAKEA插件使用指南。
（可选）配置SSH客户端的加密算法列表	**ssh client cipher** { **aes128_ctr** | **aes256_ctr** } *	缺省情况下，不安装WEAKEA插件，SSH客户端只支持**aes128_ctr**和**aes256_ctr**算法，不可以使用**undo ssh client cipher**命令，安装WEAKEA插件后，增加支持**aes256_cbc**、**aes128_cbc**、**3des_cbc**和**des_cbc**算法，并且可以使用**undo ssh client cipher**命令。 系统软件中不包含**aes256_cbc**、**aes128_cbc**、**3des_cbc**和**des_cbc**参数，如需使用，需要安装WEAKEA插件，但是该算法安全性低。为了保证更好的安全性，建议配置**aes256_ctr**或**aes128_ctr**参数。WEAKEA插件安装方法请参见WEAKEA插件使用指南。

操作步骤	命令	说明
（可选）配置SSH客户端上的校验算法列表	**ssh client hmac sha2_256**	缺省情况下，不安装WEAKEA插件，SSH服务器只支持**sha2_256**校验算法，不可以使用**undo ssh server hmac**命令，安装WEAKEA插件后，增加支持**sha2_256_96**、**sha1**、**sha1_96**、**md5**和**md5_96**校验算法，并且可以使用**undo ssh server hmac**命令。 系统软件中不包含**sha2_256_96**、**sha1**、**sha1_96**、**md5**和**md5_96**参数，如需使用，需要安装WEAKEA插件，但是该算法安全性低。为了保证更好的安全性，建议配置**sha2_256**参数。 WEAKEA插件安装方法请参见WEAKEA插件使用指南。
（可选）配置SSH客户端重协商密钥时的参数	**ssh client rekey** { **time** *rekey-time* | **data-limit** *data-limit* | **max-packet** *max-packet* } *	缺省情况下，SSH客户端触发密钥重协商的时间间隔为60分钟，重协商密钥收发数据大小上限为1000MB，重协商密钥收发数据包个数上限为268435456（2^28）个。
IPv4地址	**scp** [**-port** *port-number* | { **public-net** | **vpn-instance** *vpn-instance-name* } | **identity-key** { **dsa** | **rsa** | **ecc** | **rsa_sha2_256** | **rsa_sha2_512** } | **user-identity-key** { **rsa** | **dsa** | **ecc** } | { **-a** *source-address* | **-i** *interface-type interface-number* } | **-r** | **-cipher** *cipher* | **-c**] * *sourcefile destinationfile*	根据地址类型选其一。 **说明** 在使用中需要注意，为了安全性考虑，用户选择加密算法时，建议采用aes128或aes256算法。

操作步骤	命令	说明
IPv6地址	**scp ipv6** [**-port** *port-number* | { **public-net** | **vpn-instance** *vpn-instance-name* } | **identity-key** { **dsa** | **rsa** | **ecc** | **rsa_sha2_256** | **rsa_sha2_512** } | **user-identity-key** { **rsa** | **dsa** | **ecc** } | **-a** *source-address* | **-r** | **-cipher** *-cipher* | **-c**] * *sourcefile destinationfile* [**-oi** *interface-type interface-number*]	

说明

由于文件系统对根目录下的文件个数有限制，当根目录中文件个数大于50个时，继续在根目录中创建文件可能会失败。

----结束

检查配置结果

- 使用**display scp-client**命令，在SCP客户端查看源配置信息。
- 使用**display ssh server-info**命令，查看客户端所有的SSH服务器与公钥之间的对应关系。

8.4.5 配置设备作为 FTPS 客户端访问其他设备的文件

前置任务

在配置通过FTPS访问其他设备的文件之前，需完成以下任务：

- 设备和安全FTP（FTPS）服务器路由可达。
- FTPS服务器端已加载数字证书，能正常访问。
- 已获取FTPS服务器的主机名或IP地址、FTP用户名及密码。

配置流程

须知

从V200R020C00版本开始，缺省情况下FTPS服务器端不接收来自任何接口登录连接的IPv4和IPv6请求，当需要授权客户可以登录服务器时，必须执行命令指定服务器端的源接口或源地址。

通过FTPS访问其他设备文件的配置流程如表8-53所示。

表 8-53 配置设备作为 FTPS 客户端访问其他设备的文件配置流程

序号	配置任务名称	配置任务说明	配置流程说明
1	上传CA证书和证书撤销列表（CRL）	通过其他文件上传方式将所需文件上传至设备。	序号1、2、3有序操作，FTPS连接建立后，序号4、5无操作顺序，序号6（断开连接操作）为最后一步。
2	配置SSL策略并加载CA证书和CRL	-	
3	使用FTPS连接其他设备	-	
4	通过FTP文件操作命令进行文件操作	包括目录操作、文件操作、配置文件传输方式、查看FTP命令在线帮助等。	
5	（可选）更改登录用户	-	
6	断开与FTP服务器的连接	-	

操作步骤

- **上传CA证书和证书撤销列表（CRL）**

  可使用FTP、SFTP或SCP方式将CA证书和CRL文件上传至设备，且要保存至security中，如设备无此目录，可执行命令**mkdir** *security*创建。

  说明

  - 访问FTPS服务器的客户端需要从CA得到CA证书，用来验证服务器数字证书的有效性。
  - CRL也由CA发布，包含了被吊销证书的序列号，若服务器端的数字证书被列入了CRL，则客户端认证服务器不成功，FTPS无法连接。

  证书格式分为PEM格式、ASN1格式和PFX格式。虽然证书的格式不相同，但是证书的内容一样。

  - PEM格式的证书是最常用的一种数字证书格式，文件的扩展名是.pem，适用于系统之间的文本模式传输。
  - ASN1是通用的数字证书格式之一，文件的扩展名是.der，是大多数浏览器的默认格式。
  - PFX是通用的数字证书格式之一，文件的扩展名是.pfx，是可移植的二进制格式。

  CRL文件支持ASN1和PEM两种类型，虽然格式不一样，但是文件的内容一样。

  具体的操作步骤请参考手册中其他文件上传方式的介绍。

- **配置SSL策略并加载CA证书和CRL**

  表 8-54 配置 SSL 策略并加载 CA 证书和 CRL

操作步骤	命令	说明
进入系统视图	**system-view**	-

操作步骤	命令	说明
（可选）定制SSL算法套	**ssl cipher-suite-list** *customization-policy-name*	创建SSL算法套定制策略并进入定制策略视图。 缺省情况下，没有配置SSL算法套定制策略。
	set cipher-suite { **tls12_ck_dss_aes_128_gcm_sha256** | **tls12_ck_dss_aes_256_gcm_sha384** | **tls12_ck_rsa_aes_128_gcm_sha256** | **tls12_ck_rsa_aes_256_gcm_sha384** }	配置SSL算法套定制策略中支持的算法套。 缺省情况下，SSL算法套定制策略中没有配置算法套。 配置算法套定制策略中支持的算法套后，SSL协商时将使用定制策略中配置的策略进行协商。 如果算法套定制策略已经被SSL策略引用，可以对算法套进行增加、修改和部分删除，但不能将算法套定制策略中的算法套全部删除。 系统软件中不包含**tls12_ck_rsa_aes_256_cbc_sha256**、**tls1_ck_dhe_dss_with_aes_128_sha**、**tls1_ck_dhe_dss_with_aes_256_sha**、**tls1_ck_dhe_rsa_with_aes_128_sha**、**tls1_ck_dhe_rsa_with_aes_256_sha**、**tls1_ck_rsa_with_aes_128_sha**和**tls1_ck_rsa_with_aes_256_sha**参数，如需使用，需要安装WEAKEA插件，但是该算法安全性低。为了保证更好的安全性，建议使用其它算法。WEAKEA插件安装方法请参见WEAKEA插件使用指南。
	quit	返回系统视图。
配置SSL策略并进入SSL策略视图	**ssl policy** *policy-name*	-

操作步骤	命令	说明
（可选）设置SSL策略所采用的最低SSL版本	**ssl minimum version** { **tls1.1** | **tls1.2** | **tls1.3** }	缺省情况下，SSL策略所采用的最低SSL版本为TLS1.2。 系统软件中不包含**tls1.0**参数，如需使用，需要安装WEAKEA插件，但是该算法安全性低。为了保证更好的安全性，建议配置**tls1.2**参数。WEAKEA插件安装方法请参见WEAKEA插件使用指南。
（可选）在SSL策略中绑定指定的SSL算法套定制策略	**binding cipher-suite-customization** *customization-policy-name*	缺省情况下，SSL策略未绑定算法套定制策略，使用默认的算法套。SSL策略默认支持如下算法套： • tls1_ck_rsa_with_aes_256_sha • tls1_ck_rsa_with_aes_128_sha • tls1_ck_dhe_rsa_with_aes_256_sha • tls1_ck_dhe_dss_with_aes_256_sha • tls1_ck_dhe_rsa_with_aes_128_sha • tls1_ck_dhe_dss_with_aes_128_sha • tls12_ck_rsa_aes_256_cbc_sha256 绑定的SSL算法套定制策略中如果仅有一种类型的算法（RSA或DSS），SSL策略需要加载对应类型的证书，确保SSL协商时能成功。
加载PEM格式的证书	**trusted-ca load pem-ca** *ca-filename*	根据证书类型，选其一。 一个SSL策略最多可以同时加载4个CA证书。如果多次加载不同的CA证书，CA证书会被增加到现有的CA证书列表中。 **说明** 从V200R008C00版本及之后版本降级至以前版本时，需要先备份当前配置中加载的SSL私钥文件。
加载ASN1格式的证书	**trusted-ca load asn1-ca** *ca-filename*	
加载PFX格式的证书	**trusted-ca load pfx-ca** *ca-filename* **auth-code cipher** *auth-code*	
加载CRL	**crl load** { **pem-crl** | **asn1-crl** } *crl-filename*	一个SSL策略最多可以同时加载2个CRL文件。如果多次加载不同的CRL文件，CRL文件会被增加到现有的CRL文件列表中。

说明

- 如果FTPS服务器端配置的证书文件包含的是单个证书，则需要在客户端配置此证书以上的各级CA证书，直接到根证书为止。
- 如果FTPS服务器端配置的是证书链，则只需在客户端配置根证书即可。
- 若没有加载CRL，其实是不影响FTPS的正常连接的，但此时客户端无法保证服务器端数字证书的有效性，建议在客户端加载CRL，并定期更新。

- **使用FTPS连接其他设备**

表 8-55 使用 FTPS 连接其他设备

操作步骤	命令	说明
IPv4网络	**ftp ssl-policy** *policy-name* [**-a** *source-ip-address* | **-i** *interface-type interface-number*] *host* [*port-number*] [**public-net** | **vpn-instance** *vpn-instance-name*]	根据地址类型，二选一。
IPv6网络	**ftp ssl-policy** *policy-name* **ipv6** *host-ipv6-address* [*port-number*]	

使用FTPS连接其他设备，也可以先执行**ftp**命令进入FTP客户端视图，然后再执行**open**命令完成FTP连接操作。

用户访问服务器时，需要经过验证，输入正确的用户名和密码后，则可以进入FTP客户端视图，对服务器上的文件进行管理和操作。

- **通过FTP命令进行文件操作**

用户访问FTPS服务器后，可对FTPS服务器中的文件进行操作（与普通FTP方式一样）。

说明

用户的操作权限受限于服务器上对该用户的权限设置。

由于文件系统对根目录下的文件个数有限制，当根目录中文件个数大于50个时，继续在根目录中创建文件可能会失败。

以下各操作没有严格顺序，可根据需求选择一种或多种操作项目。

表 8-56 通过 FTP 命令进行文件操作

操作项目	命令	说明
改变服务器上的工作路径	**cd** *remote-directory*	-

操作项目	命令	说明
改变服务器的工作路径到上一级目录	**cdup**	-
显示服务器工作路径	**pwd**	-
显示或者改变客户端的工作路径	**lcd** [*local-directory*]	与**pwd**不同的是，**lcd**命令执行后显示的是客户端的本地工作路径，而**pwd**显示的则是远端服务器的工作路径。
在服务器上创建目录	**mkdir** *remote-directory*	创建的目录可以为字母和数字等的组合，但不可以为<、>、？ 、\、： 等特殊字符。
在服务器上删除目录	**rmdir** *remote-directory*	-
显示服务器上指定目录或文件的信息	**dir/ls** [*remote-filename* [*local-filename*]]	• **ls**命令只能显示出目录/文件的名称，而**dir**命令可以查看目录/文件的详细信息，如大小，创建日期等。 • 如果指定远程文件时没有指定路径名称，那么系统将在用户的授权目录下搜索指定的文件。
删除服务器上指定文件	**delete** *remote-filename*	-
上传单个或多个文件	**put** *local-filename* [*remote-filename*] 或 **mput** *local-filenames*	• **put**命令是上传单个文件。 • **mput**命令是上传多个文件。
下载单个或多个文件	**get** *remote-filename* [*local-filename*] 或 **mget** *remote-filenames*	• **get**命令是下载单个文件。 • **mget**命令是下载多个文件。
配置传输文件的数据类型为ASCII模式或二进制模式	**ascii** 或 **binary**	二选一 • 缺省情况下，文件传输方式为ASCII模式。 • 传输文本文件使用ASCII方式，传输程序、系统软件、数据库文件等使用二进制模式。

操作项目	命令	说明
配置文件传输方式为被动方式或主动方式	**passive** 或 **undo passive**	二选一 缺省情况下，数据传输方式是主动方式。
查看FTP命令的在线帮助	**remotehelp** [*command*]	-
使能系统的提示功能	**prompt**	缺省情况下，不使能信息提示。
打开verbose开关	**verbose**	如果打开verbose开关，将显示所有FTP响应，包括FTP协议信息，以及FTP服务器返回的详细信息。

- **（可选）更改登录用户**

  设备可以在不退出FTP客户端视图的情况下，以其他的用户名登录到FTPS服务器。所建立的FTP连接，与执行**ftp ssl-policy**命令建立的FTP连接完全相同。

操作步骤	命令	说明
FTP客户端视图下，更改当前的登录用户	**user** *user-name* [*password*]	更改当前的登录用户后，原用户与服务器的连接将断开。

- **断开与FTPS服务器的连接**

  用户可以在FTP客户端视图中选择不同的命令断开与FTPS服务器的连接。

操作步骤	命令	说明
终止与服务器的连接，并退回到用户视图	**bye** 或 **quit**	二选一。
终止与服务器的连接，并退回到FTP客户端视图	**close** 或 **disconnect**	

----结束

检查配置结果

- 使用**display ssl policy**命令，查看FTPS客户端配置的SSL策略、加载的CA证书和CRL。

8.5 文件管理的配置举例

8.5.1 通过登录系统进行文件操作示例

组网需求

用户通过Console口、Telnet或STelnet方式登录设备，需要对设备上的文件进行以下操作：

- 查看当前目录下的文件及子目录。
- 创建目录**test**，将文件**vrpcfg.zip**复制至**test**目录下，并命名为**backup.zip**。
- 查看**test**目录下的文件。

图 8-2 登录设备进行文件操作组网图

操作步骤

步骤1 查看当前目录下的文件及子目录。

```
<HUAWEI> system-view
[HUAWEI] sysname Switch
[Switch] quit
<Switch> dir
Directory of flash:/

  Idx  Attr     Size(Byte)  Date        Time       FileName
    0  -rw-           889  Mar 01 2012 14:41:56   private-data.txt
    1  -rw-         6,311  Feb 17 2012 14:05:04   backup.cfg
    2  -rw-         2,393  Mar 06 2012 17:20:10   vrpcfg.zip
    3  -rw-           812  Dec 12 2011 15:43:10   hostkey
    4  drw-             -  Mar 01 2012 14:41:46   compatible
    5  -rw-           540  Dec 12 2011 15:43:12   serverkey
...
65,233 KB total (7,289 KB free)
```

步骤2 创建目录**test**，将文件**vrpcfg.zip**复制至**test**目录下，并命名为**backup.zip**。

创建目录**test**。

```
<Switch> mkdir test
```

复制**vrpcfg.zip**至**test**目录下，并命名为**backup.zip**。

```
<Switch> copy vrpcfg.zip flash:/test/backup.zip
```

说明

如果不指定目标文件名，则目标文件名默认为源文件名，即目标文件和源文件同名。

步骤3 查看**test**目录下的文件。

进入**test**目录。

```
<Switch> cd test
```

查看当前的工作路径。

```
<Switch> pwd
flash:/test
```

查看**test**目录下的文件。

```
<Switch> dir
Directory of flash:/test/

 Idx  Attr     Size(Byte)  Date        Time       FileName
   0  -rw-         2,399  Mar 12 2012 11:16:44   backup.zip

65,233 KB total (7,285 KB free)
```

----结束

配置文件

Switch的配置文件

```
#
sysname Switch
#
return
```

8.5.2 FTP 服务器配置示例

组网需求

如图8-3所示，PC与设备之间路由可达，10.136.23.5是设备的管理网口IP地址，设备需要进行升级操作，要求将设备作为FTP服务器，从终端PC将系统软件上传至设备，且保存当前设备的配置文件到终端进行备份。

图 8-3 通过 FTP 进行文件操作组网图

配置思路

采用如下的思路配置通过FTP进行文件操作：

1. 配置设备的FTP功能及FTP用户信息（包括用户名及密码、用户级别、服务类型、授权目录）。
2. 保存设备当前配置文件。
3. 从终端PC通过FTP连接设备。
4. 将系统软件上传至设备以及配置文件备份至PC。

说明

当所处环境不足够安全时，建议选择较安全的SFTP接入方式登录设备，具体配置案例请参见**SFTP服务器配置示例**。

操作步骤

步骤1 配置设备的FTP功能及FTP用户信息。

```
<HUAWEI> system-view
[HUAWEI] sysname FTP_Server
[FTP_Server] ftp server-source -i MEth 0/0/1
//如果设备无管理网口，则可配置为管理IP地址对应的接口。如果此处服务器端源地址配置为了非管理IP地址及其对应的接口，则客户端必须使用配置的源地址才能连接服务器。
[FTP_Server] ftp server enable
[FTP_Server] aaa
[FTP_Server-aaa] local-user admin1234 password irreversible-cipher YsHsjx_202206
[FTP_Server-aaa] local-user admin1234 privilege level 15
[FTP_Server-aaa] local-user admin1234 service-type ftp
[FTP_Server-aaa] local-user admin1234 ftp-directory flash:/
[FTP_Server-aaa] quit
[FTP_Server] quit
```

步骤2 保存设备当前配置文件。

```
<FTP_Server> save
```

步骤3 从终端PC通过FTP连接设备，输入用户名**admin1234**和密码**YsHsjx_202206**，并采用binary模式进行文件传输。

终端以Window XP操作系统为例说明。

```
C:\Documents and Settings\Administrator> ftp 10.136.23.5
连接到 10.136.23.5。
220 FTP service ready.
用户 (10.136.23.5:(none)): admin1234
331 Password required for admin1234.
密码:
230 User logged in.
ftp> binary
200 Type set to I.
ftp>
```

步骤4 将系统软件上传至设备以及配置文件备份至终端。

上传系统软件至设备。

```
ftp> put devicesoft.cc
200 Port command okay.
150 Opening BINARY mode data connection for devicesoft.cc
226 Transfer complete.
ftp: 发送 23876556 字节，用时 25.35Seconds 560.79Kbytes/sec.
```

备份配置文件。

```
ftp> get vrpcfg.zip
200 Port command okay.
150 Opening BINARY mode data connection for vrpcfg.zip.
226 Transfer complete.
ftp: 收到 1257 字节，用时 0.03Seconds 40.55Kbytes/sec.
```

说明

用户在进行上传和下载操作时，需要明确客户端FTP的工作路径，例如Windows XP操作系统默认的FTP路径是登录用户的用户文件夹（如：C:\Documents and Settings\Administrator）。待上传的系统软件需要预先保存至此路径下，以及备份的配置文件也将保存在此路径下。

步骤5 检查配置结果。

在设备中执行**dir**命令，查看系统软件配置文件是否上传至设备。

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

```
 Idx  Attr     Size(Byte)  Date       Time       FileName
   0  -rw-             14  Mar 13 2012 14:13:38   back_time_a
   1  drw-              -  Mar 11 2012 00:58:54   logfile
   2  -rw-              4  Nov 17 2011 09:33:58   snmpnotilog.txt
   3  -rw-         11,238  Mar 12 2012 21:15:56   private-data.txt
   4  -rw-          1,257  Mar 12 2012 21:15:54   vrpcfg.zip
   5  -rw-             14  Mar 13 2012 14:13:38   back_time_b
   6  -rw-     23,876,556  Mar 13 2012 14:24:24   devicesoft.cc
   7  drw-              -  Oct 31 2011 10:20:28   sysdrv
   8  drw-              -  Feb 21 2012 17:16:36   compatible
   9  drw-              -  Feb 09 2012 14:20:10   selftest
  10  -rw-         19,174  Feb 20 2012 18:55:32   backup.cfg
  11  -rw-         23,496  Dec 15 2011 20:59:36   20111215.zip
  12  -rw-            588  Nov 04 2011 13:54:04   servercert.der
  13  -rw-            320  Nov 04 2011 13:54:26   serverkey.der
  14  drw-              -  Nov 04 2011 13:58:36   security
...
65,233 KB total (7,289 KB free)
```

在终端FTP用户的工作路径下，可以看到**vrpcfg.zip**文件已保存至此路径。

----结束

配置文件

FTP_Server的配置文件

```
#
sysname FTP_Server
# FTP server enable
FTP server-source -i MEth 0/0/1
#
aaa
 local-user admin1234 password irreversible-cipher $1a$P2m&M5d"'JHR7b~SrcHF\Z\,2R"t&6V|zOLh9y$>M
\bjG$D>%@Ug/<3I$+=Y$
 local-user admin1234 privilege level 15
 local-user admin1234 ftp-directory flash:/
 local-user admin1234 service-type ftp
#
return
```

相关信息

视频

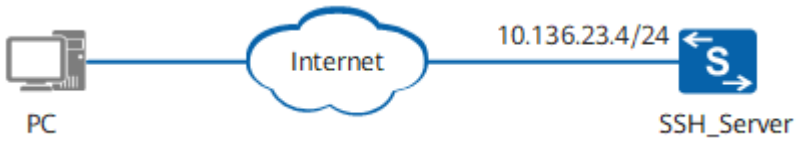
如何通过FTP拷贝文件

8.5.3 SFTP 服务器配置示例

组网需求

如图8-4所示，终端PC与设备路由可达，10.136.23.4是设备的管理网口IP地址。用户希望在终端与设备之间进行安全的文件传输操作，以防止普通FTP服务带来的“中间人”攻击和一些网络欺骗（DNS欺骗和IP欺骗）。将设备配置为SSH服务器，提供SFTP服务，服务器通过对客户端的认证和双向的数据加密，实现用户对安全文件传输操作的要求。

图 8-4 配置通过 SFTP 进行文件操作组网图



配置思路

采用如下的思路配置用户通过SFTP进行文件操作：

1. 在SSH服务器端生成本地密钥对及使能SFTP服务器功能，实现在服务器端和客户端进行安全地数据交互。
2. 配置SSH服务器端的VTY用户界面。
3. 配置SSH用户，包括认证方式、服务类型、授权目录以及用户名和密码等。
4. 从终端通过第三方软件OpenSSH实现访问SSH服务器。

操作步骤

步骤1 在服务器端生成本地密钥对，并使能SFTP服务器功能。

```
<HUAWEI> system-view
[HUAWEI] sysname SSH_Server
[SSH_Server] dsa local-key-pair create
Info: The key name will be: SSH_Server_Host_DSA.
Info: The key modulus can be any one of the following : 1024,
2048.
Info: If the key modulus is greater than 512, it may take a few
minutes.
Please input the modulus [default=2048]:
Info: Generating keys...
Info: Succeeded in creating the DSA host keys.
[SSH_Server] ssh server-source -i MEth 0/0/1
//如果设备无管理网口，则可配置为管理IP地址对应的接口。如果此处服务器端源地址配置为了非管理IP地址及其对应的接口，则客户端必须使用配置的源地址才能连接服务器。
[SSH_Server] sftp server enable
```

步骤2 在服务器端配置VTY用户界面。

```
[SSH_Server] user-interface vty 0 14
[SSH_Server-ui-vty0-14] authentication-mode aaa
[SSH_Server-ui-vty0-14] protocol inbound ssh
[SSH_Server-ui-vty0-14] quit
```

步骤3 配置SSH用户，包括认证方式、服务类型、授权目录以及用户名和密码等。

```
[SSH_Server] ssh user client001 authentication-type password
[SSH_Server] ssh user client001 service-type sftp
[SSH_Server] ssh user client001 sftp-directory flash:
[SSH_Server] aaa
[SSH_Server-aaa] local-user client001 password irreversible-cipher YsHsjx_202206
[SSH_Server-aaa] local-user client001 privilege level 15
[SSH_Server-aaa] local-user client001 service-type ssh
[SSH_Server-aaa] quit
```

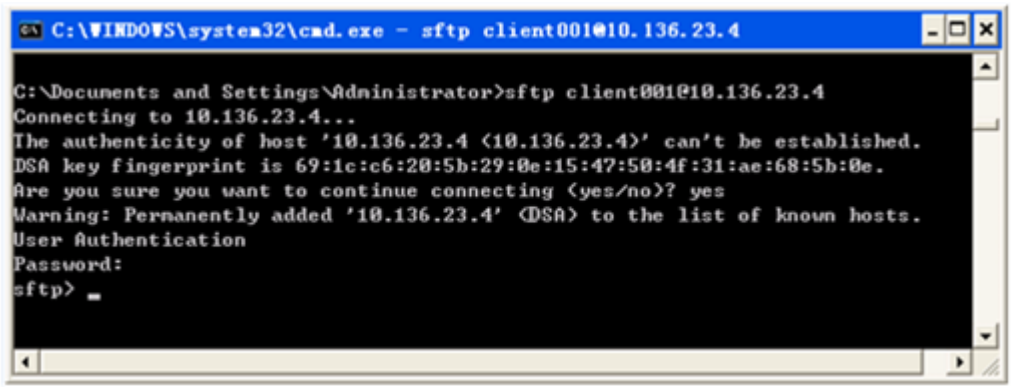
步骤4 从终端通过OpenSSH软件实现访问SFTP服务器。

只有在用户终端安装了OpenSSH软件后，Windows命令行提示符才能识别OpenSSH相关命令。

说明

请使用与当前终端操作系统相匹配的OpenSSH版本，否则可能会导致通过SFTP方式访问交换机失败。

图 8-5 访问界面



通过第三方软件连接设备后，进入SFTP视图，此时可以执行一系列文件操作。

----结束

配置文件

SSH_Server的配置文件

```
#
sysname SSH_Server
#
aaa
 local-user client001 password irreversible-cipher $1a$P2m&M5d"'JHR7b~SrcHF\Z\,2R"t&6V|zOLh9y$>M\bjG
$D>%@Ug/<3I$+=Y$
 local-user client001 privilege level 15
 local-user client001 service-type ssh
#
sftp server enable
ssh user client001
ssh user client001 authentication-type password
ssh user client001 service-type sftp
ssh user client001 sftp-directory flash:
ssh server-source -i MEth 0/0/1 #
user-interface vty 0 14
 authentication-mode aaa
#
return
```

8.5.4 FTPS 服务器配置示例

组网需求

如图8-6所示，终端与设备之间路由可达，10.137.217.201是设备的管理网口IP地址。

用户希望终端与设备之间进行安全的文件传输操作，因为传统的FTP不具备安全机制，采用明文的形式传输数据，会造成“中间人”攻击和网络欺骗。可在设备上部署SSL策略，利用数据加密、身份验证和消息完整性验证机制，为网络上数据的传输提供安全性保证。SSL是在传统FTP服务的基础上提供安全连接，从而很大程度上改善了传统FTP服务器安全性问题。

图 8-6 通过 FTPS 进行文件操作组网图

配置思路

采用如下的思路配置通过FTPS进行文件操作：

1. 先配置设备的普通FTP功能，将PC上存储的数字证书上传到设备上。
2. 将FTPS服务器根目录下的数字证书拷贝到security子目录中，再配置SSL策略并加载数字证书，以实现客户端对服务器的身份验证。
3. 使能安全FTP服务器功能及配置FTP本地用户。
4. 用户通过终端第三方软件连接FTPS服务器。

操作步骤

步骤1 先配置服务器的普通FTP功能，将PC上存储的数字证书上传到服务器上。

配置普通FTP功能：使能FTP功能和配置FTP用户信息。

```
<HUAWEI> system-view
[HUAWEI] sysname FTPS_Server
[FTPS_Server] ftp server-source -i MEth 0/0/1
//如果设备无管理网口，则可配置为管理IP地址对应的接口。如果此处服务器端源地址配置为了非管理IP地址及其对应的接口，则客户端必须使用配置的源地址才能连接服务器。
[FTPS_Server] ftp server enable
[FTPS_Server] aaa
[FTPS_Server-aaa] local-user admin password irreversible-cipher huawei@6789
[FTPS_Server-aaa] local-user admin service-type ftp
[FTPS_Server-aaa] local-user admin privilege level 3
[FTPS_Server-aaa] local-user admin ftp-directory flash:
[FTPS_Server-aaa] quit
[FTPS_Server] quit
```

在终端PC上进入windows命令行提示符输入，执行**ftp**命令指定FTP服务器的连接地址。然后输入正确的用户名和密码与FTP服务器建立FTP连接。在用户终端将数字证书及私钥文件上传到服务器上。

上述步骤成功执行后，在FTP服务器端执行命令**dir**，可看到成功上传的数字证书及私钥文件。

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

Idx  Attr     Size(Byte)  Date       Time        FileName
   0  drw-              -  May 10 2011 05:05:40   src
   1  -rw-        524,575  May 10 2011 05:05:53   private-data.txt
   2  -rw-            446  May 10 2011 05:05:51   vrpcfg.zip
   3  -rw-          1,302  May 10 2011 05:32:05   4_servercert_der_dsa.der
   4  -rw-            951  May 10 2011 05:32:44   4_serverkey_der_dsa.der
...
65,233 KB total (7,289 KB free)
```

步骤2 配置SSL策略并加载数字证书。

创建security子目录，并将安全证书移动到security子目录。


```
<FTPS_Server> mkdir security/
<FTPS_Server> move 4_servercert_der_dsa.der security/
<FTPS_Server> move 4_serverkey_der_dsa.der security/
```

上述步骤成功执行后，在security子目录下执行命令**dir**，可看到拷贝成功的数字证书及私钥文件。

```
<FTPS_Server> cd security/
<FTPS_Server> dir
Directory of flash:/security/

 Idx  Attr     Size(Byte)  Date        Time       FileName
   0  -rw-          1,302  May 10 2011 05:44:34   4_servercert_der_dsa.der
   1  -rw-            951  May 10 2011 05:45:22   4_serverkey_der_dsa.der

65,233 KB total (7,289 KB free)
```

创建SSL策略，并加载ASN1格式的数字证书。

```
<FTPS_Server> system-view
[FTPS_Server] ssl policy ftp_server
[FTPS_Server-ssl-policy-ftp_server] certificate load asn1-cert 4_servercert_der_dsa.der key-pair dsa key-file 4_serverkey_der_dsa.der
[FTPS_Server-ssl-policy-ftp_server] quit
```

步骤3 使能安全FTP服务器功能及配置FTP本地用户。

使能安全FTP服务器功能。

说明

使能安全FTP服务功能，必须去使能普通FTP服务器功能。

```
[FTPS_Server] undo ftp server
[FTPS_Server] ftp secure-server ssl-policy ftp_server
[FTPS_Server] ftp secure-server enable
```

配置FTP本地用户。

使用上面配置过的**admin**用户即可。

步骤4 用户通过终端第三方软件连接FTPS服务器。

具体操作过程请参见第三方软件的帮助文档。

步骤5 检查配置结果。

在安全FTP服务器端执行命令**display ssl policy**，可以看到加载的证书详细信息。

```
[FTPS_Server] display ssl policy

      SSL Policy Name: ftp_server
    Policy Applicants:
       Key-pair Type: DSA
 Certificate File Type: ASN1
     Certificate Type: certificate
 Certificate Filename: 4_servercert_der_dsa.der
    Key-file Filename: 4_serverkey_der_dsa.der
           Auth-code:
                MAC:
          CRL File:
      Trusted-CA File:
         Issuer Name:
  Validity Not Before:
   Validity Not After:
```

在安全FTP服务器端执行命令**display ftp-server**，可以看到SSL策略名称、安全FTP服务器的状态是running。

```
[FTPS_Server] display ftp-server
  FTP server is stopped
```

```
Max user number              5
User count                   1
Timeout value(in minute)     30
Listening port               21
Acl number                   0
FTP server's source address  0.0.0.0
FTP SSL policy               ftp_server
FTP Secure-server is running
```

用户可以通过支持SSL的FTP客户端软件与安全FTP服务器建立连接，并实现文件的上传和下载。

----结束

配置文件

FTPS_Server的配置文件

```
#
sysname FTPS_Server
#
FTP secure-server enable
FTP server-source -i MEth 0/0/1
ftp secure-server ssl-policy ftp_server
#
aaa
 local-user admin password irreversible-cipher $1a$P2m&M5d"'JHR7b~SrcHF\Z\,2R"t&6V|zOLh9y$>M\bjG
$D>%@Ug/<3I$+=Y$
 local-user admin privilege level 3
 local-user admin ftp-directory flash:
 local-user admin service-type ftp
#
ssl policy ftp_server
 certificate load asn1-cert 4_servercert_der_dsa.der key-pair dsa key-file 4_serverkey_der_dsa.der
#
return
```

8.5.5 TFTP 客户端配置示例

组网需求

如图8-7所示，远端服务器提供TFTP Server功能，IP地址为10.1.1.1/24。设备作为TFTP客户端，IP地址为10.2.1.1/24，与服务器之间的路由可达。

设备需要进行升级操作，要求：从TFTP服务器上下载系统软件至设备，且备份当前设备的配置文件到TFTP服务器。

图 8-7 配置通过 TFTP 访问其他设备文件组网图

配置思路

采用如下的思路配置TFTP传输文件功能：

1. 在TFTP服务器端运行TFTP软件，并设置TFTP的工作路径。
2. 在设备上使用TFTP命令下载和上传文件。

操作步骤

步骤1 在TFTP服务器端运行TFTP软件，并设置TFTP的工作路径。（具体操作见第三方软件帮助文档）

步骤2 在设备上使用TFTP命令下载和上传文件。

```
<HUAWEI> tftp 10.1.1.1 get devicesoft.cc
Info: Transfer file in binary mode.
Downloading the file from the remote TFTP server. Please wait...\
TFTP: Downloading the file successfully.
23876556 bytes received in 199 seconds.
<HUAWEI> tftp 10.1.1.1 put vrpcfg.zip
Info: Transfer file in binary mode.
Uploading the file to the remote TFTP server. Please wait...|
TFTP: Uploading the file successfully.
7717 bytes send in 1 second.
```

步骤3 检查配置结果。

在设备中执行**dir**命令，查看系统软件是否下载至设备。

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

  Idx  Attr     Size(Byte)  Date        Time       FileName
    0  -rw-            14  Mar 13 2012 14:13:38   back_time_a
    1  drw-             -  Mar 11 2012 00:58:54   logfile
    2  -rw-             4  Nov 17 2011 09:33:58   snmpnotilog.txt
    3  -rw-        11,238  Mar 12 2012 21:15:56   private-data.txt
    4  -rw-         7,717  Mar 12 2012 21:15:54   vrpcfg.zip
    5  -rw-            14  Mar 13 2012 14:13:38   back_time_b
    6  -rw-    23,876,556  Mar 13 2012 14:24:24   devicesoft.cc
    7  drw-             -  Oct 31 2011 10:20:28   sysdrv
    8  drw-             -  Feb 21 2012 17:16:36   compatible
    9  drw-             -  Feb 09 2012 14:20:10   selftest
   10  -rw-        19,174  Feb 20 2012 18:55:32   backup.cfg
   11  -rw-        43,496  Dec 15 2011 20:59:36   20111215.zip
   12  -rw-           588  Nov 04 2011 13:54:04   servercert.der
   13  -rw-           320  Nov 04 2011 13:54:26   serverkey.der
   14  drw-             -  Nov 04 2011 13:58:36   security
...
65,233 KB total (7,289 KB free)
```

在TFTP服务器的工作路径下，可以看到**vrpcfg.zip**文件已保存至此路径。

----结束

配置文件

无

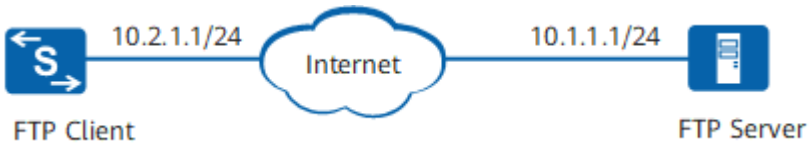
8.5.6 FTP 客户端配置示例

组网需求

如图8-8所示，远端服务器提供FTP Server功能，IP地址为10.1.1.1/24。设备作为FTP客户端，IP地址为10.2.1.1/24，与服务器之间的路由可达。

设备需要进行升级操作，要求：从FTP服务器上下载系统软件至设备，且备份当前设备的配置文件到FTP服务器。

图 8-8 配置通过 FTP 访问其他设备文件组网图



配置思路

采用如下的思路配置FTP访问其他设备文件功能：

1. 在FTP服务器端运行FTP软件，并设置FTP用户的相关信息。
2. 通过FTP与FTP服务器建立连接。
3. 在设备上使用FTP命令下载和上传文件。

操作步骤

步骤1 在FTP服务器端运行FTP软件，并设置FTP用户的相关信息。（具体操作见第三方软件帮助文档）

步骤2 通过FTP与FTP服务器建立连接。

```
<HUAWEI> ftp 10.1.1.1
Trying 10.1.1.1 ...
Press CTRL+K to abort
Connected to 10.1.1.1.
220 FTP service ready.
User(10.1.1.1:(none)):admin
331 Password required for admin.
Enter password:
230 User logged in.

[ftp]
```

步骤3 在设备上使用FTP命令下载和上传文件。

```
[ftp] binary
[ftp] get devicesoft.cc
[ftp] put vrpcfg.zip
[ftp] quit
```

步骤4 检查配置结果。

在设备中执行**dir**命令，查看系统软件是否下载至设备。

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

 Idx  Attr     Size(Byte)  Date        Time       FileName
   0  -rw-           14  Mar 13 2012 14:13:38   back_time_a
   1  drw-            -  Mar 11 2012 00:58:54   logfile
   2  -rw-            4  Nov 17 2011 09:33:58   snmpnotilog.txt
   3  -rw-       11,238  Mar 12 2012 21:15:56   private-data.txt
   4  -rw-        7,717  Mar 12 2012 21:15:54   vrpcfg.zip
   5  -rw-           14  Mar 13 2012 14:13:38   back_time_b
   6  -rw-   23,876,556  Mar 13 2012 14:24:24   devicesoft.cc
   7  drw-            -  Oct 31 2011 10:20:28   sysdrv
   8  drw-            -  Feb 21 2012 17:16:36   compatible
   9  drw-            -  Feb 09 2012 14:20:10   selftest
  10  -rw-       19,174  Feb 20 2012 18:55:32   backup.cfg
  11  -rw-       43,496  Dec 15 2011 20:59:36   20111215.zip
  12  -rw-          588  Nov 04 2011 13:54:04   servercert.der
```



```
  13  -rw-          320  Nov 04 2011 13:54:26   serverkey.der
  14  drw-            -  Nov 04 2011 13:58:36   security
...
65,233 KB total (7,289 KB free)
```

在FTP服务器的工作路径下，可以看到**vrpcfg.zip**文件已保存至此路径。

----结束

配置文件

无

8.5.7 SFTP 客户端配置示例

组网需求

SSH提供了在一个传统不安全的网络环境中，服务器通过对客户端的认证及双向的数据加密，为网络终端访问提供了安全的服务。通过SFTP方式，客户端可以安全地连接到SSH服务器，进行文件的安全传输。

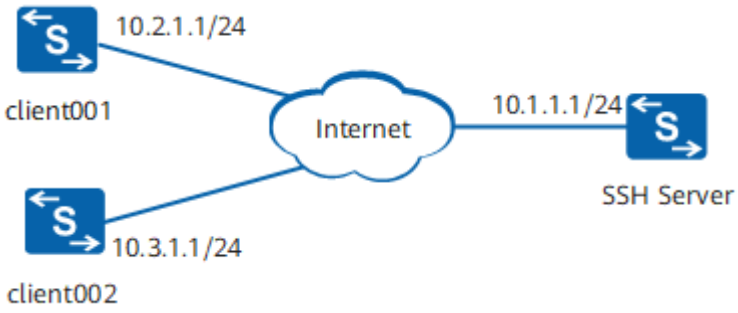
如图8-9所示，SSH服务器与客户端client001、client002路由可达，此例中用华为设备作为SSH服务器。

要求：两个客户端分别使用password方式和DSA方式与SSH服务器连接，实现安全访问服务器上的文件。

说明

Password认证为不安全的认证，实际应用中建议使用AAA认证。

图 8-9 通过 SFTP 访问其他设备文件组网图



配置思路

采用如下思路配置通过SFTP访问其他设备文件功能：

1. 在服务器端生成本地密钥对及使能SFTP服务器功能，实现在服务器端和客户端进行安全地数据交互。
2. 在SSH服务器上配置用户client001和client002，分别使用password和DSA的认证方式登录SSH服务器。
3. 在客户端client002生成本地密钥对，并将客户端生成的DSA公钥配置到SSH服务器上，实现客户端登录服务器端时，对客户端进行验证。

4. 用户client001和client002分别以SFTP方式登录SSH服务器，实现访问服务器上的文件。

操作步骤

步骤1 在服务器端生成本地密钥对及使能SFTP服务器功能。

```
<HUAWEI> system-view
[HUAWEI] sysname SSH Server
[SSH Server] dsa local-key-pair create
Info: The key name will be: SSH Server_Host_DSA.
Info: The key modulus can be any one of the following : 1024,
2048.
Info: If the key modulus is greater than 512, it may take a few
minutes.
Please input the modulus [default=2048]:
Info: Generating keys...
Info: Succeeded in creating the DSA host keys.
[SSH_Server] ssh server-source -i Vlanif 10   //假设服务器IP地址10.1.1.1对应的接口为Vlanif 10。
[SSH Server] sftp server enable
```

步骤2 在服务器端创建SSH用户。

配置VTY用户界面。

```
[SSH Server] user-interface vty 0 4
[SSH Server-ui-vty0-4] authentication-mode aaa
[SSH Server-ui-vty0-4] protocol inbound ssh
[SSH Server-ui-vty0-4] user privilege level 3
[SSH Server-ui-vty0-4] quit
```

新建用户名为client001的SSH用户，且认证方式为password。

```
[SSH Server] ssh user client001
[SSH Server] ssh user client001 authentication-type password
[SSH Server] ssh user client001 service-type sftp
[SSH Server] ssh user client001 sftp-directory flash:
[SSH Server] aaa
[SSH Server-aaa] local-user client001 password irreversible-cipher Helloworld@6789
[SSH Server-aaa] local-user client001 service-type ssh
[SSH Server-aaa] local-user client001 privilege level 3
[SSH Server-aaa] quit
```

新建用户名为client002的SSH用户，且认证方式为DSA。

```
[SSH Server] ssh user client002
[SSH Server] ssh user client002 authentication-type dsa
[SSH Server] ssh user client002 service-type sftp
[SSH Server] ssh user client002 sftp-directory flash:
```

步骤3 在客户端client002生成本地密钥对，并将客户端生成的DSA公钥配置到SSH服务器上。

客户端生成客户端的本地密钥对。

```
<HUAWEI> system-view
[HUAWEI] sysname client002
[client002] dsa local-key-pair create
Info: The key name will be: SSH Server_Host_DSA.
Info: The key modulus can be any one of the following : 1024,
2048.
Info: If the key modulus is greater than 512, it may take a few
minutes.
Please input the modulus [default=2048]:
Info: Generating keys...
Info: Succeeded in creating the DSA host keys.
```

查看客户端上生成DSA公钥。


```
[client002] display dsa local-key-pair public

=============================================
Time of Key pair created: 2014-03-03 19:11:04+00:00
Key name: client002_Host
Key type: DSA encryption Key
=============================================
Key code:
30820109
  02820100
    C7D92E27 E88745D4 933AB1F5 DA692AC4 1D544BDC
    8EA252B0 E90A5001 1F2567C6 3952DEFD 95EF93C2
    D77E8CDF B36E7F43 57C1D7BA 0978DD7A 2F7F7187
    04FD6A03 C4FFDB58 04B3A0C4 B6E50528 AAE56FF9
    5F66EE00 8E4702DB AA764006 322E6F72 CC9C1A39
    462DBCD0 EA934441 1678BA23 40473EC4 58DF84FA
    20C9CB60 98E5ACDA 2E98B55A 0299FBAB FE91EFA3
    E155E065 7C7FFCD4 4EAB71EC A7A73DD7 AC8474B7
    2DD37D1C 710C6E14 57DA200C 477E45BC 38AC7685
    BD8D6325 CCBE3F32 85435E5B EB6A08DF 752B7EBD
    CE21CFCB F3AC0C35 671E5ACC AFC36F0B 54E646F6
    D12B4BA3 6E9EF69F A5BED377 954709EB CE29A923
    04B347D7 29296E7D 3D5F69AB 4365AA2F
  0203
    010001

 Host public key for PEM format code:
---- BEGIN SSH2 PUBLIC KEY ----
AAAAB3NzaC1yc2EAAAADAQABAAABAQDH2S4n6IdF1JM6sfXaaSrEHVRL3I6iUrDp
ClABHyVnxjlS3v2V75PC136M37Nuf0NXwde6CXjdei9/cYcE/WoDxP/bWASzoMS2
5QUoquVv+V9m7gCORwLbqnZABjIub3LMnBo5Ri280OqTREEWeLojQEc+xFjfhPog
yctgmOWs2i6YtVoCmfur/pHvo+FV4GV8f/zUTqtx7KenPdeshHS3LdN9HHEMbhRX
2iAMR35FvDisdoW9jWMlzL4/MoVDXlvragjfdSt+vc4hz8vzrAw1Zx5azK/DbwtU
5kb20StLo26e9p+lvtN3lUcJ684pqSMEs0fXKSlufT1faatDZaov
---- END SSH2 PUBLIC KEY ----

Public key code for pasting into OpenSSH authorized_keys file :
ssh-dsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDH2S4n6IdF1JM6sfXaaSrEHVRL3I6iUrDpClABHyVnxjlS3v2V75PC13
6M37Nuf0NXwde6CXjdei9/cYcE/WoDxP/bWASz
oMS25QUoquVv+V9m7gCORwLbqnZABjIub3LMnBo5Ri280OqTREEWeLojQEc
+xFjfhPogyctgmOWs2i6YtVoCmfur/pHvo+FV4GV8f/zUTqtx7KenPdeshHS3LdN9HHEMbhRX
2iAMR35FvDisdoW9jWMlzL4/MoVDXlvragjfdSt+vc4hz8vzrAw1Zx5azK/DbwtU5kb20StLo26e9p
+lvtN3lUcJ684pqSMEs0fXKSlufT1faatDZaov= dsa-key
```

将客户端上产生的DSA公钥配置到服务器端(上面**display**命令显示信息中黑体部分即为客户端产生的DSA公钥，将其拷贝粘贴至服务器端)。

```
[SSH Server] dsa peer-public-key dsakey001 encoding-type der
[SSH Server-dsa-public-key] public-key-code begin
[SSH Server-dsa-key-code] 30820109
[SSH Server-dsa-key-code] 02820100
[SSH Server-dsa-key-code] C7D92E27 E88745D4 933AB1F5 DA692AC4 1D544BDC
[SSH Server-dsa-key-code] 8EA252B0 E90A5001 1F2567C6 3952DEFD 95EF93C2
[SSH Server-dsa-key-code] D77E8CDF B36E7F43 57C1D7BA 0978DD7A 2F7F7187
[SSH Server-dsa-key-code] 04FD6A03 C4FFDB58 04B3A0C4 B6E50528 AAE56FF9
[SSH Server-dsa-key-code] 5F66EE00 8E4702DB AA764006 322E6F72 CC9C1A39
[SSH Server-dsa-key-code] 462DBCD0 EA934441 1678BA23 40473EC4 58DF84FA
[SSH Server-dsa-key-code] 20C9CB60 98E5ACDA 2E98B55A 0299FBAB FE91EFA3
[SSH Server-dsa-key-code] E155E065 7C7FFCD4 4EAB71EC A7A73DD7 AC8474B7
[SSH Server-dsa-key-code] 2DD37D1C 710C6E14 57DA200C 477E45BC 38AC7685
[SSH Server-dsa-key-code] BD8D6325 CCBE3F32 85435E5B EB6A08DF 752B7EBD
[SSH Server-dsa-key-code] CE21CFCB F3AC0C35 671E5ACC AFC36F0B 54E646F6
[SSH Server-dsa-key-code] D12B4BA3 6E9EF69F A5BED377 954709EB CE29A923
[SSH Server-dsa-key-code] 04B347D7 29296E7D 3D5F69AB 4365AA2F
[SSH Server-dsa-key-code] 0203
[SSH Server-dsa-key-code] 010001
[SSH Server-dsa-key-code] public-key-code end
[SSH Server-dsa-public-key] peer-public-key end
```


为SSH用户client002绑定SSH客户端的DSA公钥。

```
[SSH Server] ssh user client002 assign dsa-key dsakey001
```

步骤4 SFTP客户端连接SSH服务器。

第一次登录，使能SSH客户端首次认证功能。

使能客户端client001首次认证功能。

```
<HUAWEI> system-view
[HUAWEI] sysname client001
[client001] ssh client first-time enable
```

使能客户端client002首次认证功能。

```
[client002] ssh client first-time enable
```

SFTP客户端client001用password认证方式连接SSH服务器。

```
[client002] sftp 10.1.1.1
Please input the username:client001
Trying 10.1.1.1 ...
Press CTRL+K to abort
Connected to 10.1.1.1 ...
password:SSH_SERVER_CODE

Please select public key type for user authentication [R for RSA; D for DSA; Enter for Skip publickey
authentication; Ctrl_C for Cancel], Please select [R, D, Enter or
Ctrl_C]:D

sftp-client>
```

SFTP客户端client002用DSA认证方式连接SSH服务器。

```
[client002] sftp 10.1.1.1
Please input the username:client002
Trying 10.1.1.1 ...
Press CTRL+K to abort
Connected to 10.1.1.1 ...
password:SSH_SERVER_CODE

Please select public key type for user authentication [R for RSA; D for DSA; Enter for Skip publickey
authentication; Ctrl_C for Cancel], Please select [R, D, Enter or
Ctrl_C]:D

sftp-client>
```

步骤5 检查配置结果。

配置完成后，在SSH服务器端执行**display ssh server status**命令可以查看到SFTP服务已经使能。执行**display ssh user-information**命令可以查看服务器端SSH用户信息。

查看SSH状态信息。

```
[SSH Server] display ssh server status
 SSH version                    :1.99
 SSH connection timeout             :60 seconds
 SSH server key generating interval  :0 hours
 SSH authentication retries         :3 times
 SFTP server                   :Enable
 Stelnet server                :Disable
 Scp server                    :Disable
 SSH server source                :0.0.0.0
 ACL4 number                      :0
 ACL6 number                      :0
```

查看SSH用户信息。


```
[SSH Server] display ssh user-information
 User 1:
     User Name           : client001
     Authentication-type  : password
     User-public-key-name : -
     User-public-key-type : -
     Sftp-directory       : flash:
     Service-type         : sftp
     Authorization-cmd    : No
 User 2:
     User Name           : client002
     Authentication-type  : dsa
     User-public-key-name : dsakey001
     User-public-key-type : dsa
     Sftp-directory       : flash:
     Service-type         : sftp
     Authorization-cmd    : No
```

----结束

配置文件

- SSH服务器上的配置文件

```
#
sysname SSH Server
#
dsa peer-public-key dsakey001 encoding-type der
 public-key-code begin
  30820109
    02820100
      C7D92E27 E88745D4 933AB1F5 DA692AC4 1D544BDC 8EA252B0 E90A5001 1F2567C6
      3952DEFD 95EF93C2 D77E8CDF B36E7F43 57C1D7BA 0978DD7A 2F7F7187 04FD6A03
      C4FFDB58 04B3A0C4 B6E50528 AAE56FF9 5F66EE00 8E4702DB AA764006 322E6F72
      CC9C1A39 462DBCD0 EA934441 1678BA23 40473EC4 58DF84FA 20C9CB60 98E5ACDA
      2E98B55A 0299FBAB FE91EFA3 E155E065 7C7FFCD4 4EAB71EC A7A73DD7 AC8474B7
      2DD37D1C 710C6E14 57DA200C 477E45BC 38AC7685 BD8D6325 CCBE3F32 85435E5B
      EB6A08DF 752B7EBD CE21CFCB F3AC0C35 671E5ACC AFC36F0B 54E646F6 D12B4BA3
      6E9EF69F A5BED377 954709EB CE29A923 04B347D7 29296E7D 3D5F69AB 4365AA2F
    0203
      010001
 public-key-code end
peer-public-key end
#
aaa
 local-user client001 password irreversible-cipher $1a$P2m&M5d"'JHR7b~SrcHF\Z\,2R"t&6V|zOLh9y
$>M\bjG$D>%@Ug/<3I$+=Y$
 local-user client001 privilege level 3
 local-user client001 service-type ssh
#
sftp server enable
ssh user client001
ssh user client001 authentication-type password
ssh user client001 service-type sftp
ssh user client001 sftp-directory flash:
ssh user client002
ssh user client002 authentication-type dsa
ssh user client002 assign dsa-key dsakey001
ssh user client002 service-type sftp
ssh user client002 sftp-directory flash:
ssh server-source -i Vlanif 10
#
user-interface vty 0 4
 authentication-mode aaa
 user privilege level 3
#
return
```

- SSH客户端client001的配置文件

```
#
sysname client001
#
ssh client first-time enable
#
return
```

- SSH客户端client002的配置文件

```
#
sysname client002
#
ssh client first-time enable
#
return
```

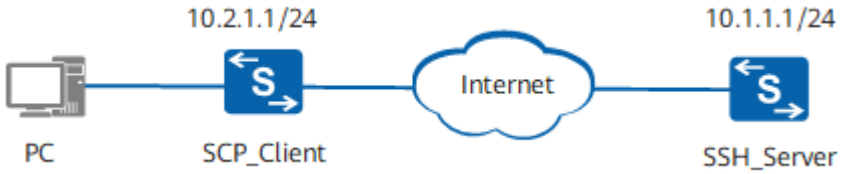
8.5.8 SCP 客户端配置示例

组网需求

与使用SFTP协议传输文件相比，SCP协议可以简化用户传输文件的操作，将用户身份认证、文件传输等步骤合并，提高配置效率。

如图8-10所示，作为SCP客户端的设备和服务器路由可达，并从SSH服务器中下载文件至客户端。

图 8-10 配置通过 SCP 访问其他设备文件配置示例组网图



配置思路

采用如下的思路配置通过SCP访问其他设备文件：

1. 在SSH服务器端生成本地密钥对。
2. 在SSH服务器端创建SSH用户。
3. 在SSH服务器端使能SCP功能。
4. 从SSH服务器下载文件至本地。

操作步骤

步骤1 在服务器端生成本地密钥对。

```
<HUAWEI> system-view
[HUAWEI] sysname SSH_Server
[SSH_Server] dsa local-key-pair create
Info: The key name will be: SSH_Server_Host_DSA.
Info: The key modulus can be any one of the following : 1024, 2048.
Info: If the key modulus is greater than 512, it may take a few minutes.
Please input the modulus [default=2048]:
Info: Generating keys...
Info: Succeeded in creating the DSA host keys.
```

步骤2 在服务器端创建SSH用户。

配置VTY用户界面。

```
[SSH_Server] user-interface vty 0 14
[SSH_Server-ui-vty0-14] authentication-mode aaa
[SSH_Server-ui-vty0-14] protocol inbound ssh
[SSH_Server-ui-vty0-14] quit
```

新建用户名为Client001的SSH用户，且认证方式为password，服务方式为all。

```
[SSH_Server] ssh user client001
[SSH_Server] ssh user client001 authentication-type password
[SSH_Server] ssh user client001 service-type all
```

为SSH用户Client001配置密码为Helloworld@6789。

```
[SSH_Server] aaa
[SSH_Server-aaa] local-user client001 password irreversible-cipher Helloworld@6789
[SSH_Server-aaa] local-user client001 service-type ssh
[SSH_Server-aaa] local-user client001 privilege level 3
[SSH_Server-aaa] quit
```

步骤3 在服务器端使能SCP服务。

```
[SSH_Server] ssh server-source -i Vlanif 10   //假设服务器IP地址10.1.1.1对应的接口为Vlanif 10。
[SSH_Server] scp server enable
```

步骤4 从SCP客户端下载服务器上的文件。

第一次登录，使能SSH客户端首次认证功能。

```
<HUAWEI> system-view
[HUAWEI] sysname SCP_Client
[SCP_Client] ssh client first-time enable
```

使用aes256加密算法将文件backup.cfg从IP地址为10.1.1.1的远端SSH服务器下载至本地用户目录下。

```
[SCP_Client] scp -cipher aes256 client001@10.1.1.1:backup.cfg backup.cfg
Trying 10.1.1.1 ...
Press CTRL+K to abort
Connected to 10.1.1.1 ...
The server has not been authenticated. Continue to access it? [Y/N]:y
Do you want to save the server's public key? [Y/N]:y
The server's public key will be saved with the name 10.1.1.1. Please wait.
..
Enter password:
backup.cfg                   100%       19174Bytes          7KByte(s)/sec
```

----结束

配置文件

- SSH_Server的配置文件

```
#
sysname SSH_Server
#
aaa
 local-user client001 password irreversible-cipher $1a$P2m&M5d"'JHR7b~SrcHF\Z\,2R"t&6V|zOLh9y
$>M\bjG$D>%@Ug/<3I$+=Y$
 local-user client001 privilege level 3
 local-user client001 service-type ssh
#
scp server enable
ssh user client001
ssh user client001 authentication-type password
ssh user client001 service-type all
```



```
ssh server-source -i Vlanif 10
#
user-interface vty 0 14
 authentication-mode aaa
#
return
```

- SCP_Client的配置文件

```
#
sysname SCP_Client
#
ssh client first-time enable
#
return
```

8.5.9 FTPS 客户端配置示例

组网需求

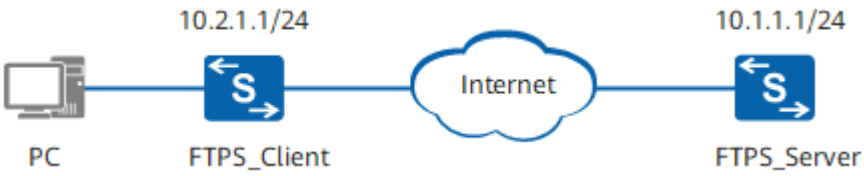
用户希望终端与设备之间进行安全的文件传输操作，因为传统的FTP不具备安全机制，采用明文的形式传输数据，会造成“中间人”攻击和网络欺骗。可在设备上部署SSL策略，利用数据加密、身份验证和消息完整性验证机制，为网络上数据的传输提供安全性保证。SSL是在传统FTP服务的基础上提供安全连接，从而很大程度上改善了传统FTP服务器安全性问题。

如图8-11所示，FTPS客户端和服务器之间路由可达，要求从客户端连接到安全FTP（FTPS）服务器上实现远程管理文件。

- 在作为FTPS客户端的设备上部署SSL策略，并加载CA证书文件，检查证书持有者身份的合法性，并签发证书，以防证书被伪造或篡改，以及对证书和密钥进行管理。
- 在作为FTPS服务器的设备上部署SSL策略，加载数字证书并使能安全FTP服务器功能，检查CA证书文件的合法性，保证合法客户端安全登录服务器。

服务器和客户端所要加载的证书文件需要预先从CA获取。此例中用华为设备作为FTPS服务器。

图 8-11 配置通过 FTPS 访问其他设备文件组网图



配置思路

采用如下的思路配置通过FTPS访问其他设备文件配置示例：

1. 上传证书。
   - 将数字证书及私钥文件上传至作为FTPS服务器的设备上。
   - 将CA证书文件上传至作为FTP客户端的设备上。
2. 加载证书，并配置SSL策略。

- 将服务器根目录下的数字证书文件拷贝到security子目录中，再配置SSL策略并加载数字证书。
- 将客户端根目录下的CA证书文件拷贝到security子目录中，再配置SSL策略并加载CA证书文件。

3. 在FTP服务器端使能安全FTP服务器功能及配置FTP本地用户。
4. 在客户端通过FTP命令连接安全FTP服务器，实现远程文件管理。

操作步骤

步骤1 上传证书。

- 在客户端和服务器分别配置普通FTP服务功能，将所需证书文件上传至客户端和服务器。具体操作可参考**8.3.2 通过FTP进行文件操作**。

  # 上传完成后，使用**dir**命令，在服务器端可看到成功上传的数字证书及私钥文件。

```
<HUAWEI> system-view
[HUAWEI] sysname FTPS_Server
[FTPS_Server] quit
<FTPS_Server> dir
Directory of flash:/

 Idx  Attr     Size(Byte)  Date       Time       FileName
   0  drw-              -  May 10 2011 05:05:40   src
   1  -rw-        524,575  May 10 2011 05:05:53   private-data.txt
   2  -rw-            446  May 10 2011 05:05:51   vrpcfg.zip
   3  -rw-          1,302  Mar 13 2012 18:23:28   4_servercert_der_dsa.der
   4  -rw-            951  Mar 13 2012 18:30:20   4_serverkey_der_dsa.der
...

65,233 KB total (7,289 KB free)
```

  # 在客户端使用**dir**命令，可看到成功上传的CA证书文件。

```
<HUAWEI> system-view
[HUAWEI] sysname FTPS_Client
[FTPS_Client] quit
<FTPS_Client> dir
Directory of flash:/

 Idx  Attr     Size(Byte)  Date       Time       FileName
   0  -rw-        524,558  May 10 2011 04:50:39   private-data.txt
   1  -rw-          1,237  Mar 14 2012 07:46:24   cacert.der
   2  -rw-          1,241  Mar 14 2012 07:46:20   rootcert.der
   3  drw-              -  Apr 09 2011 19:46:14   src
   4  -rw-            421  Apr 09 2011 19:46:14   vrpcfg.zip
   5  -rw-      1,308,478  Apr 14 2011 19:22:45   we1.zip
   6  drw-              -  Apr 10 2011 01:35:54   logfile
   7  -rw-              4  Apr 19 2011 04:24:28   snmpnotilog.txt
   8  drw-              -  Apr 13 2011 11:37:40   lam
...

65,233 KB total (17,489 KB free)
```

步骤2 配置SSL策略并加载证书。

- 在服务器上进行如下配置。

  # 创建security子目录，并将安全证书移动到security子目录。

```
<FTPS_Server> mkdir security/
<FTPS_Server> move 4_servercert_der_dsa.der security/
<FTPS_Server> move 4_serverkey_der_dsa.der security/
```

  # 上述步骤成功执行后，在security子目录下执行命令**dir**，可看到拷贝成功的数字证书及私钥文件。

```
<FTPS_Server> cd security/
<FTPS_Server> dir
```



```
Directory of flash:/security/

 Idx  Attr     Size(Byte)  Date       Time       FileName
   0  -rw-          1,302  Mar 13 2012 18:23:28   4_servercert_der_dsa.der
   1  -rw-            951  Mar 13 2012 18:30:20   4_serverkey_der_dsa.der

65,233 KB total (7,289 KB free)
```

创建SSL策略，并加载ASN1格式的数字证书。

```
<FTPS_Server> system-view
[FTPS_Server] ssl policy ftp_server
[FTPS_Server-ssl-policy-ftp_server] certificate load asn1-cert 4_servercert_der_dsa.der key-pair dsa key-file 4_serverkey_der_dsa.der
[FTPS_Server-ssl-policy-ftp_server] quit
```

上述步骤成功配置后，在服务器端执行命令**display ssl policy**，可以看到加载的证书详细信息。

```
[FTPS_Server] display ssl policy

      SSL Policy Name: ftp_server
    Policy Applicants:
       Key-pair Type: DSA
Certificate File Type: ASN1
    Certificate Type: certificate
Certificate Filename: 4_servercert_der_dsa.der
   Key-file Filename: 4_serverkey_der_dsa.der
         Auth-code:
               MAC:
          CRL File:
     Trusted-CA File:
        Issuer Name:
 Validity Not Before:
  Validity Not After:
```

- 在客户端进行如下配置。

  # 创建security子目录，并将CA证书文件移动到security子目录。

  ```
  <FTPS_Client> mkdir security/
  <FTPS_Client> move cacert.der security/
  <FTPS_Client> move rootcert.der security/
  ```

  # CA证书文件拷贝到security子目录后，在security子目录下执行命令**dir**，可看到拷贝成功的CA证书文件。

  ```
  <FTPS_Client> cd security/
  <FTPS_Client> dir
  Directory of flash:/security/

   Idx  Attr     Size(Byte)  Date       Time       FileName
     0  -rw-          1,237  Mar 14 2012 07:46:24   cacert.der
     1  -rw-          1,241  Mar 14 2012 07:46:20   rootcert.der

  65,233 KB total (17,489 KB free)
  ```

  # 创建SSL策略，并加载CA证书文件。

  ```
  <FTPS_Client> system-view
  [FTPS_Client] ssl policy ftp_client
  [FTPS_Client-ssl-policy-ftp_client] trusted-ca load asn1-ca cacert.der
  [FTPS_Client-ssl-policy-ftp_client] trusted-ca load asn1-ca rootcert.der
  [FTPS_Client-ssl-policy-ftp_client] quit
  ```

  # 上述步骤成功配置后，在FTP客户端执行命令**display ssl policy**，可以看到加载的CA证书文件详细信息。

  ```
  [FTPS_Client] display ssl policy

        SSL Policy Name: ftp_client
      Policy Applicants:
         Key-pair Type:
  Certificate File Type:
      Certificate Type:
  ```

```
Certificate Filename:
  Key-file Filename:
       Auth-code:
            MAC:
        CRL File:
    Trusted-CA File:
  Trusted-CA File 1: Format = ASN1, Filename = cacert.der
  Trusted-CA File 2: Format = ASN1, Filename = rootcert.der
```

步骤3 使能安全FTP服务器功能及配置FTP本地用户。

使能安全FTP服务器功能。

说明

使能安全FTP服务功能，必须去使能普通FTP服务器功能。

```
[FTPS_Server] undo ftp server
[FTPS_Server] ftp secure-server ssl-policy ftp_server
[FTPS_Server] ftp secure-server enable
[FTPS_Server] ftp server-source -i Vlanif 10    //假设服务器IP地址10.1.1.1对应的接口为Vlanif 10。
```

配置FTP本地用户。

```
[FTPS_Server] aaa
[FTPS_Server-aaa] local-user admin password irreversible-cipher Helloworld@6789
[FTPS_Server-aaa] local-user admin service-type ftp
[FTPS_Server-aaa] local-user admin privilege level 3
[FTPS_Server-aaa] local-user admin ftp-directory flash:
[FTPS_Server-aaa] quit
```

此用户可以使用上传证书时FTP用户，也可重新配置新的用户。

步骤4 在FTPS客户端通过FTP命令登录安全FTP服务器实现远程文件管理。

```
[FTPS_Client] ftp ssl-policy ftp_client 10.1.1.1
Trying 10.1.1.1 ...
Press CTRL+K to abort
Connected to 10.1.1.1.
220 FTP service ready.
234 AUTH command successfully, Security mechanism accepted.
200 PBSZ is ok.
200 Data channel security level is changed to private.
User(10.1.1.1:(none)):admin
331 Password required for admin.
Enter password:
230 User logged in.

[ftp]
```

在客户端需要正确输入用户名和密码，才能通过FTPS方式成功登录FTPS服务器。

步骤5 检查配置结果。

在安全FTP服务器端执行命令**display ftp-server**，可以看到SSL策略名称、安全FTP服务器的状态是running。

```
[FTPS_Server] display ftp-server
  FTP server is stopped
  Max user number              5
  User count                   1
  Timeout value(in minute)     30
  Listening port               21
  Acl number                   0
  FTP server's source address  0.0.0.0
  FTP SSL policy               ftp_server
  FTP Secure-server is running
```


在客户端，用户可远程管理服务器上的文件。

----结束

配置文件

- FTPS_Server的配置文件

```
#
sysname FTPS_Server
#
FTP secure-server enable
FTP server-source -i Vlanif10
ftp secure-server ssl-policy ftp_server
#
aaa
 local-user admin password irreversible-cipher $1a$P2m&M5d"'JHR7b~SrcHF\Z\,2R"t&6V|zOLh9y$>M
\bjG$D>%@Ug/<3I$+=Y$
 local-user admin privilege level 3
 local-user admin ftp-directory flash:
 local-user admin service-type ftp
#
ssl policy ftp_server
 certificate load asn1-cert 4_servercert_der_dsa.der key-pair dsa key-file 4_serverkey_der_dsa.der
#
return
```

- FTPS_Client的配置文件

```
#
sysname FTPS_Client
#
ssl policy ftp_client
 trusted-ca load asn1-ca cacert.der
 trusted-ca load asn1-ca rootcert.der
#
return
```

8.6 文件管理的常见配置错误

8.6.1 FTP 登录失败

故障原因

- 未配置FTP服务器端的源地址
- FTP服务器功能没有启动。
- FTP服务器指定端口号不是缺省端口号，且FTP客户端登录时没有指定端口号。
- 未配置FTP用户的验证信息、授权目录及用户级别。
- 登录FTP服务器的用户数达到上限。
- FTP服务器配置了ACL规则限制客户端登录。
- FTP服务器配置了多种认证模式。

操作步骤

步骤1 检查设备上是否配置了FTP服务器端的源地址。

- 对于FTP IPv4

在系统视图下执行命令**display this**，查看是否有**ftp server-source**的配置。如果没有，可以在系统视图下执行命令**ftp server-source**，配置FTP服务器端的源IPv4地址。

- 对于FTP IPv6

  在系统视图下执行命令**display this**，查看是否有**ftp ipv6 server-source**的配置。如果没有，可以在系统视图下执行命令**ftp ipv6 server-source**，配置FTP服务器端的IPv6源地址。

步骤2 检查FTP服务器功能是否启动。

在任意视图下执行命令**display ftp-server**查看FTP服务器的状态。

- 如果FTP服务器没有启动，显示信息如下：

```
<HUAWEI> display ftp-server
Info: The FTP server is already disabled.
```

在系统视图下执行命令**ftp server enable**，使能FTP服务器功能。

```
<HUAWEI> system-view
[HUAWEI] ftp server enable
Info: Succeeded in starting the FTP server.
```

- 如果FTP服务器功能启动，显示信息如下:

```
<HUAWEI> display ftp-server
  FTP server is running
  Max user number              5
  User count                   0
  Timeout value(in minute)     30
  Listening port               21
  Acl number                   0
  FTP server's source address  0.0.0.0
  FTP SSL policy
  FTP Secure-server is stopped
```

步骤3 检查FTP服务器的端口号是否是缺省端口号。

1. 在任意视图下执行命令**display tcp status**查看当前TCP端口尝试连接状态，是否有FTP的缺省端口号是21。

```
<HUAWEI> display tcp status
TCPCB     Tid/Soid Local Add:port       Foreign Add:port      VPNID  State
2a67f47c  6  /1    0.0.0.0:21           0.0.0.0:0             23553  Listening
2b72e6b8  115/4    0.0.0.0:22           0.0.0.0:0             23553  Listening
3265e270  115/1    0.0.0.0:23           0.0.0.0:0             23553  Listening
2a6886ec  115/23   10.137.129.27:23     10.138.77.43:4053     0      Establish
ed
2a680aac  115/14   10.137.129.27:23     10.138.80.193:1525    0      Establish
ed
2a68799c  115/20   10.137.129.27:23     10.138.80.202:3589    0      Establish
ed
```

2. 在任意视图下执行命令**display ftp-server**查看FTP服务器的端口号。

```
<HUAWEI> display ftp-server
  FTP server is running
  Max user number              5
  User count                   0
  Timeout value(in minute)     30
  Listening port               21
  Acl number                   0
  FTP server's source address  0.0.0.0
  FTP SSL policy
  FTP Secure-server is stopped
```

如果当前FTP服务器的端口号不是21，执行命令**ftp server port**，设置FTP服务器的端口号为21。

```
<HUAWEI> system-view
[HUAWEI] undo ftp server
```



```
Warning: The operation will stop the FTP server. Continue? [Y/N]:y
Info: Succeeded in closing the FTP server.
[HUAWEI] ftp server port 21
[HUAWEI] ftp server enable
Info: Succeeded in starting the FTP server.
```

或者在FTP连接时，在客户端指定服务端设置的端口号。

步骤4 检查是否配置FTP用户的验证信息、授权目录及用户级别。

FTP用户名、密码、授权目录和用户级别是必配置项。没有指定FTP授权目录及用户级别而登录失败是常见故障。

1. 执行命令**aaa**，进入AAA视图。
2. 执行命令**local-user** *user-name* **password irreversible-cipher** *password*，配置本地用户名和密码。
3. 执行命令**local-user** *user-name* **ftp-directory** *directory*，配置FTP用户的授权目录。
4. 执行命令**local-user** *user-name* **privilege level** *level*，必须将用户级别配置在3级及3级以上，否则FTP连接将无法成功。

接入类型是可选项。缺省情况下，系统支持所有接入类型。如果配置了其中一项或者几项服务，那么只为该用户提供配置的这几项服务。

执行命令**local-user** *user-name* **service-type ftp**，配置FTP服务类型。

步骤5 检查登录FTP服务器的用户数是否达到上限。

执行命令**display ftp-users**，查看FTP用户数是否达到5个。

步骤6 检查FTP服务器端是否配置了ACL。

执行命令**display** [**ipv6**] **ftp-server**，查看FTP服务器端是否配置了ACL。

如果配置了ACL规则，系统仅允许在ACL规则列表中指定的IP地址登录FTP服务器。

步骤7 检查FTP服务器端是否配置了多种认证模式。

1. 执行命令**aaa**，进入AAA视图。
2. 执行命令**display this**，查看是否配置了多种认证模式。详细信息请参考**AAA配置**。

----结束

8.6.2 上传文件失败

故障原因

- 源路径、目的路径中含有空格等设备不支持的字符。
- 服务器根目录存储空间不足。
- 服务器、客户端由于调整MTU发送的数据帧长度超过了对端所能够承受的最大值，或者是超过了发送路径上途经的某台设备所能够承受的最大值，导致数据帧被丢弃。

操作步骤

步骤1 源路径、目的路径中含有空格等设备不支持的字符。

设备中目录名使用的字符不可以是空格、“~”、“*”、“/”、“\”、“:”、“'”、“"”。

如果路径中含有以上设备不支持的字符，请修改路径。

步骤2 检查服务器根目录存储空间是否不足。

在服务器端执行命令**dir**，查看服务器根目录下的空闲空间。

如果存储空间已满，在用户视图下执行命令**delete /unreserved**删除不需要的文件。

步骤3 检查服务器、客户端接口上配置的MTU是否超过了设备所能承受的最大值。

分别在服务器、客户端的接口视图下执行命令**display this**查看接口当前的MTU值，如果没有显示，则MTU为缺省值1500字节。

如果配置的MTU大小超过了服务器或者客户端所能承受的最大帧长，在该接口视图下执行命令**mtu**减小MTU值。设备所能承受的最大帧长可以参见《FAQ》接口管理 中的“接口MTU和接口允许通过的最大帧长”章节。

----结束

8.7 文件管理 FAQ

8.7.1 如何查看已删除文件

设备提供回收站功能，使用**delete**命令删除的文件保留在回收站中，只有使用**delete / unreserved**命令才能真正删除文件。

使用**dir**命令不显示已经被删除并被放入回收站中的文件，只有使用**dir /all**命令才能显示回收站中的文件，这些文件的文件名被“[]”包含。

8.7.2 设备支持的 SSH 版本号

设备支持的SSH版本号是1.99，即支持SSH1（SSH1.x）协议和SSH2（SSH2.0）协议。

设备做SSH客户端时，只能做SSH服务器端版本为2.0的客户端，不能做SSH服务器端版本为1.x的客户端；设备做SSH服务器端时，允许版本号为1.x和2.0的SSH客户端登录该设备。

8.7.3 为什么 ssh 用户在配置远端认证时必须同时在设备本地配置用户才能通过认证

在设备本地配置用户不是必需操作，当在设备上配置**ssh authentication-type default password**后，无须再在本地配置用户。

8.7.4 当存储设备出现异常时，如何修复

- 如果用户在设备上执行**dir**命令查看设备中的指定文件或目录的信息，当显示信息中含有**unknown**信息时，如: 30,000 KB total (672 KB free, 25,560 KB used, **3,616 KB unknown**)，可以通过在用户视图下执行**fixdisk** *device-name*命令释放**unknown**空间。

  此命令是问题修复类命令，在系统未出现问题时，建议用户不要执行此命令。
- 如果用户在设备上执行**dir**命令查看不到文件，但是存储空间被占用。则可能存在以下情况：

被删除的文件放在回收站中。用户可以执行命令**dir /all**命令显示所有文件信息，包括已经删除的文件信息（用[ ]标识）。此类文件可使用**undelete**命令恢复。若要从回收站中删除该文件，使用**reset recycle-bin**命令。

须知

- 执行**fixdisk** *device-name*命令后，会清空指定存储器中的所有文件和目录，并且不可恢复，请谨慎使用。
- **fixdisk** *device-name*命令无法修复设备级的故障。

8.7.5 如何上传/下载文件

用户可以通过Console口（串口）、FTP、TFTP、SFTP、SCP、FTPS方式，在设备与设备之间或者设备与主机之间传送文件。设备、主机在文件传输的过程中，均可以充当服务器或者客户端的角色。各种文件传输方式的应用场景及优缺点如表8-57所示，用户可以根据需求选择其中一种方式。具体每种传输方式的配置方法请参见相应版本“配置指南-基础配置”中的“文件管理”部分。

表 8-57 文件传输方式

文件传输方式	应用场景	优点	缺点
Console口	通过设备的BootLoad菜单实现，适用于没有网络环境、设备的管理网口损坏或者无法正常登录的场景。	• 只需要使用一根串口线连接主机与设备。 • 传输过程不需要网络环境，可以避免网络带来的不安全因素。	传输速度较慢。
FTP（File Transfer Protocol）	适用于对网络安全性要求不是很高的文件传输场景，广泛用于版本升级等业务中。	• 配置较简单。 • 具有授权和认证功能。	明文传输数据，存在安全隐患。
TFTP（Trivial File Transfer Protocol）	在网络条件良好的实验室局域网中，可以使用TFTP进行版本的在线加载和升级。适用于客户端和服务器之间，不需要复杂交互的环境。	TFTP所占的内存要比FTP小。	TFTP没有授权和认证，且是明文传输数据，存在安全隐患，易于网络病毒传输以及被黑客攻击。
SFTP（Secure File Transfer Protocol）	适用于网络安全性要求高的场景，目前被广泛用于日志下载、配置文件备份等业务中。	数据进行了严格加密和完整性保护，安全性高。	配置较复杂。

文件传输方式	应用场景	优点	缺点
SCP（Secure Copy Protocol）	适用于网络安全性要求高，且文件上传下载效率高的场景。	• 数据进行了严格加密和完整性保护，安全性高。 • 客户端与服务器连接的同时完成文件的上传下载操作（即连接和拷贝操作使用一条命令完成），效率较高。	配置较复杂（与SFTP方式的配置非常类似）。
FTPS（FTP over SSL（Secure Sockets Layer））	适用于网络安全性要求高，且不提供普通FTP功能的场景。	利用数据加密、身份验证和消息完整性验证机制，为基于TCP可靠连接的应用层协议提供安全性保证。	配置较复杂，需要预先从CA处获得一套证书。

说明

- 串口采用的传输协议是XModem协议，用户在传输文件时，注意选择正确的传输协议。
- 对于TFTP方式，设备仅支持作为客户端；对于FTP、SFTP、SCP以及FTPS方式，设备可作为客户端，也可作为服务器。
- 在上传系统文件到设备中时，请保持设备正常供电。否则可能会引起文件损坏或文件系统损坏，从而造成设备存储介质损坏或设备不能正常启动等问题。
- Console口、FTP、TFTP、SFTP、SCP以及FTPS文件传输方式不支持定时从服务器中下载文件。

8.7.6 怎么限制 FTP 上传/下载速度

FTP协议本身没有限速的机制，只能通过在用于FTP客户端/服务器通信的接口上配置接口限速，设置FTP上传或者下载的最高限速。具体请参见相应版本“配置指南-QoS”中的“流量监管、流量整形和接口限速配置”部分。

8.7.7 如何检查文件上传是否完整

用户文件上传完之后，可以通过比较文件上传前后的大小来检查文件上传是否完整。上传文件之前查看并记录文件的大小，文件上传完之后执行**dir**命令查看存储器中文件的大小，比较这两个数值的大小：如果大小一致，说明上传的文件是完整的；如果大小不一致，说明上传的文件不完整，需要执行**delete**命令删除不完整文件，重新上传。

```
<HUAWEI> dir /all
Directory of flash:/

 Idx  Attr     Size(Byte)  Date        Time       FileName
   0  -rw-             14  Feb 27 2012 11:20:12   back_time_a
   1  -rw-             16  Dec 28 2011 13:10:56   abc.tbl
   2  drw-              -  Feb 25 2012 14:19:56   logfile
   3  drw-              -  Oct 31 2011 15:05:26   sysdrv
   4  drw-              -  Feb 25 2012 14:20:08   compatible
   5  drw-              -  Oct 31 2011 15:19:02   selftest
```



```
  6  -rw-           14  Feb 27 2012 11:20:12   back_time_b
  7  -rw-        9,637  Feb 25 2012 14:18:22   vrpcfg.cfg
  8  -rw-            4  Jan 18 2012 16:34:56   snmpnotilog.txt
  9  -rw-        1,968  Feb 25 2012 14:20:22   private-data.txt
 10  -rw-          637  Nov 04 2011 11:48:46   cacert.der
 11  -rw-        4,303  Feb 09 2012 21:16:06   vrpcfg1.cfg.bak
 12  -rw-          639  Nov 04 2011 11:49:04   rootcert.der
 13  drw-            -  Nov 04 2011 11:50:24   security
 14  -rw-           13  Nov 29 2011 20:33:40   tftp_test.txt
 15  -rw-   52,770,448  Dec 05 2011 17:00:06   basicsoft.cc
 16  -rw-   98,139,547  Jan 31 2012 16:11:52   devicesoft.cc
 17  -rw-      463,309  Jan 31 2012 15:55:40   rbsaveddata.txt

509,256 KB total (272,952 KB free)
```

回显信息中的**Size(Byte)**即为文件的大小。

8.7.8 各类型文件的后缀名是什么

各类型文件的后缀名如表8-58所示。

表 8-58 各类型文件的后缀名

文件类型	后缀名
web网页文件	.7z
license文件	.dat
配置文件	.cfg或者.zip
系统文件	.cc
补丁文件	.pat

8.7.9 日志文件存放在哪里

交换机将日志文件保存在主交换机flash的**syslogfile**或**logfile**文件夹下。

```
<HUAWEI>dir            //显示flash目录下的所有文件和文件夹
Directory of flash:/

  Idx  Attr     Size(Byte)  Date        Time       FileName
    0  -rw-         1,766  Dec 24 2040 03:37:54   private-data.txt
    3  drw-             -  Dec 24 2040 03:40:12   syslogfile
    4  drw-             -  Dec 24 2040 03:37:58   compatible
   16  -rw-        10,571  Jan 04 2041 03:51:18   elabel-slot0.fls
......
<HUAWEI>cd logfile          //进入logfile文件夹
<HUAWEI>dir
Directory of flash:/logfile/

  Idx  Attr     Size(Byte)  Date        Time       FileName
    0  -rw-         10,824  Jan 24 2042 09:15:04   logfile-2042-01-24-09-15-03.zip
    1  -rw-         15,334  Feb 03 2042 14:45:08   logfile-2042-02-03-14-45-08.zip
```

8.7.10 如何删除文件

执行**delete** [**/unreserved**] [**/quiet**] { *filename* | *devicename* } [**all**]命令可以删除存储器中的指定文件，包括系统文件、配置文件、paf、license、日志文件等。

- 删除存储器中的文件。

```
<HUAWEI> delete test.txt
Delete flash:/test.txt?[Y/N]:y
Info: Deleting file flash:/test.txt...succeeded.
```

  说明

  - 以上显示信息请以设备实际显示为准。
  - 参数**all**仅在设备堆叠情况下支持该参数。指定参数**all**可以批量删除所有成员设备上对应路径下的文件。
  - 不能在命令行界面删除设备当前正在使用的版本文件（包括系统软件、补丁文件、Web网页文件和配置文件等）。

- 日志文件保存在Flash的**logfile**或**syslogfile**目录下。用户可以切换到**logfile**或**syslogfile**目录下删除日志文件，也可以在Flash下使用绝对路径删除日志文件。

  # 切换到**logfile**目录下删除日志文件。

```
<HUAWEI> cd logfile/
<HUAWEI> delete logfile-2013-01-24-09-15-03.zip
Delete flash:/logfile/logfile-2013-01-24-09-15-03.zip?[Y/N]:y
Info: Deleting file flash:/logfile/logfile-2013-01-24-09-15-03.zip...succeeded.
```

  # 在Flash下使用绝对路径删除日志文件。

```
<HUAWEI> delete flash:/logfile/logfile-2013-01-24-09-15-03.zip
Delete flash:/logfile/logfile-2013-01-24-09-15-03.zip?[Y/N]:y
Info: Deleting file flash:/logfile/logfile-2013-01-24-09-15-03.zip...succeeded.
```

8.7.11 怎么在两台设备之间传送文件

如果需要在两台设备之间传送文件，例如补丁文件、配置文件等，可以将一台设备作为服务器，另一台设备作为客户端，使用FTP、TFTP、SFTP、SCP和FTPS方式在服务器设备和客户端设备之间上传或者下载文件，具体请参见相应版本“配置指南-基础配置”中的“文件管理”部分。

9 配置系统启动

9.1 系统启动简介
9.2 管理配置文件
9.3 恢复出厂配置
9.4 配置系统启动文件
9.5 重新启动设备
9.6 配置系统启动的配置举例

9.1 系统启动简介

系统启动的场景一般有以下几种：

- 对设备进行升级操作，即系统软件从低版本至高版本升级。

  当增加了新特性或者需要对原有性能进行优化以及解决当前运行版本的问题时，则需要对设备进行升级。此时需要加载高版本的系统软件，并重新启动设备来实现。
- 对设备进行降级操作（版本回退），即系统软件从高版本至低版本降级。

  设备完成升级后，如果业务出现异常，为保证业务正常可以先将设备版本进行回退。此时需要加载低版本的系统软件，并重新启动设备来实现。
- 在开局场景下，可以对一个新设备加载已有的满足用户需求的配置文件。

  新设备中只包含了设备出厂时的缺省配置，如果需要使这台新设备连接至网络再运行业务，则需要用户在设备上进行大量的配置，花费不少时间。对于这种情况，只需要为这台新设备指定满足用户需求的配置文件，然后重新启动设备即可，极大提升了用户对设备的配置效率。
- 对设备指定升级后的补丁文件。

  可以在设备升级的同时指定之前未安装过的补丁文件，当设备升级完成后，补丁也会立即生效。

说明

- 设备的升级与每次发布的版本相关，在发布新版本的同时会配套发布相应的升级指导书，用户可以根据升级指导书进行设备升级。升级指导书获取路径：请先登录华为公司企业业务支持网站（**http://support.huawei.com/enterprise**），登录后，根据产品型号和版本名称，获取相应的升级指导书。
- 设备升级的命令请参见“设备升级命令”。

安全启动

通信设备的本质是由多个嵌入式计算机系统组成，其软件有可能被病毒入侵，也可能被攻击者通过漏洞等方式进行程序篡改、木马植入。一旦系统被攻击者入侵后，通过修改配置、截取报文等方法，就可以实现数据的窃取与窃听。

安全启动是基于一个信任链的传递机制，即从一个初始的信任根出发，在每一次转换计算环境时，信任状态以传递方式保持下去，保证其计算环境是可信的。系统启动时，从安全启动平台信任根出发，按照BIOS、OS Kernel、应用程序的启动顺序，每一级负责度量下一级的boot阶段，建立完整的信任链，从而实现信任链的建立与传递。

系统软件

设备的软件包括BootROM/BootLoad软件和系统软件。设备上电后，先运行BootROM/BootLoad软件，初始化硬件并显示设备的硬件参数，然后运行系统软件。系统软件一方面提供对硬件的驱动和适配功能，另一方面实现了业务特性。BootROM/BootLoad软件与系统软件是设备启动、运行的必备软件，为整个设备提供支撑、管理、业务等功能。

设备在升级时包括升级BootROM/BootLoad软件和升级系统软件。

目前设备的系统软件（.cc）中已经包含了BootROM/BootLoad软件，在升级系统软件的同时即可自动升级BootROM/BootLoad。

配置文件

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

配置文件为文本文件，其规则如下：

- 以命令格式保存。
- 为了节省空间，只保存非缺省的参数。
- 以命令视图为基本框架，同一命令视图的命令组织在一起，形成一节，节与节之间通常用空行或注释行隔开（以“#”开始的为注释行）。空行或注释行可以是一行或多行。
- 文件中各节的顺序安排通常为：全局配置、接口配置、各种协议配置和用户界面配置。
- 配置文件必须以“.cfg”或“.zip”作为扩展名，而且必须存放在存储设备的根目录下。
  - “.cfg”为纯文本格式，可直接查看其内容。指定为配置文件后，启动时系统对里面的命令逐条进行恢复。
  - “.zip”是“.cfg”的压缩格式，占用空间较小。指定为配置文件后，启动时先解压成“.cfg”格式，然后逐条恢复。

- 配置文件中，命令表达式必须是全写，请勿使用缩写。
- 配置文件中，每行命令使用“\r\n”换行，禁止使用其他形式不可见字符换行。
- 配置文件传输至设备时，推荐使用FTP的binary模式。

设备运行过程中，有出厂配置、配置文件和当前配置，区别如下表：

概念	描述	查看方式
出厂配置	设备在出厂时，通常会被安装一些基本的配置，称为出厂配置。出厂配置用来保证设备在没有配置文件或者配置文件丢失、损坏的情况下，能够正常启动、运行。	-
配置文件	设备上电时，从默认存储路径中读取配置文件进行设备的初始化操作，因此该配置文件中的配置称为初始配置。如果默认存储路径中没有配置文件，则设备用缺省参数初始化配置。	• 使用**display startup**命令可以查看到设备本次以及下次启动的配置文件。 • 使用**display saved-configuration**命令可以查看设备下次启动时的配置文件信息。
当前配置	与初始配置相对应，设备运行过程中正在生效的配置称为当前配置。	使用**display current-configuration**命令查看设备的当前配置信息。

用户通过命令行接口可以修改设备当前配置，为了使当前配置能够作为设备下次启动时的起始配置，需要使用**save**命令保存当前配置到默认存储器中，形成配置文件。

说明

配置文件支持包含30000条命令行。如果超过了30000条，在设备进行升级时，不能保证所有命令在升级后兼容。

如果使用不完整格式进行配置，由于命令保存到配置文件中时使用的是完整格式，可能导致配置文件中存在长度超过510个字符的命令（系统可正确执行的命令长度最大为510个字符）。系统重启时，这类命令将无法恢复。

证书文件

证书文件是一个包含用户者公钥和相关身份信息的文件。设备从传统模式切换成NETCONF模式，以及从控制器获取地址时，需要用到证书文件。

当前版本设备启动时所需的证书文件有**device.pem**、**default_ca.cer**、**root.cer**、**default_local.cer**、**ca_config.ini**和**private-data.txt**。这些文件属于系统文件，不能通过命令行删除，若从BootLoad菜单中强制删除，会导致设备注册控制器失败。

补丁文件

补丁是一种与设备系统软件兼容的软件，用于解决设备系统软件少量且急需解决的问题。在设备的运行过程中，有时需要对设备系统软件进行一些适应性和排错性的修改，如改正系统中存在的缺陷、优化某功能以适应业务需求等。

补丁通常以补丁文件的形式发布，一个补丁文件可能包含一个或多个补丁，不同的补丁具有不同的功能。当补丁文件被用户从存储器加载到内存补丁区中时，补丁文件中的补丁将被分配一个在此内存补丁区中唯一的单元序号，用于标志、管理和操作各补丁。

补丁分类

根据补丁生效对业务运行的影响，补丁分成热补丁和冷补丁：

- 热补丁HP（Hot Patch）：补丁生效不中断业务，不影响业务运行，同时可以降低设备升级成本，避免升级风险。
- 冷补丁CP（Cold Patch）：要使补丁生效需要重启设备，影响业务的运行。

根据补丁间的依赖关系，补丁可分为增量型补丁和非增量型补丁。

- 增量型补丁：是指对在其前面的补丁有依赖性的补丁。一个新的补丁文件必须包含前一个补丁文件中的所有补丁信息。用户可以在不卸载原补丁文件的情况下直接安装新的补丁文件。
- 非增量型补丁：只允许当前系统安装一个补丁文件。如果用户安装完补丁之后希望重新安装另一个补丁文件，则需要先卸载当前的补丁文件，然后再重新安装并运行新的补丁文件。

说明

目前，产品发布的补丁类型都为热补丁与增量型补丁。在后续的描述中如无特别说明都是指此类补丁。

补丁状态

每个补丁都有自身的状态，只有在用户命令行的干预下才能发生切换。

补丁状态详细信息如表9-1所示。

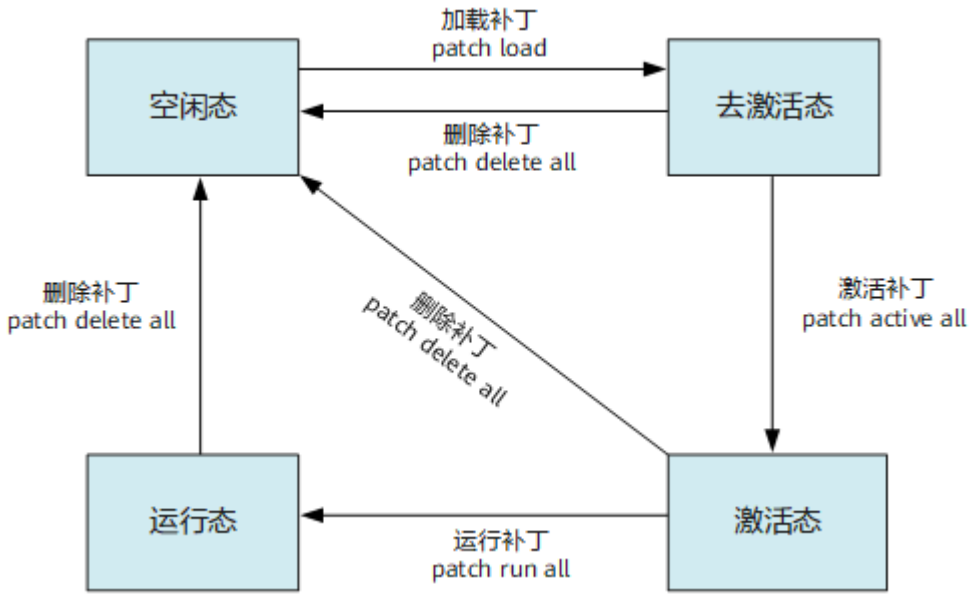
表 9-1 补丁状态

状态	说明	各状态之间的转换关系
空闲态（Idle）	补丁文件存储在设备的存储器中，但没有被加载到内存补丁区时，补丁处于空闲状态。	当用户将补丁从存储器中加载到内存补丁区后，补丁的状态将被设置为去激活。
去激活（Deactive）	当补丁被加载到内存补丁区时，补丁处于去激活状态。	用户可以对去激活状态的补丁进行以下两种操作： • 卸载此补丁，使补丁从内存补丁区中被删除。 • 临时运行此补丁，使补丁的状态变为激活状态。
激活（Active）	当处于去激活状态的补丁被临时运行时，补丁处于激活状态。 当重启设备后，重启前处于激活状态的补丁将会处于去激活状态。	用户可以对激活状态的补丁进行以下两种操作： • 卸载此补丁，使补丁从内存补丁区中被删除。 • 永久运行此补丁，使补丁的状态变为运行状态。

状态	说明	各状态之间的转换关系
运行（Running）	当处于激活状态的补丁被永久运行时，补丁处于运行状态。 当重启设备后，重启前处于运行状态的补丁将保持运行状态。	用户可以卸载处于运行状态的补丁，使补丁从内存补丁区中被删除。

各状态之间的转换关系如图9-1所示。

图 9-1 补丁状态的转换关系



补丁安装

为设备安装补丁也是设备升级的一种方式。补丁安装方式有以下两种：

- 一般均采用不中断业务的方式，在设备运行过程中直接加载运行补丁，这也是热补丁的优势。

  这种安装方式的详细过程请参见随补丁版本同时配套发布的补丁安装指导书，用户可以根据补丁安装指导书进行补丁安装。相应的命令请参见“设备升级命令”。
- 另外一种方式就是本章介绍的指定系统下次启动的补丁文件，这种方式需要设备重启之后补丁才能生效。一般用于设备升级的同时安装补丁文件。

9.2 管理配置文件

前置任务

在进行配置之前，需完成以下任务：

- 用户成功登录设备。

配置流程

以下配置任务，根据需求选择其中一项或几项进行配置。

9.2.1 保存配置文件

背景信息

用户通过命令行可以修改设备的当前配置，而这些配置是暂时的，如果要使当前配置在系统下次重启时仍然有效，在重启设备前，需要将当前配置保存到配置文件中。可以通过以下两种方法保存配置文件：

- 自动保存配置。
- 手动保存配置。

说明

设备在保存配置文件时，不允许其他用户进行配置。同样，如果当前用户正在进行配置，其他用户也不允许进行保存配置操作。

操作步骤

- 自动保存配置。
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**set save-configuration** [**interval** *interval* | **cpu-limit** *cpu-usage* | **delay** *delay-interval*] *，配置系统定时保存配置。

     缺省情况下，系统不启动定时保存配置的功能。

     系统在定时保存配置文件之前，会查看配置文件情况，发生如下情况会触发定时保存：

     - 配置文件与上次保存的不同。
     - 配置文件与上次保存的相同，但是期间有过改动。例如执行了某条命令后，又删除了该命令，配置文件虽然与之前相同，但是也会触发定时保存。

     当出现如下情况时，系统会取消定时保存配置文件的操作：

     - 当前存在写配置文件操作。
     - 设备正在进行配置恢复。
     - CPU利用率较高。
  c. （可选）执行命令**set save-configuration backup-to-server server** *server-ip* [**vpn-instance** *vpn-instance-name*] **transport-type** { **ftp** | **sftp** } [**port** *port-number*] **user** *user-name* **password** *password* [**path** *path*]或**set save-configuration backup-to-server server** *server-ip* [**vpn-instance** *vpn-instance-name*] **transport-type tftp** [**path** *path*]，配置服务器的相关信息，包括自动保存配置文件的服务器的IP地址、用户名及其密码、端口号、配置文件自动保存的目的路径和配置文件自动保存至服务器的传输方式。

说明

使用TFTP传输方式保存配置文件时，可执行命令**tftp client-source**配置设备的Loopback接口作为客户端源地址。

建议使用安全性更高的SFTP协议保存配置文件至文件服务器。

- 手动保存配置。
  - 执行命令**save** [**all**] [**force**] [*configuration-file*]，保存当前配置。

    将当前配置保存到指定文件时，文件必须以“.zip”或“.cfg”作为扩展名。而且系统启动配置文件必须存放在存储设备的根目录下。

    - 在第一次保存配置文件时，如果不指定可选参数*configuration-file*，则设备将提示是否将文件名保存为“vrpcfg.zip”。“vrpcfg.zip”是系统缺省的配置文件，初始状态是空配置。
    - 如果不指定*configuration-file*参数，则配置信息将保存至系统当前启动配置文件里，执行**display startup**命令可以查看系统当前启动配置文件的文件名。
    - 执行**pwd（用户视图）**命令，可以查看系统当前存储路径。
    - 执行**cd（用户视图）**命令，可以更改系统当前存储路径。

----结束

9.2.2 比较配置文件

背景信息

用户可以通过比较当前配置（包含离线配置）和下次启动的配置文件，查看哪些配置项是不一致的，决定是否需要将当前配置设置为下次启动时加载的配置文件。

系统在比较出不同之处时，将从两者有差异的地方开始显示字符（默认显示150个字符），如果该不同之处到文件末尾不足150个字符，将显示到文件尾为止。

比较当前配置（包含离线配置）和下次启动的配置文件时，如果下次启动的配置文件为空，或者下次启动的配置文件存在，但是内容为空，系统将提示读文件失败。

说明

所比较的配置文件必须以“.cfg”或“.zip”作为扩展名。

操作步骤

- 执行命令**compare configuration** [*configuration-file*] [*current-line-number save-line-number*]，比较当前的配置（包含离线配置）与下次启动的配置文件或者指定的配置文件的内容是否一致。

  如果不输入参数，表示从配置文件的首行开始进行比较。*current-line-number*和*save-line-number*这两个参数用来在发现配置文件不同之处后，跳过该不同处继续进行比较。

----结束

9.2.3 备份配置文件

背景信息

为防止设备意外损坏，导致配置文件无法恢复，可以通过以下五种方法进行备份配置文件：

- 直接屏幕拷贝。
- 备份配置文件到存储器中。
- 通过FTP、TFTP、FTPS、SFTP和SCP备份配置文件。
- 通过执行命令行进行备份。
- 通过执行命令行实时备份当前配置。

操作步骤

- 直接屏幕拷贝

  在命令行界面上，执行**display current-configuration**命令，并拷贝所有显示信息到TXT文本文件中，从而将配置文件备份到维护终端的硬盘中。

  说明

  屏幕上显示的配置信息受终端软件的影响，可能会出现某配置过长而换行的情况。对于换行的配置，拷贝至TXT文本中时，需要删除换行，保证一条配置信息在只处在一行中。否则当使用制作的TXT文本恢复配置时，换行的配置将无法恢复。

- 备份配置文件到flash中

  该步骤主要便于用户在设备的flash中及时备份当前配置文件。在设备启动之后，使用如下命令在设备的flash中备份配置文件。

  ```
  <HUAWEI> save config.cfg
  <HUAWEI> copy config.cfg backup.cfg
  ```

- 通过FTP、TFTP、FTPS、SFTP和SCP备份配置文件

  设备支持通过FTP、TFTP、FTPS、SFTP和SCP备份配置文件。其中使用FTP和TFTP备份配置文件比较简单，但是存在安全风险。在安全要求比较高的场景中，建议使用FTPS、SFTP和SCP备份配置文件。以下仅以FTP作为示例介绍备份配置文件。关于TFTP、FTPS、SFTP和SCP的使用，请参见**8 文件管理**。

  a. 设备作为FTP服务器，启动FTP服务。

     在设备上启动FTP服务器功能，并创建用户名为**huawei**，密码为**Helloworld@6789**的FTP用户，授权此用户可访问的目录是“flash:”。

     ```
     <HUAWEI> system-view
     [HUAWEI] ftp server enable
     Warning: FTP is not a secure protocol, and it is recommended to use SFTP.
     Info: Succeeded in starting the FTP server.
     [HUAWEI] aaa
     [HUAWEI-aaa] local-user huawei password irreversible-cipher Helloworld@6789
     [HUAWEI-aaa] local-user huawei ftp-directory flash:
     [HUAWEI-aaa] local-user huawei service-type ftp
     [HUAWEI-aaa] local-user huawei privilege level 15
     ```

  b. 从维护终端向设备发起FTP连接。

     在PC上，通过FTP客户端与设备建立FTP连接（例如设备的IP地址是10.110.24.254）。

```
C:\Documents and Setting\Administrator> ftp 10.110.24.254
Connected to 10.110.24.254.
220 FTP service ready.
User (10.110.24.254:(none)): huawei
331 Password required for huawei.
Password:
230 User logged in.
```

c. 设置传输参数。

FTP用户验证通过后，FTP客户端显示提示符“ftp>”，在“ftp>”提示下键入**binary**（二进制传输模式），并设置FTP客户端存放上载文件的目录路径。

```
ftp> binary
200 Type set to I.
ftp> lcd c:\temp
Local directory now C:\temp.
```

d. 传输配置文件。

在PC上，使用**get**命令将配置文件下载至本地指定目录中，并保存为backup.cfg。

```
ftp> get config.cfg backup.cfg
```

e. 确认config.cfg和backup.cfg的文件大小是否一致。如果文件大小一致则认为备份成功。

- 通过执行命令行进行备份

执行命令**configuration copy startup to file** *file-name*，将设备的启动配置文件备份到指定的文件中。

指定的目的文件必须以“.cfg”或“.zip”作为扩展名，且后缀必须与被备份文件的后缀一致。

当存在同名文件时，系统会提示是否覆盖。输入“Y”进行覆盖，输入“N”不进行覆盖。

- 通过执行命令行实时备份当前配置

在系统视图下执行命令**undo configuration backup local disable**，使能设备备份当前运行配置的功能。当配置发生变化2小时后，设备将自动备份当前的运行配置到本地。

缺省情况下，备份运行配置到本地的功能处于打开状态。如果需要设置为去使能，执行命令**configuration backup local disable**。

----结束

9.2.4 恢复配置文件

背景信息

用户进行了错误的配置，导致功能异常，可以通过以下两种方法进行配置文件恢复：

- 从存储器恢复配置文件。
- 通过FTP、TFTP、FTPS、SFTP和SCP恢复配置文件。

说明

在恢复配置文件后，为了让配置文件生效，需要重新启动设备。先使用**startup saved-configuration**命令指定重新启动使用的配置文件（如果配置文件命名没有变，则该步骤省略），然后使用**reboot**命令重新启动设备。

操作步骤

- 从存储器恢复配置文件

  该步骤主要便于用户将存储在设备flash中的备份配置文件恢复成当前系统运行的配置文件。在设备正常工作时，使用如下命令。

  ```
  <HUAWEI> copy flash:/backup.cfg flash:/config.cfg
  ```

- 通过FTP、TFTP、FTPS、SFTP和SCP恢复配置文件

  设备支持通过FTP、TFTP、FTPS、SFTP和SCP恢复配置文件。其中使用FTP和TFTP恢复配置文件比较简单，但是存在安全风险。在安全要求比较高的场景中，建议使用FTPS、SFTP和SCP恢复配置文件。以下仅以FTP作为示例介绍恢复备份在PC上的配置文件。关于TFTP、FTPS、SFTP和SCP的使用，请参见**8 文件管理**。

  a. 设备作为FTP服务器，启动FTP服务。

     在设备上启动FTP服务器功能，并创建用户名为**huawei**，密码为**Helloworld@6789**的FTP用户，授权此用户可访问的目录是“flash:”。

     ```
     <HUAWEI> system-view
     [HUAWEI] ftp server enable
     Warning: FTP is not a secure protocol, and it is recommended to use SFTP.
     Info: Succeeded in starting the FTP server.
     [HUAWEI] aaa
     [HUAWEI-aaa] local-user huawei password irreversible-cipher Helloworld@6789
     [HUAWEI-aaa] local-user huawei ftp-directory flash:
     [HUAWEI-aaa] local-user huawei service-type ftp
     [HUAWEI-aaa] local-user huawei privilege level 15
     ```

  b. 从维护终端向设备发起FTP连接。

     在PC上，通过FTP客户端与设备建立FTP连接（例如设备的IP地址是10.110.24.254）。

     ```
     C:\Documents and Setting\Administrator> ftp 10.110.24.254
     Connected to 10.110.24.254.
     220 FTP service ready.
     User (10.110.24.254:(none)): huawei
     331 Password required for huawei.
     Password:
     230 User logged in.
     ```

  c. 设置传输参数。

     FTP用户验证通过后，FTP客户端显示提示符“ftp>”，在“ftp>”提示下键入**binary**（二进制传输模式），并设置FTP客户端存放上载文件的目录路径。

     ```
     ftp> binary
     200 Type set to I.
     ftp> lcd c:\temp
     Local directory now C:\temp.
     ```

  d. 传输配置文件。

     在PC上，使用**put**命令将配置文件上传至本地指定目录中，并保存为backup.cfg。

     ```
     ftp> put config.cfg backup.cfg
     ```

  e. 在设备上确认上传的backup.cfg文件是否成功。如果设备上存在backup.cfg文件，且文件大小正确则认为恢复配置文件成功。

----结束

9.2.5 执行配置文件

操作步骤

- 执行命令**configuration copy file** *file-name* **to running**，执行指定配置文件中的命令。

  如需要运行已存在的配置文件时，可执行该命令。通过该命令可以一次性将指定配置文件中的命令全部执行。

  本命令同时只允许一个用户执行。

  该命令执行过程中，如果发生配置恢复、批量备份操作，则命令执行终止。

  该命令执行过程中，如果某条命令执行失败，则跳过继续执行下一条命令。

----结束

9.2.6 清除配置

背景信息

用户可以根据不同的场景，选择不同的方式清除配置：

- 清除配置文件内容：当设备软件升级后原配置文件与当前软件不匹配，配置文件遭到破坏，或者加载了错误的配置文件时，用户可以清空原有的配置文件，然后再重新指定一个配置文件。
- 一键式清除接口下的配置信息：当用户需要将设备上的某个接口用作其他用途时，原始的配置需要逐条删除。如果该接口下存在大量的配置，那么用户将耗费大量的时间进行删除动作，增大了用户的维护量。为了减少用户的维护量和降低操作的复杂度，可以一键式清除接口下的配置。
- 清除设备上的非激活配置信息：当设备上的插卡不在位时，插卡上原来的配置会保留在交换机上；当堆叠环境中的备/从交换机不在位时，这些交换机上的配置会保留在主交换机上。这些无效的配置均叫做非激活配置，也叫做离线配置。用户可以执行命令行清除设备上所有的非激活配置信息，增加设备的可用空间。

须知

配置清除后不可恢复，请谨慎操作，建议在技术支持人员指导下使用。

操作步骤

- 清除配置文件内容

  执行命令**reset saved-configuration**，清空设备下次启动使用的配置文件的内容，并取消指定系统下次启动时使用的配置文件，从而使设备配置恢复到缺省值。

说明

- 执行该命令后，如果当前启动配置文件与下次启动配置文件相同，当前启动的配置文件也会被清空。
- 执行该命令后，用户手动重启设备时，系统会提示用户是否保存配置，这时候选择不保存才能清空配置。
- 取消指定系统下次启动时使用的配置文件后，如果不使用**startup saved-configuration**命令重新指定新的配置文件，或者不保存配置文件，设备重启后，将会以缺省配置启动。
- 如果当前启动配置文件为空，下次启动配置文件不为空，执行该命令后，则正常清除下次启动配置文件的设置。
- 如果下次启动配置文件为空，当前启动配置文件不为空，执行该命令后，系统将提示错误，并且不做任何清除操作。

- 一键式清除指定接口下配置信息或将配置恢复到缺省值

  具体操作请参见表9-2。

  表 9-2 一键式清除指定接口下配置信息或将配置恢复到缺省值

视图	操作	说明	注意事项
系统视图	**clear configuration interface** { *interface-type-start interface-number-start* [**to** *interface-type-end interface-number-end*] } &<1-10>	选择该操作将清除指定接口下配置信息或将配置恢复到缺省值，命令需要在系统视图下执行，并记住需要清除的接口类型和编号，否则会导致其他接口配置可能被清除，从而导致业务中断。	无论是在系统视图下还是在接口视图下执行命令清除指定接口下配置信息或将配置恢复到缺省值，使用时请慎重。被清除配置文件的接口将被置为shutdown状态。
接口视图	**clear configuration this**	选择该操作将清除当前接口下配置信息或将配置恢复到缺省值，用户直接在接口视图下执行该操作，简化用户操作。 **说明** 该命令不支持在Tunnel和stack-port类型接口下执行。	

- 清除设备的非激活配置信息
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**clear inactive-configuration all**，清除设备的非激活配置信息。

----结束

9.3 恢复出厂配置

用户可以根据不同的场景将配置文件或设备恢复至出厂配置状态。

长按 PNP 键，配置文件恢复出厂配置状态

用户长按PNP键（6秒以上），设备恢复默认配置并自动重新启动。

说明

- 仅S2720-EI、S5720-LI、S5720S-LI、S5720I-SI、S5735S-H、S5736-S、S5731-S、S5731S-S、S5731-H、S5731-H-K、S5731S-H、S5732-H、S5732-H-K、S2730S-S、S5735-L-I、S5735-L1、S300、S5735-L、S5735S-L1、S5735S-L、S5735S-L-M、S500、S5735-S、S5735-S24T4X-I、S5735S-S、S6720S-S、S6730-H、S6730-H-K、S6730-S、S6730S-H和S6730S-S支持此操作。
- 此操作会开启Console口登录功能。
- 此操作清除业务配置和数据文件与**reset factory-configuration**命令功能一致。
- 此操作不会删除protected目录和protected/$_default.cfg文件。
- 如果存在protected/$_default.cfg文件，执行此操作会将$_default.cfg文件设置为下次启动的配置文件；如果没有，则下次启动的配置文件为空。
- 如果不希望任何人使用PNP按钮重置交换机配置时，可以执行**pnp-button disable**命令关闭设备的PNP按钮功能。
- 对于使用专用线缆组建堆叠的设备，须先拔下一端设备的线缆，否则设备重启后会自动重新组建堆叠。
- 在堆叠环境中，缺省情况下，堆叠中的任意设备长按PNP键，会使得单机恢复默认配置并自动重新启动。当用户希望清除整台堆叠设备的业务配置和数据文件时，可以执行**pnp-button mode reset-system**命令配置长按PNP按钮后的设备行为。

设备一键恢复出厂配置状态

当用户希望清除所有的业务配置和数据文件时，可以通过执行命令，一键式将设备还原至出厂配置状态。

1. 在用户视图下，执行命令**reset factory-configuration**，设备重新启动，并恢复至出厂配置状态。

   须知

   该命令不仅会将系统配置文件恢复至出厂配置状态，还会清除设备上的业务配置和数据文件，请谨慎使用。

2. 在用户视图下，执行命令**display factory-configuration reset-result**，查看设备最近一次恢复出厂配置的结果。

9.4 配置系统启动文件

前置任务

在配置系统启动文件之前，需完成以下任务：

- 设备运行正常，用户可以本地或远程登录设备。
- 设备启动时所需的系统启动文件已保存至设备的根目录。

背景信息

在进行配置前，用户可以使用**display startup**命令查看当前设备指定的下次启动时加载的文件。

- 如果没有配置设备下次启动时加载的系统软件，则下次启动时将默认启动此次加载的系统软件。当需要更改下次启动的系统文件（如设备升级）时，则需要指定下次启动时加载的系统软件，此时还需要提前将系统软件通过文件传输方式保存至设备，系统软件必须存放在存储器的根目录下，文件名必须以“.cc”作为扩展名。
- 设置设备下一次启动的系统软件时，设备会对系统软件的完整性进行校验。如果系统软件的数字签名不合法，设置将会失败。请确保系统软件来源的合法性。
- 如果没有配置下次启动时加载的配置文件，则下次启动采用缺省配置文件（如vrpcfg.zip）。如果默认存储器中没有配置文件，则设备启动时将使用缺省参数初始化。配置文件的文件名必须以“.cfg”或“.zip”作为扩展名，而且必须存放在存储器的根目录下。
- 补丁文件的扩展名为“.pat”，在指定下次启动时加载的补丁文件前也需要提前将补丁文件保存至设备存储器的根目录下。
- 用户请勿自行手动修改配置文件，并指定为下次启动时的配置文件，否则可能会造成设备启动异常。

  说明

  S5735S-H、S5736-S、S5731-H-K、S5731-H、S5731-S、S5731S-H、S5731S-S、S5732-H、S5732-H-K、S6720S-S、S6730-H-K、S6730-H、S6730S-H、S6730-S和S6730S-S支持安全FLASH启动。

操作步骤

- （可选）执行命令**check file-integrity** *filename signature-filename*对系统软件合法性进行校验。

  说明

  需要先将系统软件和对应的签名文件上传至设备才可以使用此命令进行校验。

- 执行命令**startup system-software** *system-file*，配置设备下次启动时加载的系统软件。

  说明

- 执行命令**startup saved-configuration** *configuration-file*，指定系统下次启动时使用的配置文件。

  设备上电时，默认从存储器根目录中读取配置文件进行初始化。

- （可选）执行命令**startup patch** *patch-name* [**slave-board** | **slot** *slot-id*]，指定设备下次启动时加载的补丁文件。

  如果用户希望设备重新启动后加载运行补丁文件，并使之生效，则可以执行本命令指定下次启用的补丁文件。

----结束

检查配置结果

配置完系统启动文件后，可使用**display startup**命令查看系统下次启动相关的系统软件、配置文件以及补丁文件。

9.5 重新启动设备

前置任务

在重新启动设备之前，需完成以下任务：

- 配置系统启动文件。

背景信息

重新启动设备有以下两种方式：

- 立即重新启动设备：执行命令行后立即重新启动。
- 定时重新启动设备：可以设置在未来的某一时刻重新启动设备。配置完下次系统启动文件后，为了不影响当前设备的运行，可以将设备设置在业务量少的时间点进行定时重新启动。

设备重新启动的相关信息会被记录下来，通过**display reboot-info**命令进行查看。执行**reset reboot-info**命令可清除这些信息。

须知

- 一般情况下，不要轻易重新启动设备，因为这将导致在短时间内服务中断。
- 在重新启动设备之前，如果需要将当前配置在重新启动设备后仍生效，请先确保当前配置已保存。

操作步骤

- 立即重新启动设备

  在用户视图下，执行命令**reboot** [**fast** | **save diagnostic-information**]，实现对设备的重新启动。

  - 指定**fast**，表示快速重启设备，不会提示是否保存配置文件。
  - 指定**save diagnostic-information**，表示系统在重新启动前会将诊断信息保存到设备存储器的根目录下。

- 定时重新启动设备

  在用户视图下，执行命令**schedule reboot** { **at** *time* | **delay** *interval* [**force**] }，使能定时重新启动功能。

  - **at** *time*：设置设备定时重新启动的具体时间。
  - **delay** *interval* [**force**]：设置设备在定时重新启动前等待的时间。

    如果不指定**force**参数，系统首先会将当前配置与配置文件进行比较，如果不一致，则会提示是否保存当前配置，用户进行选择后系统又将提示用户确认设置的定时重启时间，键入“Y”或者“y”后，设置生效。如果指定**force**参数，则系统不会出现任何提示，设置生效，当前配置不会被比较及保存。

----结束

检查配置结果

- 如果配置了定时重启功能，可以执行**display schedule reboot**命令查看设备定时重启的相关配置。

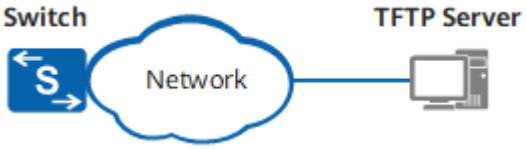
9.6 配置系统启动的配置举例

9.6.1 备份配置文件示例

组网需求

如图9-2所示，用户登录设备，为防止设备意外损坏，导致配置文件无法恢复，将配置文件备份至TFTP服务器上。

图 9-2 备份配置文件组网图



配置思路

采用如下的思路进行配置：

1. 保存配置文件。
2. 通过TFTP备份配置文件。

须知

使用TFTP备份配置文件比较简单，但是存在安全风险。在安全要求比较高的场景中，建议使用FTPS、SFTP和SCP备份配置文件。以下仅以TFTP作为示例介绍备份配置文件。

操作步骤

步骤1 保存配置到config.cfg文件

```
<HUAWEI> save config.cfg
```

步骤2 通过TFTP备份配置文件

1. 启动TFTP服务器程序。

   在PC上启动TFTP服务器应用程序，设置好配置文件的传输路径、TFTP服务器IP地址、端口号。

2. 传输配置文件。

   在用户视图下执行**tftp**命令，用来备份指定的配置文件。

```
<HUAWEI> tftp 10.110.24.254 put flash:/config.cfg backup.cfg
```

----结束

9.6.2 恢复配置文件示例

组网需求

如图9-3所示，用户登录设备，当用户进行了错误的配置，导致功能异常的时候，将TFTP服务器上保存的配置文件下载到设备并设置为下次启动配置文件。

图 9-3 恢复配置文件组网图

配置思路

采用如下的思路进行配置：

1. 通过TFTP恢复备份在PC上的配置文件。

须知

使用TFTP恢复配置文件比较简单，但是存在安全风险。在安全要求比较高的场景中，建议使用FTPS、SFTP和SCP恢复配置文件。以下仅以TFTP作为示例介绍恢复备份在PC上的配置文件。

2. 设置恢复的配置文件为下次启动配置文件。

操作步骤

步骤1 通过TFTP恢复备份在PC上的配置文件

1. 启动TFTP服务器程序。

   在PC上启动TFTP服务器应用程序，设置好下载配置文件的传输路径、TFTP服务器IP地址、端口号。

2. 传输配置文件。

   在用户视图下执行**tftp**命令。

   ```
   <HUAWEI> tftp 10.110.24.254 get backup.cfg config.cfg
   ```

步骤2 设置恢复的配置文件为下次启动配置文件

```
<HUAWEI> startup saved-configuration config.cfg
```

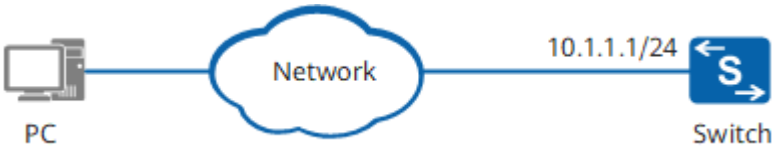
----结束

9.6.3 配置系统启动示例

组网需求

如图9-4所示，设备当前系统软件版本已经不能满足用户需求，用户需要部署更多的特性。此时需要远程为该设备进行系统软件升级。

图 9-4 配置系统启动组网图



配置思路

采用如下的思路配置系统启动以实现系统升级：

1. 将新的系统软件上传至设备根目录。
2. 保存系统当前配置，以使升级后配置仍生效。
3. 配置设备下次启动时加载的系统软件。
4. 配置设备下次启动时加载的配置文件。
5. 重新启动设备实现设备的升级。

操作步骤

步骤1 将新的系统软件上传至设备根目录

在进行配置前，可以先执行**display startup**命令查看当前设备下次启动文件的配置情况。

```
<HUAWEI> display startup
MainBoard:
  Configured startup system software:       flash:/basicsoft.cc
  Startup system software:                  flash:/basicsoft.cc
  Next startup system software:             flash:/basicsoft.cc
  Startup saved-configuration file:         flash:/vrpcfg.zip
  Next startup saved-configuration file:    flash:/vrpcfg.zip
  Startup paf file:                         NULL
  Next startup paf file:                    NULL
  Startup license file:                     NULL
  Next startup license file:                NULL
  Startup patch package:                    NULL
  Next startup patch package:               NULL
```

采用文件传输方式将新的系统软件文件上传至设备。文件传输方式较多，此处将设备配置为FTP服务器，从客户端获取系统软件文件。上传文件前需确保存储器有足够的空间保存新的系统软件文件，若是空间不足，需要清理存储器。

```
<HUAWEI> system-view
[HUAWEI] ftp server enable
[HUAWEI] aaa
[HUAWEI-aaa] local-user huawei password irreversible-cipher Helloworld@6789
[HUAWEI-aaa] local-user huawei service-type ftp
[HUAWEI-aaa] local-user huawei ftp-directory flash:
```

```
[HUAWEI-aaa] local-user huawei privilege level 15
[HUAWEI-aaa] quit
[HUAWEI] quit
```

在用户终端PC的命令行提示符中，执行**ftp 10.1.1.1**命令成功与设备建立FTP连接后，使用**put**命令向设备上传新的系统软件文件**newbasicsoft.cc**。上传成功后，可执行**dir**命令查看上传后的系统软件文件。

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

  Idx  Attr     Size(Byte)  Date        Time       FileName
    0  -rw-       515,160  Oct 01 2008 00:06:14   bootrom.bin
    1  -rw-         1,799  Jan 01 2012 00:22:58   private-data.txt
    2  drw-             -  Jan 01 2012 00:25:20   logfile
    3  drw-             -  Jan 29 2012 00:00:54   resetinfo
    4  -rw-    26,493,884  Dec 31 2011 23:46:52   basicsoft.cc
    5  -rw-         1,111  Nov 29 2011 19:43:54   vrpcfg.zip
    6  drw-    27,403,824  Jul 16 2012 19:14:26   newbasicsoft.cc
...

65,233 KB total (8,284 KB free)
```

步骤2 保存系统当前配置

```
<Switch> save
The current configuration will be written to the device.
Are you sure to continue? [Y/N]y
Now saving the current configuration to the slot 0.
Info: Save the configuration successfully.
```

步骤3 配置设备下次启动时加载的系统软件

```
<HUAWEI> startup system-software newbasicsoft.cc
```

步骤4 配置设备下次启动时加载的配置文件

```
<HUAWEI> startup saved-configuration vrpcfg.zip
```

说明

在步骤1中，通过**display startup**查看下次启动文件的配置情况，可以看到“Next startup saved-configuration file: flash:/**vrpcfg.zip**”，说明当前设备已经指定**vrpcfg.zip**作为下次启动时加载的配置文件，所以此步骤可以省略。但如果需要指定其他的配置文件作为下次启动时加载的配置文件时，必须要执行此步骤。

步骤5 检查配置结果

配置完成之后，执行如下命令，查看设备下次启动时加载的系统软件和配置文件。

```
<HUAWEI> display startup
MainBoard:
  Configured startup system software:        flash:/basicsoft.cc
  Startup system software:                   flash:/basicsoft.cc
  Next startup system software:              flash:/newbasicsoft.cc
  Startup saved-configuration file:          flash:/vrpcfg.zip
  Next startup saved-configuration file:     flash:/vrpcfg.zip
  Startup paf file:                          NULL
  Next startup paf file:                     NULL
  Startup license file:                      NULL
  Next startup license file:                 NULL
  Startup patch package:                     NULL
  Next startup patch package:                NULL
```

步骤6 重新启动设备

由于已保存过配置文件，所以此时可以执行**reboot fast**进行快速重新启动。

```
<Switch> reboot fast
System will reboot! Continue? [Y/N]:y
Info: system is rebooting ,please wait...
```


步骤7 验证配置结果

等候几分钟，设备重启完成，可再次进入系统。此时可执行命令**display version**，可以看到设备当前的系统软件版本为新的版本，表明升级完成。

display version命令的显示信息略。

----结束

配置文件

```
#
FTP server enable
#
vlan batch 10
#
aaa
 local-user huawei password irreversible-cipher $1a$C"d3YGyf411I-z$.si9E-TOVAw^&9Ttgw
%WAr0'~XC9n/;goO~V9XdV6aOE'$
 local-user huawei privilege level 15
 local-user huawei ftp-directory flash:
 local-user huawei service-type ftp
#
interface Vlanif10
 ip address 10.1.1.1 255.255.255.0
#
interface GigabitEthernet0/0/1  port link-type trunk  port trunk allow-pass vlan 10#
return
```


10 智能升级

10.1 智能升级简介
10.2 传统升级方式与智能升级方式的对比
10.3 智能升级配置注意事项
10.4 智能升级缺省配置
10.5 配置智能升级功能
10.6 立即执行智能升级操作
10.7 配置交换机智能升级功能升级交换机示例
10.8 配置AP智能升级功能升级AP示例
10.9 智能升级配置失败常见处理办法

10.1 智能升级简介

定义

当前设备数量逐年倍增，传统升级操作复杂繁琐，升级维护成本越来越高，为了能够更为便捷的将设备升级到最新版本，可以部署智能升级功能实现一键式快捷升级。

智能升级是一种通过互联网与华为在线升级平台（Huawei Online Upgrade Platform，HOUP）相连接，实现一键式加载/升级新版本的升级方式。

开启智能升级功能后，交换机定时向HOUP平台上送待升级交换机或AP的信息（包含设备名称、ESN号、当前系统软件版本和补丁），HOUP平台根据维护策略返回此设备最新的版本信息（包括推荐的系统软件版本、补丁、补丁类型、下载路径和文件大小），客户确认立即升级后自动下载软件包并且完成升级。交换机将升级结果上报HOUP平台。

说明

智能升级功能下载的系统文件由HOUP定制的维护策略决定，不需要用户手动指定。

部署方式

为了实现对智能升级的部署，交换机需要确保可以连入外网环境，如图10-1所示。如果交换机处于内网环境，可以通过设置代理服务器的方式间接接入到外网，如图10-2所示。

图 10-1 部署外网智能升级示意图

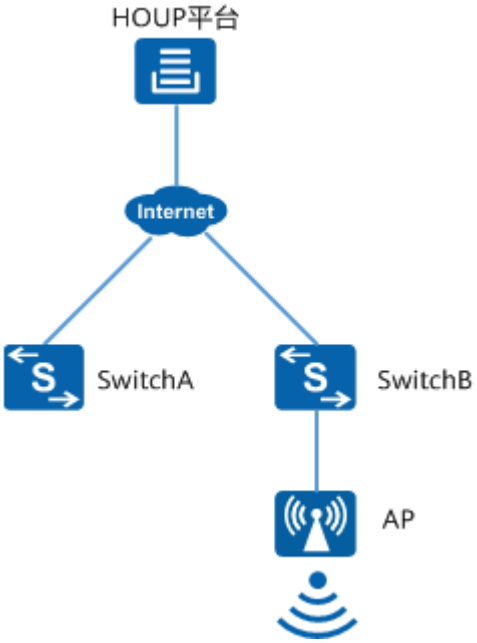
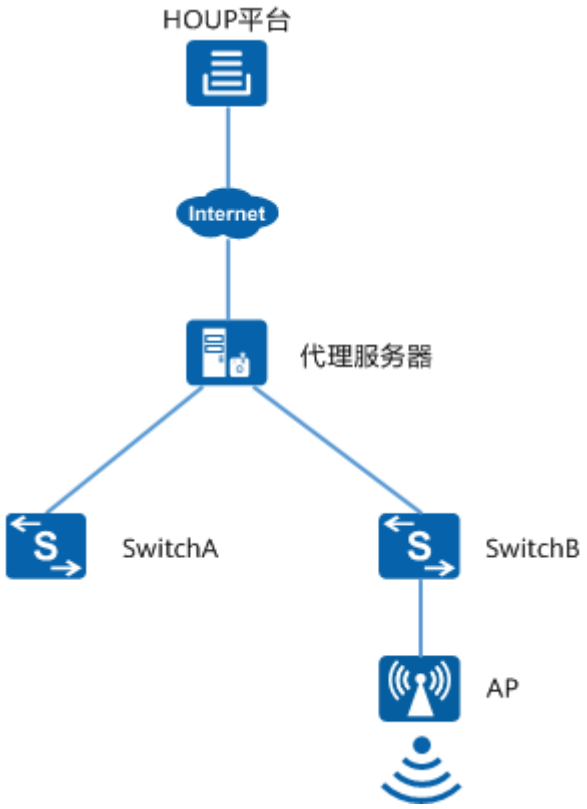


图 10-2 部署内网智能升级示意图



实现机制

在HOUP平台与交换机之间实现一键式智能升级的交互流程，如图10-3和图10-4所示。

图 10-3 交换机智能升级交互流程示意图

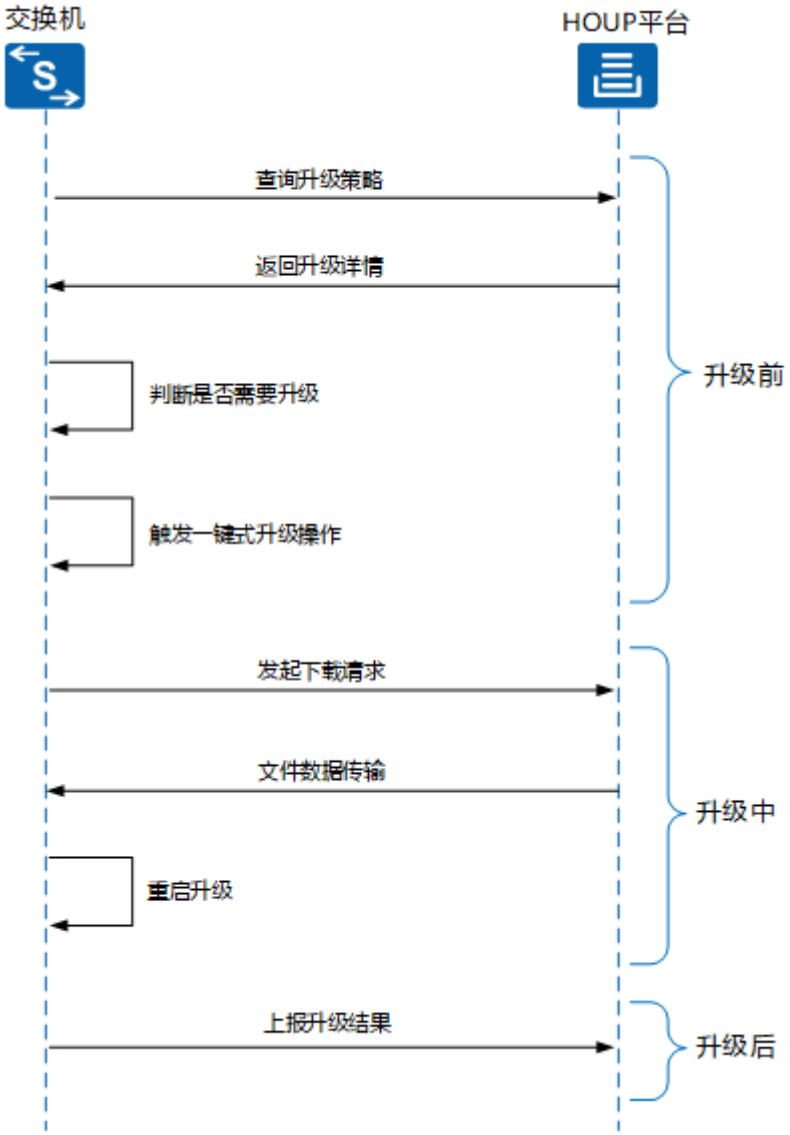
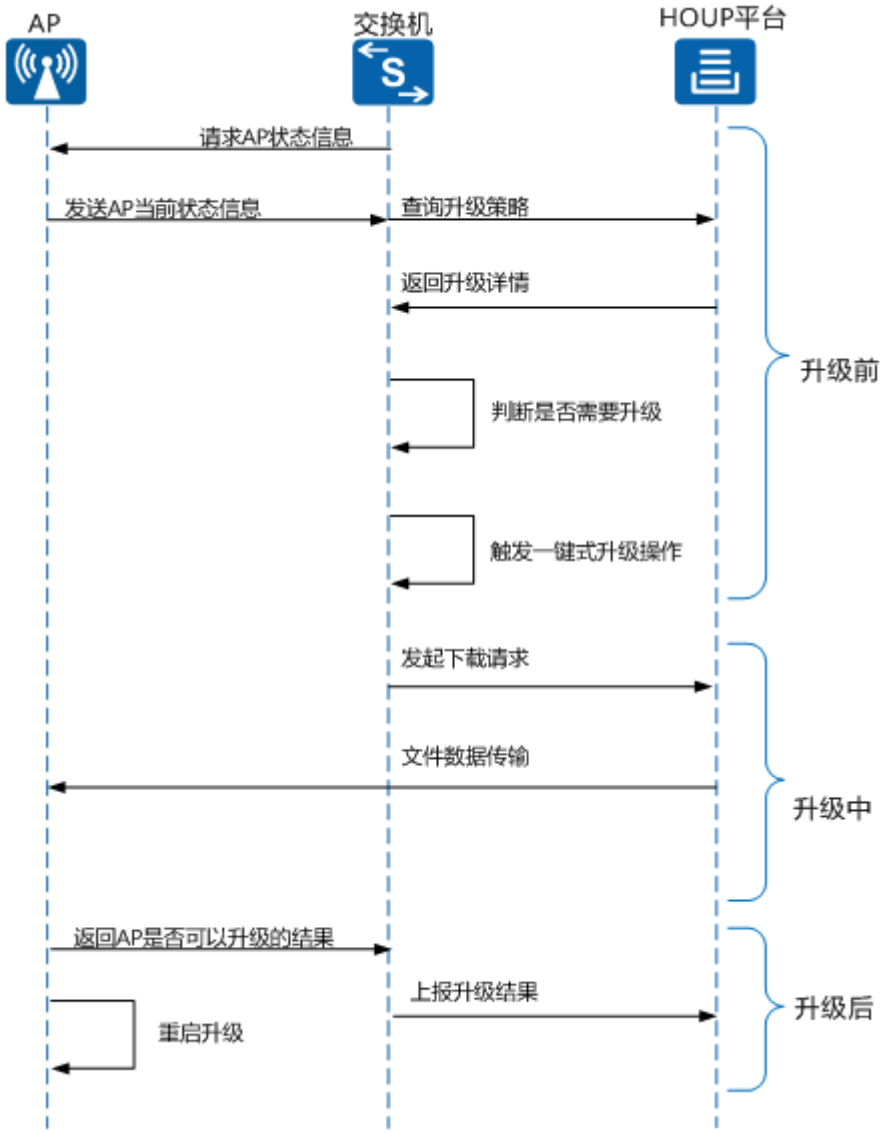


图 10-4 AP 智能升级交互流程示意图



具体交互流程如下：

升级前

1. 交换机上开启交换机或AP智能升级功能后，将会每隔24小时（使能时刻为起始时刻），自动给HOUP平台上报交换机或AP当前状态信息，请求更新升级详细情况。
2. HOUP平台内部根据已经制定的维护策略返回交换机或AP升级详细情况（包括最新系统软件版本信息、补丁）。
3. 管理员根据返回的升级详情判断是否需要升级。Web网管界面为升级提示信息，命令行界面根据命令查看是否需要升级。
4. 管理员手动触发一键式升级操作。在Web网管界面点击“立即升级”按键，命令行界面执行**smart-upgrade right-now**命令实现一键式设备升级。

升级中

1. 交换机执行立即智能升级的操作后，向HOUP平台请求下载最新的系统文件。

2. HOUP平台根据交换机的下载请求，通过HTTPS传输具体系统文件。
3. 系统文件下载完成后，交换机或AP自动设置下次启动的系统软件或补丁。对于交换机的智能升级，交换机会自动重启升级；对于AP的智能升级，AP会返回是否可以升级的结果给交换机后，再重启升级。（如果仅加载热补丁，不自动重启交换机或AP）

升级后

- 对于交换机的智能升级，重启交换机后，交换机自动上报升级结果。升级失败时，HOUP平台通知华为维护工程师升级失败。
- 对于AP的智能升级，AP返回可以升级的结果给交换机后，交换机就会自动上报升级结果。如果AP返回的结果是升级失败，HOUP平台通知华为维护工程师升级失败。

10.2 传统升级方式与智能升级方式的对比

表 10-1 传统升级方式与智能升级方式比较

维度	传统升级	智能升级
常用应用场景	基本所有场景都适用	可以与公网HOUP平台通信的交换机
升级方式	1. 获取系统软件或补丁 2. 上传系统软件或补丁 3. 配置设备下次启动时使用的系统软件或补丁文件 4. 重启设备	一键式升级
下载升级过程耗时	比智能升级方式耗时短	比传统升级方式耗时长
前提条件	1. 系统软件或补丁 2. 拥有运维技能的维护人员	● 设备处于外网环境当中，与HOUP平台路由可达（Ping通） ● 设备处于内网环境时，需配置代理服务器，与HOUP平台路由可达（Ping通）
支持版本	ALL	V200R019C00及之后版本
用户体验	需要专门的维护人员操作，体验相对不佳	体验上佳
回滚的支持情况	支持	支持
是否支持文件断点续传	支持	支持
是否支持通过Web操作	支持	支持

维度	传统升级	智能升级
隐私情况	无个人隐私输入	智能升级失败时，向HOUP平台上送电话及Email **说明** 设置智能升级联系电话和邮箱为用户可选功能。 联系方式主要是用作升级版本失败时的紧急联系，不会用作其他用途。

10.3 智能升级配置注意事项

涉及网元

需要与HOUP平台配合使用。

License 支持

智能升级是交换机的基本功能，无需获得License许可即可应用此功能。

V200R022C00 版本特性支持情况

除S5731-L和S5731S-L外，S300, S500, S2700, S5700, S6700系列交换机中所有款型均支持智能升级。

仅如下款型支持AP智能升级：

S5731-H、S5731-H-K、S5731S-H、S5732-H、S5732-H-K、S6730-H、S6730-H-K、S6730S-H

说明

如需了解交换机软件配套详细信息，请点击**硬件中心**，并选择产品型号进行查询。

S5731-L和S5731S-L属于远端模块，不支持Web管理、YANG和命令行，仅支持通过中心交换机对其下发配置，相关操作请参见《S300, S500, S2700, S5700, S6700 V200R022C00 配置指南-设备管理》中的“智能极简园区网络配置（小行星方案）”。

特性依赖和限制

- 在升级过程中，不允许合并拆分堆叠设备。
- 在升级过程中，不允许进行主备倒换。
- 在升级过程中，不允许进行格式化操作。

10.4 智能升级缺省配置

表 10-2 智能升级缺省配置

参数	缺省值
智能升级功能	未使能
AP智能升级功能	未使能
绑定智能升级的SSL策略	未绑定
设置智能升级代理	• 缺省URL为s.houp.huawei.com • 缺省HTTPS端口号为443
设置智能升级联系的电话和邮箱	未设置
智能升级不验证服务器功能	未使能

10.5 配置智能升级功能

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**ssl policy** *policy-name*，创建SSL策略并进入SSL策略视图。

步骤3 执行命令**trusted-ca load pem-ca** *ca-filename*，为SSL策略加载HOUP平台CA证书。

缺省情况下，SSL策略未加载信任证书。

说明

- HOUP平台CA证书**houp_root.cer**设备启动自动生成，不需要单独导入。
- 当误删除CA证书，或者CA证书失效时，可以创建一个没有CA证书的空的SSL策略（执行**ssl policy** *policy-name*命令创建SSL策略后，直接返回系统视图），然后执行命令**smart-upgrade verify-server disable**，临时关闭认证HOUP平台CA证书功能。
- 为充分保证设备通信安全，建议不要关闭CA证书验证功能。CA证书失效后，请及时前往**HOUP平台**获取。

步骤4 执行命令**quit**，返回系统视图。

步骤5 （可选）执行命令**smart-upgrade** { **url** *host* | **https-port** *https-port* }，设置智能升级代理服务器的地址及端口号。

缺省情况下，**url**为s.houp.huawei.com，**https-port**为443端口。

如果设备在内网中，无法直接连接到s.houp.huawei.com，连接一个代理服务器，通过该代理服务器与HOUP平台传输数据。

步骤6 执行命令**smart-upgrade ssl-policy** *policy-name*，为智能升级绑定SSL策略。

缺省情况下，智能升级未绑定SSL策略。

智能升级功能使能前，必须绑定一个SSL策略，因为智能升级使用HTTPS和HOUP平台建立连接关系。

步骤7 根据需要，使能交换机的智能升级功能或者AP的智能升级功能。

表 10-3 使能交换机的智能升级功能或者 AP 的智能升级功能

操作	命令	说明
使能交换机的智能升级功能	**smart-upgrade enable**	缺省情况下，交换机智能升级功能处于关闭状态。
对于S5731-H、S5731-H-K、S5731S-H、S5732-H、S5732-H-K、S6730-H、S6730-H-K、S6730S-H，使能AP的智能升级功能	1. **smart-upgrade enable** 2. **smart-upgrade ap enable**	缺省情况下，AP的智能升级功能处于关闭状态。 使能AP的智能升级功能前，需先执行**smart-upgrade enable**命令，使能交换机智能升级功能。

步骤8 （可选）执行命令**smart-upgrade information telephone** *phonevalue* **email** *emailvalue*，设置智能升级联系电话和邮箱命令。

缺省情况下，未设置智能升级联系电话和邮箱。

步骤9 （可选）执行命令**smart-upgrade web-prompt disable**，关闭智能升级Web提示功能。

缺省情况下，智能升级Web提示功能处于开启状态。

说明

关闭智能升级Web提示功能后，Web网管首页将不再提醒智能升级的工作状态和最新的软件版本信息。

步骤10 （可选）执行命令**smart-upgrade schedule at** *download-time* [**reboot at** *reboot-time*]，配置交换机的定时智能升级功能。

缺省情况下，交换机的定时智能升级功能处于关闭状态。

----结束

检查配置结果

- 执行命令**display ssl policy**，查看SSL策略的配置信息。
- 执行命令**display smart-upgrade information**，查看智能升级的详细信息。

10.6 立即执行智能升级操作

背景信息

当用户了解到有新的系统软件，想要升级体验新版本内容时，可以立即执行智能升级操作，实现设备的一键式加载/升级。

前置任务

在执行智能升级前，需要确保如下状态：

- 确保有新的系统软件版本。
- 开启了智能升级功能。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**display smart-upgrade information**，确认设备版本的检查结果**Check version result**字段为：**needUpdate**。

步骤3 （可选）执行命令**smart-upgrade download**，触发软件下载。

步骤4 执行命令**smart-upgrade right-now**，立即执行一次智能升级。

如果在执行该命令前未执行**smart-upgrade download**命令，本次智能升级会包含系统文件下载和系统升级两部分操作。如果在执行该命令前执行了**smart-upgrade download**命令，则本次智能升级直接进行系统升级操作。

说明

智能升级的下载过程支持断点续传，如果之前下载文件因为网络问题下载失败，再次执行相应命令，从断点处重新开始下载。

----结束

检查升级结果

升级完成后，执行命令**display version** [**slot** *slot-id*]或**display patch-information** [**history**]，查看交换机的版本信息或补丁信息，或者执行命令**display ap version all**，查看AP的版本信息或补丁信息。

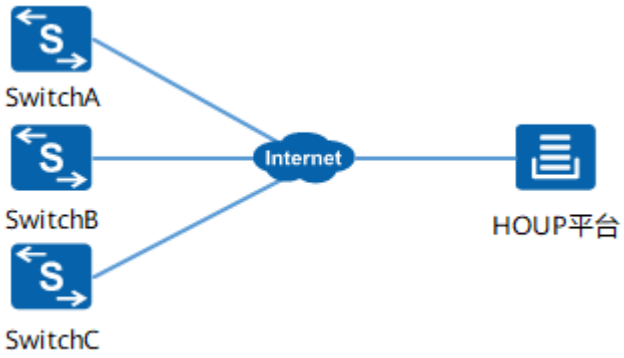
10.7 配置交换机智能升级功能升级交换机示例

大量交换机需要升级到最优版本当中，此时通过配置智能升级功能，可以实现交换机更加简便的升级。

组网需求

如图10-5所示的网络中，Switch处于公网环境，配置智能升级功能，实现从HOUP平台下载系统软件或补丁。

图 10-5 配置智能升级功能组网图



操作思路

1. 配置SSL策略并绑定CA证书。
2. 配置智能升级功能，包括绑定SSL策略、使能智能升级功能等。
3. 查看交换机设备状态。
4. 触发立即智能升级。

操作步骤

步骤1 在SwitchA配置SSL策略并绑定CA证书。SwitchB、SwitchC的配置与SwitchA类似，不再赘述。

```
<HUAWEI> system-view
[HUAWEI] ssl policy houp
[HUAWEI-ssl-policy-houp] trusted-ca load pem-ca houp_root.cer
[HUAWEI-ssl-policy-houp] quit
```

步骤2 在SwitchA配置智能升级功能。SwitchB、SwitchC的配置与SwitchA类似，不再赘述。

```
[HUAWEI] smart-upgrade ssl-policy houp    //智能升级绑定SSL策略。
[HUAWEI] smart-upgrade enable    //使能智能升级功能。
[HUAWEI] smart-upgrade information telephone 111111111 email abcd@huawei.com    //设置智能升级联系电话和邮箱命令。
```

步骤3 检查交换机版本状态和网络的连通性。

查看交换机与HOUP平台的连通性和交换机当前版本状态。

```
[HUAWEI] display smart-upgrade information
Info: Loading the information, please wait .

Configuration:
   URL                    : s.houp.huawei.com
   HTTPS port             : 443
   Bind SSL policy        : houp
   Verify HTTPS server    : true
   Telephone              : 1****1111
   Email                  : ****@huawei.com

Version information:
   Refresh time           : 2019-01-23 12:24:06
   Check version result   : needUpdate    //交换机版本非最优版本，建议升级。（如果与HOUP平台网络不通，显示netError）
   Recommended software version : V200R022C00
   Recommended patch version    : V200R020SPH001
   Upgrade description    :
```

```
  Firmware and Patch Description in English:1)description:2)CC+SPH

  Software package name       : S5730-HI-V200R022C00.cc
  Software package size(B)    : 120101636
  Patch package name          : S5730-HI-V200R020SPH001
  Patch package size(B)       : 14910

Upgrade information:
  Upgrade Time                : 2019-01-23 11:13
  Upgrade status              : success
  Cancellation status         : -
  Software download time      : -
  Software download progress(%): -
  Software download speed(KB/s): -
  Patch download time         : -
  Patch download progress(%)  : -
  Patch download speed(KB/s)  : -
  Last upgrade time           : 2019-01-23 11:13
  Last upgrade result         : success

Local information:
  Device name                 : S5730HI-44C-HI-24S
  ESN                         : 2102351XFR12xxxxxxxx
  Software version            : V200R022C00
  Patch version               : V200R020SPH

Schedule Upgrade Information:
  Download time               : -
  Download triggered          : no
  Download pre-check result   : -
  Reboot time                 : -
  Reboot triggered            : no
  Reboot triggered result     : -
```

步骤4 触发设备智能升级。SwitchB、SwitchC的配置与SwitchA类似，不再赘述。

```
[HUAWEI] smart-upgrade right-now
Info: Getting version information from houp, please wait ...
Info: If you want to stop the upgrade, please press CTRL + C.
Info: Downloading file basic-soft.cc ...
Info: The file already exists, check whether it can be resumed from the breakpoint.
Info: Resume from the 15728640 bytes breakpoint.
Info: Current percent is 100%.
Info: 104372996 byte(s) received in 197.329 second(s) 516.53 Kbyte(s)/sec.
Info: Downloading file basic-soft.cc.asc ...
Info: Current percent is 100%.
Info: 490 byte(s) received in 0.201 second(s) 2.38 Kbyte(s)/sec.
Info: Downloading file basic-patch.pat ...
Info: The file already exists, check whether it can be resumed from the breakpoint.
Info: The file size is OK and the content is consistent.
Info: Downloading file basic-patch.pat.asc ...
Info: The file already exists, check whether it can be resumed from the breakpoint.
Info: The file size is OK and the content is consistent.
Info: Start verifying signature ...
Info: Signature verification passed.
Info: Set next startup patch basic-patch.pat successfully.
Info: Start set next startup file, please wait...
Info: Set next startup file basic-soft.cc successfully.
Info: System will rebooting for upgrade...
```

步骤5 查看升级后的软件版本。

```
<HUAWEI> display version
Huawei Versatile Routing Platform Software
VRP (R) software, Version 5.170 (S5730-HI V200R022C00)
Copyright (C) 2000-2018 HUAWEI TECH Co., Ltd.
HUAWEI S5730HI-44C-HI-24S Routing Switch uptime is 0 week, 0 day, 13 hours, 49
minutes

ES5D2S52C004 1(Master)  : uptime is 0 week, 0 day, 13 hours, 47
minutes
```



```
DDR             Memory Size : 4096  M bytes
FLASH Total     Memory Size : 1024  M bytes
FLASH Available Memory Size : 842   M bytes
SSD             Memory Size : 223   G bytes
Pcb          Version   : VER.A
BootROM      Version   : 020d.0000
BootLoad     Version   : 020d.0000
CPLD         Version   : 0102
Software     Version   : VRP (R) Software, Version 5.170 (V200R022C00)    //设备当前的软件版
本。
FLASH        Version   : 0000
CARD1 information
Pcb          Version   : ES5D21X08T00 VER.C
CPLD         Version   : 010c
PWR1 information
Pcb          Version   : PWR VER.A
FAN1 information
Pcb          Version   : NA
```

----结束

配置文件

- SwitchA的配置文件

```
#
smart-upgrade ssl-policy houp
smart-upgrade enable
smart-upgrade information telephone %^%#io6P(j9(U;):/}VIw8@T}G4/4{`@TX{' email %^%#r~|
i3Gp6U2k)YHDat=l1}G4/4{`@TX{'{'<tO+P<g"%^%#
#
ssl policy houp
 trusted-ca load pem-ca houp_root.cer
 ssl minimum version tls1.2       // ssl policy自动生成
#
```

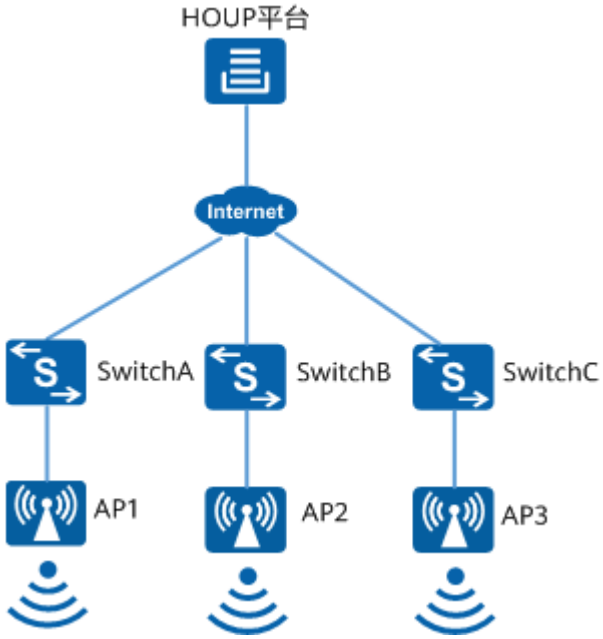
10.8 配置 AP 智能升级功能升级 AP 示例

大量AP需要升级到最优版本，此时通过配置AP智能升级功能，可以实现AP更加简便的升级。

组网需求

如图10-6所示的网络中，Switch处于公网环境，配置AP智能升级功能，实现从HOUP平台下载系统软件或补丁。

图 10-6 配置 AP 智能升级功能组网图



操作思路

1. 配置SSL策略并绑定CA证书。
2. 配置智能升级功能，包括绑定SSL策略、使能AP智能升级功能等。
3. 查看AP状态。
4. 触发软件下载。
5. 触发立即智能升级。

操作步骤

步骤1 在SwitchA配置SSL策略并绑定CA证书。SwitchB、SwitchC的配置与SwitchA类似，不再赘述。

```
<HUAWEI> system-view
[HUAWEI] ssl policy houp
[HUAWEI-ssl-policy-houp] trusted-ca load pem-ca houp_root.cer
[HUAWEI-ssl-policy-houp] quit
```

步骤2 在SwitchA配置AP智能升级功能。SwitchB、SwitchC的配置与SwitchA类似，不再赘述。

```
[HUAWEI] smart-upgrade ssl-policy houp    //智能升级绑定SSL策略。
[HUAWEI] smart-upgrade enable    //使能交换机智能升级功能。
[HUAWEI] smart-upgrade ap enable    //使能AP智能升级功能。
[HUAWEI] smart-upgrade information telephone 111111111 email abcd@huawei.com    //设置智能升级联系电话和邮箱命令。
```

步骤3 检查AP版本状态和网络的连通性。

查看交换机与HOUP平台的连通性和AP当前版本状态。

```
[HUAWEI] display smart-upgrade information
Info: Loading the information, please wait .

Configuration:
```

```
  URL                     : s.houp.huawei.com
  HTTPS port              : 443
  Bind SSL policy         : houp
  Verify HTTPS server     : true
  Telephone               : 1****1111
  Email                   : ****@huawei.com
Version information:
  Refresh time            : 2020-06-10 12:24:06
  Check version result    : needUpdate   //AP版本非最优版本，建议升级。（如果与HOUP平台网络不通，
显示netError）
  Recommended software version : V200R022C00
  Recommended patch version   : -
  Upgrade description         : -
  Software package name       : AirEngineX760_V200R022C00.bin
  Software package size(B)    : 13019148

Upgrade information:
  Upgrade Time            : 2020-06-10 10:58:08
  Upgrade status          : success
  Cancellation status     : -
  Software download time  : -
  Software download progress(%): -
  Software download speed(KB/s): -
  Last upgrade time       : 2020-06-10 10:58:08
  Last upgrade result     : success

Local information:
  Device name             : AirEngine 8760-X1-PRO
  ESN                     : 2102351XFR12xxxxxxxx
  Software version        : V200R019C10
  Patch version           : -

AP information:
  Device Type             : AirEngine 8760-X1-
PRO
  Hardware Type           : 228

Schedule Upgrade Information:
  Download time           : -
  Download triggered      : no
  Download pre-check result   : -
  Reboot time             : -
  Reboot triggered        : no
  Reboot pre-check result     : -
```

步骤4 触发软件下载。SwitchB、SwitchC的配置与SwitchA类似，不再赘述。

```
[HUAWEI] smart-upgrade download
Info: Getting version information from houp, please wait ...
Info: If you want to stop the upgrade, please press CTRL + C.
Info: Downloading file AirEngineX760_V200R022C00.bin ...
Info: Current percent is 100%.
Info: 13019148 byte(s) received in 20.263 second(s) 627.45 Kbyte(s)/sec..
```

步骤5 触发设备智能升级。SwitchB、SwitchC的配置与SwitchA类似，不再赘述。

```
[HUAWEI] smart-upgrade right-now
Info: Getting version information from houp, please wait ...
Info: If you want to stop the upgrade, please press CTRL + C.
Info: Downloading file
AirEngineX760_V200R022C00.bin ...
Info: The file already exists, check whether it can be resumed from the breakpoint.
Info: The file size is OK and the content is consistent.
Info: Successfully upgraded the system software of APs.
```

步骤6 查看升级后的软件版本。

```
[HUAWEI] display ap version all
Compatible version : V200R020 V200R019 V200R010 V200R009 V200R010 V200R008 V200R009 V200R010
V200R007
--------------------------------------------------------------------------------------------
ID    Name          Group   Type          Version             PatchVersion     state
```

```
-------------------------------------------------------------------------------------------
0     00e0-fc76-e360 default AirEngine 8760-X1-PRO       V200R022C00          -              normal
-------------------------------------------------------------------------------------------
Total: 1
```

----结束

配置文件

- SwitchA的配置文件

```
#
smart-upgrade ssl-policy houp
smart-upgrade enable
smart-upgrade information telephone %^%#io6P(j9(U;):/}VIw8@T}G4/4{`@TX{' email %^%#r~|
i3Gp6U2k)YHDat=l1}G4/4{`@TX{'{'<tO+P<g"%^%#
smart-upgrade ap enable
#
ssl policy houp
 trusted-ca load pem-ca houp_root.cer
 ssl minimum version tls1.2       // ssl policy自动生成
#
```

10.9 智能升级配置失败常见处理办法

故障现象

在查询智能升级更新状态信息的命令**display smart-upgrade information**回显信息中，**Check version result**项目显示为netError。

操作步骤

1. 检查是否为SSL策略加载信任证书机构文件。

   缺省情况下，服务器CA证书验证功能开启，因此需要加载CA证书。在系统视图下执行命令**display ssl policy**，查看智能升级绑定的SSL策略是否加载了CA证书，确认证书名称为**houp_root.cer**（系统自带）。如果未加载CA证书，可以执行命令**trusted-ca load pem-ca** *ca-filename*，为SSL策略加载CA证书。

2. 检查交换机与HOUP平台的网络连通性。

   由于HOUP平台处于公网当中，因此需要交换机可以连接公网环境。在用户视图下执行命令**ping** s.houp.huawei.com，检测与HOUP平台的网络连通性。

   如果检测失败，根据实际组网判断交换机所处环境：

   - 当处于内网环境时，通过命令**smart-upgrade url**、**smart-upgrade https-port**，配置连接代理服务器的代理站点和HTTPS端口。
   - 当处于外网环境时，检查交换机与HOUP平台之间每一条链路都处于连通状态。

3. 判断交换机与公网之间是否需要穿越防火墙。

   如果交换机与公网之间需要穿越防火墙，需要在防火墙上放通相应的策略，涉及到的策略如下：

   a. 交换机与HOUP平台间使用HTTPS通信。

   b. HOUP平台会用到的通信端口号443。

11 BootLoad 菜单操作

11.1 BootLoad菜单
11.2 启动配置信息子菜单Enter startup submenu
11.3 以太网子菜单Enter ethernet submenu
11.4 修改以太网参数Modify ethernet interface boot parameter
11.5 文件系统子菜单Enter filesystem submenu
11.6 密码子菜单Enter password submenu
11.7 清除Console登录密码Clear password for console user
11.8 BootLoad诊断菜单
11.9 通过BootLoad菜单升级系统软件

11.1 BootLoad 菜单

设备启动过程中，将启动BootLoad程序。

当出现“Press Ctrl+B to enter BootLoad menu:”时，及时（3秒内）按下快捷键Ctrl+B，进入BootLoad菜单。

```
Press Ctrl+B to enter BootLoad menu : 2
Info: The password is empty. For security purposes, change the password.

New password:   //设置BootLoad密码
Verify:
```

为保证设备的安全，防止非法用户进入BootLoad菜单操作，进入BootLoad菜单需要输入密码。

BootLoad菜单密码修改方法有两种：

- 通过**11.6.1 修改BootLoad密码Modify bootload password**菜单进行修改。
- 通过安装BOOTROMPSW插件后执行**bootrom password change**命令修改，详见《插件使用指南》中“BOOTROMPSW使用指南”章节。

您可以在《S系列交换机缺省帐号与密码》（**企业网**、**运营商**）文档中获取各种缺省帐号与密码信息。获取该文档需要权限，如需升级权限，请查看网站帮助。

说明

如果三次输入错误的BootLoad密码，设备会自动重启。

为充分保证设备安全，请您定期修改密码。

设备启动过程中，当出现“Press Ctrl+T to Start Memory Test”或“Press CTRL+T for full memory test”或“Press [Ctrl+T] to entry diag menu in 1 seconds”时，用户此时如果按下快捷键Ctrl+T，则设备将进行内存检测。

输入正确的BootLoad密码后，显示的BootLoad菜单如下

```
    BootLoad Menu

  1. Boot with default mode
  2. Enter startup submenu
  3. Enter ethernet submenu
  4. Enter filesystem submenu
  5. Enter password submenu
  6. Clear password for console user
  7. Reboot
 (Press Ctrl+E to enter diag menu)

Enter your choice(1-7):
```

表 11-1 BootLoad 菜单介绍

项目	描述
Boot with default mode	不进入重启BootLoad阶段，直接从当前阶段继续启动。 当用户需要快速启动设备时，或者在BootLoad菜单下做的操作不涉及BootLoad程序自身（例如修改BootLoad密码）时，可以执行此操作。
Enter startup submenu	进入启动配置信息子菜单。此菜单下可以查看和修改启动配置信息。
Enter ethernet submenu	进入以太网子菜单。此菜单下可以实现通过以太网口下载文件到内存和存储器，还可以备份配置文件。 使用以太网口进行操作需要预设文件服务器，并配置网络参数以保证设备和服务器路由可达，优点是文件传输速率快。
Enter filesystem submenu	进入文件系统子菜单。此菜单下可以实现对文件系统的管理和维护。
Enter password submenu	进入密码子菜单。此菜单下可以修改BootLoad密码或者恢复BootLoad密码为缺省值。
Clear password for console user	清除Console口登录验证密码。当用户遗忘Console口登录密码导致无法登录设备时，可以通过此菜单清除Console登录密码。
Reboot	当修改的参数对BootLoad菜单前面的初始化工作有影响时，可执行**Reboot**先进入重启BootLoad阶段，再启动其他部件。

项目	描述
(Press Ctrl+E to enter diag menu)	按下快捷键<Ctrl+E>进入诊断菜单。关于诊断菜单的介绍，请参见**BootLoad诊断菜单**。
快捷键	在BIOS菜单中，可以使用Ctrl+M、Ctrl+J和Ctrl+E三个快捷键。具体功能描述如下： • Ctrl+M和Ctrl+J：在BIOS任何菜单中使用该快捷键，其功能类似于回车键。 • Ctrl+E：只能在BIOS主菜单中执行该快捷键，执行快捷键后会打印框类型信息。

11.2 启动配置信息子菜单 Enter startup submenu

在BootLoad菜单下，选择2，进入启动配置信息子菜单。

```
      BootLoad Menu

   1. Boot with default mode
   2. Enter startup submenu
   3. Enter ethernet submenu
   4. Enter filesystem submenu
   5. Enter password submenu
   6. Clear password for console user
   7. Reboot
  (Press Ctrl+E to enter diag menu)

Enter your choice(1-7): 2

      Startup Configuration Submenu

   1. Display startup configuration
   2. Modify startup configuration
   3. Return to main menu

Enter your choice(1-3):
```

表 11-2 启动配置信息子菜单介绍

项目	描述
Display startup configuration	查看设备当前启动和上次启动使用的系统软件、配置文件和补丁文件。 在系统升级或降级之前，可以通过此菜单查看启动加载文件是否正确。
Modify startup configuration	修改启动配置信息。 在系统升级或降级之前，可以通过此菜单指定设备启动时使用的系统软件，配置文件或者补丁文件。
Return to main menu	返回主菜单。

11.2.1 查看启动配置信息 Display startup configuration

在系统升级或降级之前，通过在启动配置信息菜单下，选择“1. Display startup configuration”查看是否为正确的启动加载文件。

```
    Startup Configuration Submenu

  1. Display startup configuration
  2. Modify startup configuration
  3. Return to main menu

Enter your choice(1-3): 1
Current startup configuration
  startup type      : Flash
  startup file      : s5720hi.cc
  configuration file: vrpcfg.zip
  patch package     :

Last time startup state : Success
Latest successful startup configuration
  startup file      : s5720hi.cc
  configuration file: vrpcfg.zip
  patch package     :
```

表 11-3 输出信息描述

项目	描述
Current startup configuration	表示下方为当前启动使用的配置信息。
startup type	表示启动存储器，即系统软件、配置文件和补丁文件所在的存储器。设备仅支持Flash存储器，取值为Flash。
startup file	表示系统软件，格式为“*.cc”。
configuration file	表示配置文件，格式为“*.zip”或“*.cfg”。
patch package	表示补丁文件，格式为“*.pat”。
Last time startup state	表示上次启动状态。取值为： ● Success：成功 ● failed：失败
Latest successful startup configuration	表示上一次成功启动时，使用的配置信息。

11.2.2 修改启动配置信息 Modify startup configuration

背景信息

当设备的系统软件损坏，无法正常登录设备时，可以利用BootLoad程序上传系统软件和补丁文件，然后指定设备按照上传的文件启动，可以完成设备的系统软件修复和升级。

说明

修改启动配置信息前，请使用**11.3 以太网子菜单Enter ethernet submenu**中的文件上传功能，将指定的文件上传至Flash中。

操作步骤

步骤1 在启动配置信息菜单下，选择2，进入启动配置信息修改菜单。

```
    Startup Configuration Submenu

  1. Display startup configuration
  2. Modify startup configuration
  3. Return to main menu

Enter your choice(1-3): 2
```

步骤2 选择启动存储器。

```
Note: startup file field can not be cleared
'.'=clear field; '^D'=quit; Enter=use current configuration

startup type(1: Flash)
  current: 1
  new    :
```

目前设备仅支持Flash存储器，无需设置，直接跳入下一项。

步骤3 指定系统软件。

```
Flash startup file (can not be cleared)
  current: s5720hi.cc
  new    :
```

输入新的系统软件名，并回车进入下一项。如果设备当前的系统软件可用，并且不希望更换，直接回车，进入下一项。

说明

- 设置新的系统软件时，设备会对系统软件的完整性进行校验。如果系统软件的数字签名不合法，设置将会失败。请确保系统软件来源的合法性。
- 需确保指定的系统软件存在于设备的Flash中，并且可用，否则设备会启动失败。按照设置的系统软件多次（3次）启动失败后，设备会按照上次成功启动时使用的系统软件启动。
- 如果指定的系统软件是V200R008及之前版本，用户必须先通过**恢复BootLoad菜单密码**为缺省值后再指定系统软件。否则可能会导致BootLoad密码不可用或者设备出现故障。

步骤4 指定补丁文件。

```
patch package
  current: s5720hi-sph005.pat
  new    :
```

直接输入补丁文件名，并回车退出修改Flash描述界面，回到启动配置信息子菜单。如果不升级补丁文件，直接回车退出修改Flash描述界面。缺省情况下，未指定补丁文件。

----结束

11.3 以太网子菜单 Enter ethernet submenu

使用以太网菜单中的功能进行文件传输前，需要预先设置一台FTP/TFTP/SFTP服务器，作为文件服务器，并且将设备的管理网口与FTP/TFTP/SFTP服务器相连。

说明

对于没有管理网口的设备，使用第一个接口与FTP/TFTP/SFTP服务器相连，有些设备的第一个接口为Combo口，那就使用此Combo口的电口。

通过以太网口传输文件相比串口传输的明显优势在于传输速率快，但是需要预先准备FTP/TFTP/SFTP服务器和单独连接线缆。

在BootLoad主菜单下，选择3，进入以太网子菜单。

```
    BootLoad Menu

  1. Boot with default mode
  2. Enter startup submenu
  3. Enter ethernet submenu
  4. Enter filesystem submenu
  5. Enter password submenu
  6. Clear password for console user
  7. Reboot
 (Press Ctrl+E to enter diag menu)

Enter your choice(1-7): 3

    ETHERNET  SUBMENU

  1. Download file to Flash through ethernet interface
  2. Modify ethernet interface boot parameter
  3. Return to main menu

Enter your choice(1-3):
```

表 11-4 以太网子菜单介绍

项目	描述
Download file to Flash through ethernet interface	通过以太网口向Flash中加载文件。
Modify ethernet interface boot parameter	修改以太网口参数。通过以太网口上传文件之前，需要正确配置以太网口的参数。 这里所说的以太网口指设备的管理网口，设置此网口的IP地址、需要上传的文件、FTP/TFTP/SFTP用户名和密码等信息，实现设备与FTP/TFTP/SFTP服务器的连接。
Return to main menu	返回主菜单。

11.4 修改以太网参数 Modify ethernet interface boot parameter

背景信息

当格式化存储器之后，可以通过此选项重新上传系统软件、配置文件等信息。

BootLoad菜单支持配置设备与其他设备或PC建立FTP、TFTP和SFTP连接，用以快速传输系统软件、配置文件和补丁等文件，但是在使用此功能前需对相连的以太网口（即设备的管理网口）进行参数设置，保证FTP/TFTP/SFTP连接两端的参数相匹配。

前置任务

BootLoad菜单下的设备仅支持作为FTP/TFTP/SFTP客户端，在使用此菜单进行文件传输前，需预先配置FTP/TFTP/SFTP服务器作为文件服务器，并保证FTP/TFTP/SFTP服务器与设备的管理网口相连，而且两者可以实现互通。

操作步骤

步骤1 在以太网子菜单下，选择**Modify ethernet interface boot parameter**项，进入修改以太网参数菜单。

```
      BOOTLINE  SUBMENU

1. Set TFTP protocol parameters
2. Set FTP protocol parameters
3. Set SFTP protocol parameters
4. Return to ethernet menu

Enter your choice(1-4):
```

说明

此功能输入的FTP/TFTP/SFTP协议参数信息会在退出BootLoad菜单后清空。

步骤2 根据事先配置的服务器类型选择配置TFTP协议参数、FTP协议参数还是SFTP协议参数。

表 11-5 修改以太网参数菜单操作说明

操作	含义
输入字符 **说明** 以太网参数取值不支持空格、“~”、“*”、“/”、“\”、“:”、“'”和“"”等字符，不区分大小写。	表示需要变更此项已有的值，按回车键Enter确认输入。
小数点.	表示清空此区域已有内容。
短横杠-	表示回退到上一项。
Ctrl+D	表示退出以太网口参数修改界面，回到以太网子菜单。
不输入字符，直接回车	表示此项不作修改，跳至下一项。

- 如果配置的文件服务器是TFTP服务器，选择1，进入TFTP协议参数设置界面。

```
      BOOTLINE  SUBMENU

  1. Set TFTP protocol parameters
  2. Set FTP protocol parameters
  3. Set SFTP protocol parameters
  4. Return to ethernet menu

Enter your choice(1-4): 1

'.' = clear field;  '-' = go to previous field;  'Ctrl+D' = quit
```



```
Load File name      : s6720li.cc
Switch IP address   : 192.168.1.15
Server IP address   : 192.168.1.40
```

表 11-6 TFTP 协议参数设置菜单介绍

项目	描述
Load File name	需要上传的文件。文件名为字符串形式，长度范围是1～64，不支持空格、问号、“\"”、“\'”、“\\”、“*”、“~”、“/”、“:”、“|”，且不能以“.”开头或者结尾。
Switch IP address	设置本设备管理IP地址。缺省情况下，设备管理IP地址为192.168.1.15。 **说明** 设置的IP地址注意与TFTP服务器的IP地址处在同一网段。
Server IP address	TFTP服务器的IP地址。

- 如果配置的文件服务器是FTP服务器，选择2，进入FTP协议参数设置界面。

```
        BOOTLINE  SUBMENU

  1. Set TFTP protocol parameters
  2. Set FTP protocol parameters
  3. Set SFTP protocol parameters
  4. Return to ethernet menu

Enter your choice(1-4): 2

'.' = clear field;  '-' = go to previous field;  'Ctrl+D' = quit

Load File name      : s6720li.cc
Switch IP address   : 192.168.1.15
Server IP address   : 192.168.1.40
FTP User Name       : huawei
FTP User Password   :
```

表 11-7 FTP 协议参数设置菜单介绍

项目	描述
Load File name	需要上传的文件。文件名为字符串形式，长度范围是1～64，不支持空格、问号、“\"”、“\'”、“\\”、“*”、“~”、“/”、“:”、“|”，且不能以“.”开头或者结尾。
Switch IP address	设置本设备管理IP地址。缺省情况下，设备管理IP地址为192.168.1.15。 **说明** 设置的IP地址注意与FTP服务器的IP地址处在同一网段。
Server IP address	FTP服务器的IP地址。
FTP User Name	FTP服务器的用户名。

项目	描述
FTP User Password	FTP服务器的登录密码，为密文形式。

- 如果配置的文件服务器是SFTP服务器，选择3，进入SFTP协议参数设置界面。

```
        BOOTLINE  SUBMENU

  1. Set TFTP protocol parameters
  2. Set FTP protocol parameters
  3. Set SFTP protocol parameters
  4. Return to ethernet menu

Enter your choice(1-4): 3

'.' = clear field;  '-' = go to previous field;  'Ctrl+D' = quit

Load File name      : s6720li.cc
Switch IP address   : 192.168.1.15
Server IP address   : 192.168.1.40
SFTP User Name      : huawei
```

表 11-8 SFTP 协议参数设置菜单介绍

项目	描述
Load File name	需要上传的文件。文件名为字符串形式，长度范围是1～64，不支持空格、问号、“\"”、“\'”、“\\”、“*”、“~”、“/”、“:”、“|”，且不能以“.”开头或者结尾。
Switch IP address	设置本设备管理IP地址。缺省情况下，设备管理IP地址为192.168.1.15。 **说明** 设置的IP地址注意与SFTP服务器的IP地址处在同一网段。
Server IP address	SFTP服务器的IP地址。
SFTP User Name	SFTP服务器的用户名。

----结束

11.5 文件系统子菜单 Enter filesystem submenu

在BootLoad主菜单下，选择4，进入文件系统子菜单。

```
      BootLoad Menu

  1. Boot with default mode
  2. Enter startup submenu
  3. Enter ethernet submenu
  4. Enter filesystem submenu
  5. Enter password submenu
  6. Clear password for console user
  7. Reboot
 (Press Ctrl+E to enter diag menu)

Enter your choice(1-7): 4
```

```
    FILESYSTEM SUBMENU


  1. Format Flash
  2. Delete file from Flash
  3. Rename file from Flash
  4. Display Flash files
  5. Return to main menu
Enter your choice(1-5):
```

表 11-9 文件系统子菜单介绍

项目	描述
Format flash	格式化存储器。 当存储器发生坏区、无法使用等故障时，可以通过格式化存储器排除故障。如果格式化仍不能排除故障，请联系技术支持人员。 **须知** 格式化Flash后，设备将无法启动，需重新加载系统软件，请谨慎使用。
Delete file from Flash	删除Flash中的文件。 **说明** 进入删除操作界面后，设备会显示目前Flash中的所有文件，方便选取需要删除的文件名。
Rename file from Flash	重命名文件名。 **说明** 进入重命名操作界面后，设备会显示目前Flash中的所有文件，方便选取需要重命名的文件名。
Display Flash files	查看Flash中包含的文件。显示Flash包含的所有文件的同时，也会显示Flash总空间和剩余空间的大小。
Return to main menu	返回主菜单。

11.6 密码子菜单 Enter password submenu

在BootLoad主菜单下，选择5，进入密码子菜单。

```
    BootLoad
Menu
  1. Boot with default mode
  2. Enter startup submenu
  3. Enter ethernet submenu
  4. Enter filesystem submenu
  5. Enter password submenu
  6. Clear password for console user
  7. Reboot
 (Press Ctrl+E to enter diag menu)

Enter your choice(1-7):5
```

```
    PASSWORD  SUBMENU

1. Modify bootload password
2. Reset bootload password
3. Return to main menu

Enter your choice(1-3):
```

表 11-10 密码子菜单介绍

项目	描述
Modify bootload password	修改BootLoad密码。为防止非法用户进入BootLoad菜单，用户可以通过此菜单重新设置登录密码。
Reset bootload password	恢复BootLoad密码为缺省值。 您可以在《S系列交换机缺省帐号与密码》（**企业网**、**运营商**）文档中获取各种缺省帐号与密码信息。获取该文档需要权限，如需升级权限，请查看网站帮助。
Return to main menu	返回主菜单。

11.6.1 修改 BootLoad 密码 Modify bootload password

背景信息

您可以在《S系列交换机缺省帐号与密码》（**企业网**、**运营商**）文档中获取各种缺省帐号与密码信息。获取该文档需要权限，如需升级权限，请查看网站帮助。

操作步骤

- 在BootLoad主菜单下，选择5，进入密码子菜单。

```
    BootLoad Menu

  1. Boot with default mode
  2. Enter startup submenu
  3. Enter ethernet submenu
  4. Enter filesystem submenu
  5. Enter password submenu
  6. Clear password for console user
  7. Reboot
 (Press Ctrl+E to enter diag menu)

Enter your choice(1-7): 5

    PASSWORD  SUBMENU

  1. Modify bootload password
  2. Reset bootload password
  3. Return to main menu

Enter your choice(1-3):
```

- 在密码子菜单下，选择1，进入BootLoad密码修改界面。

```
      PASSWORD  SUBMENU

   1. Modify bootload password
   2. Reset bootload password
   3. Return to main menu

Enter your choice(1-3): 1

Old password:     //输入原密码
New password:     //输入新密码
Verify:           //再次输入新密码
```

----结束

11.6.2 恢复 BootLoad 菜单密码 Reset bootload password

背景信息

用户可以在密码子菜单中选择“2. Reset bootload password”，恢复BootLoad菜单密码为缺省值。

您可以在《S系列交换机缺省帐号与密码》（**企业网**、**运营商**）文档中获取各种缺省帐号与密码信息。获取该文档需要权限，如需升级权限，请查看网站帮助。

操作步骤

- 在BootLoad主菜单下，选择5，进入密码子菜单。

```
      BootLoad
Menu
   1. Boot with default mode
   2. Enter startup submenu
   3. Enter ethernet submenu
   4. Enter filesystem submenu
   5. Enter password submenu
   6. Clear password for console user
   7. Reboot
  (Press Ctrl+E to enter diag menu)

Enter your choice(1-7):5
      PASSWORD  SUBMENU

   1. Modify bootload password
   2. Reset bootload password
   3. Return to main menu

Enter your choice(1-3):
```

- 在密码子菜单下，选择2，进入恢复BootLoad菜单密码界面。

```
      PASSWORD  SUBMENU

   1. Modify bootload password
   2. Reset bootload password
   3. Return to main menu

Enter your choice(1-3): 2

The password used to enter the boot menu will be restored to the default password, continue? [Y/N]y
Old password:
Succeeded in setting boot password to default.
```

----结束

11.7 清除 Console 登录密码 Clear password for console user

背景信息

如果用户忘记Telnet登录和Console登录密码，此时会导致设备始终无法登录。为此设置了保险措施，在BootLoad菜单下提供清除Console登录密码功能。

说明

多台设备堆叠情况下，在console口密码未知时，只有清除了主交换机的Console口密码才能正常登录堆叠系统。建议清除Console口密码时，逐台启动成员设备并对每台设备都做清除操作。

操作步骤

- 在BootLoad主菜单下，选择6，清除Console登录密码。

```
    BootLoad Menu

  1. Boot with default mode
  2. Enter startup submenu
  3. Enter ethernet submenu
  4. Enter filesystem submenu
  5. Enter password submenu
  6. Clear password for console user
  7. Reboot
 (Press Ctrl+E to enter diag menu)

Enter your choice(1-7): 6

Note: Clear password for console user? Yes or No(Y/N): y
Clear password for console user successfully.
Note: Choose "1. Boot with default mode" to boot, then set a new password.


Note: If the device is restarted during startup, you need to perform this operation again.
```

须知

清除Console密码后，注意选择BootLoad主菜单下的“1. Boot with default mode”进行启动，不能选择“7. Reboot”，也不能掉电，否则配置将会失效。

----结束

11.8 BootLoad 诊断菜单

在BootLoad主菜单中按下快捷键Ctrl+E进入诊断菜单。

须知

诊断菜单主要用于设备生产和组装过程中调试设备性能，不建议用户使用，如果使用，请在技术人员指导下使用。

您可以在《S系列交换机缺省帐号与密码》（企业网、运营商）文档中获取各种缺省帐号与密码信息。获取该文档需要权限，如需升级权限，请查看网站帮助。

BootLoad 诊断菜单

进入诊断菜单的方法 。

```
Press Ctrl+B to enter BootLoad menu: 2
password:         //输入BootLoad密码


      BootLoad Menu

   1. Boot with default mode
   2. Enter startup submenu
   3. Enter ethernet submenu
   4. Enter filesystem submenu
   5. Enter password submenu
   6. Clear password for console user
   7. Reboot
  (Press Ctrl+E to enter diag menu)//按下快捷键Ctrl+E，进入诊断菜单

Enter your choice(1-7):
```

不同款型显示不同，请以设备实际显示为准。

- 示例一：

```
**********************************************************************
* You have entered Engineering Mode. In this mode, any operation
*
* may cause irreversible damage to the device. Please note.
*
**********************************************************************


      DIAG  MENU

    1. Reserved
    2. E-Label barcode and MAC test
    3. Return to main menu

Enter your choice(1-3):
```

- 示例二：

```
**********************************************************************
* You have entered Engineering Mode. In this mode, any operation *
* may cause irreversible damage to the device. Please note!      *
**********************************************************************


      DIAG  MENU

    1. Equip test
    2. Reserved
    3. Reserved
    4. Reserved
    5. Reserved
    6. Reserved
    7. Aging test
    8. E-Label barcode and MAC test
    9. Reserved
   10. Reserved
```

```
   11. Image test
   12. Return to main menu
Enter your choice(1-12):
```

表 11-11 BootLoad 诊断菜单介绍

项目	描述
Reserved	预留项。
Aging test	进入老化测试子菜单。此菜单主要用来检测设备的存储器、内存以及CPU协议栈的读写功能是否正常。
E-Label barcode and MAC test	进入电子标签和MAC测试子菜单。此菜单主要用来查看设备的电子标签、PCB版本和子卡类型等信息。
Image test	进入镜像测试子菜单。
Return to main menu	返回BootLoad主菜单。

老化测试子菜单 Aging test

在诊断菜单中，选择“7”，进入老化测试子菜单。

```
      DIAG  MENU

   1. Reserved
   2. Reserved
   3. Reserved
   4. Reserved
   5. Reserved
   6. Reserved
   7. Aging test
   8. E-Label barcode and MAC test
   9. Reserved
  10. Reserved
  11. Image test
  12. Return to main menu

Enter your choice(1-12): 7

      AGING TEST Submenu

   1. Set aging flag
   2. Get aging flag
   3. Clear aging flag
   4. Display aging result
   5. Return to upper menu

Enter your choice(1-5):
```

表 11-12 老化测试子菜单介绍

项目	描述
Set aging flag	设置老化测试标志。
Get aging flag	获取老化测试标志。

项目	描述
Clear aging flag	清除老化测试标志。
Display aging result	显示老化测试结果。
Return to upper menu	返回上一级菜单。

电子标签和 MAC 测试子菜单 E-Label barcode and MAC test

根据设备实际显示，在诊断菜单中选择“2”或“8”，进入电子标签和MAC测试子菜单。

- 示例一：

```
      DIAG  MENU

   1. Reserved
   2. E-Label barcode and MAC test
   3. Return to main menu

Enter your choice(1-3): 2

      E-LABEL and MAC TEST Submenu

   1. Read E-lable test
   2. Read MAC address
   3. Read ict barcode
   4. Return to upper menu

Enter your choice(1-4):
```

- 示例二：

```
      DIAG  MENU

   1. Reserved
   2. Reserved
   3. Reserved
   4. Reserved
   5. Reserved
   6. Reserved
   7. Aging test
   8. E-Label barcode and MAC test
   9. Reserved
  10. Reserved
  11. Image test
  12. Return to main menu

Enter your choice(1-12): 8

      E-LABEL and MAC TEST Submenu

   1. Read E-lable test
   2. Reserved
   3. Reserved
   4. Read MAC address
   5. Reserved
   6. Read ict barcode
   7. Reserved
   8. Reserved
   9. Reserved
  10. Reserved
  11. Return to upper menu

Enter your choice(1-11):
```


表 11-13 电子标签和 MAC 测试子菜单介绍

项目	描述
Read E-lable test	显示设备的电子标签。按照设备的组件进行显示，可以分别显示主板、插卡、风扇、POE DIMM条、电源等组件的电子标签。
Reserved	保留项。
Read MAC address	显示设备的MAC地址。
Read ict barcode	显示Barcode信息。
Return to upper menu	返回上一级菜单。

镜像测试子菜单 Image test

在诊断菜单中，选择“11”，进入镜像测试子菜单。

```
      DIAG  MENU

   1. Reserved
   2. Reserved
   3. Reserved
   4. Reserved
   5. Reserved
   6. Reserved
   7. Aging test
   8. E-Label barcode and MAC test
   9. Reserved
  10. Reserved
  11. Image test
  12. Return to main menu

Enter your choice(1-12): 11

      IMAGE TEST SUBMENU

   1. Reserved
   2. Reserved
   3. Reserved
   4. Reserved
   5. Reserved
   6. Return to upper menu

Enter your choice(1-6):
```

表 11-14 镜像测试子菜单介绍

项目	描述
Reserved	保留项。
Return to upper menu	返回上一级菜单。

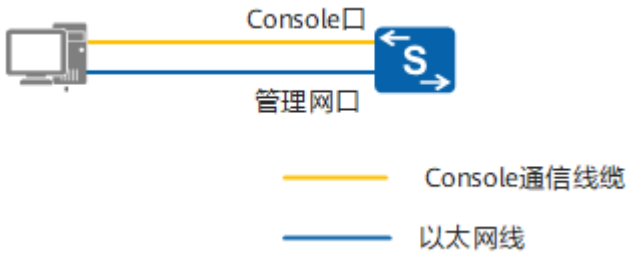
11.9 通过 BootLoad 菜单升级系统软件

组网需求

如图11-1所示，用户PC的串口与设备的Console口连接，用户PC的网口与设备的管理网口相连，用户通过终端仿真软件登录设备。

现在设备的系统软件损坏，无法登录设备。利用uBoot程序的以太网菜单功能，上传系统软件，并设置为设备的启动文件，完成对设备系统软件的加载和升级。

图 11-1 通过 Console 口连接设备组网图



说明

本例中以超级终端作为终端仿真软件举例，其他终端仿真软件的操作请参考其使用说明。

配置思路

1. 在准备使用BootLoad菜单升级系统软件前，需要设置FTP服务器，并将目标系统软件上传至FTP工作目录。本例中设置PC为FTP服务器。
2. 重启设备，进入BootLoad主菜单。
3. 设置设备的FTP参数，实现设备与FTP服务器互通，将目标系统软件通过FTP协议上传至设备的存储器。
4. 上传后的系统软件，设备并不会以此来进行启动，需在修改以太网参数下指定上传的系统软件为设备启动文件。

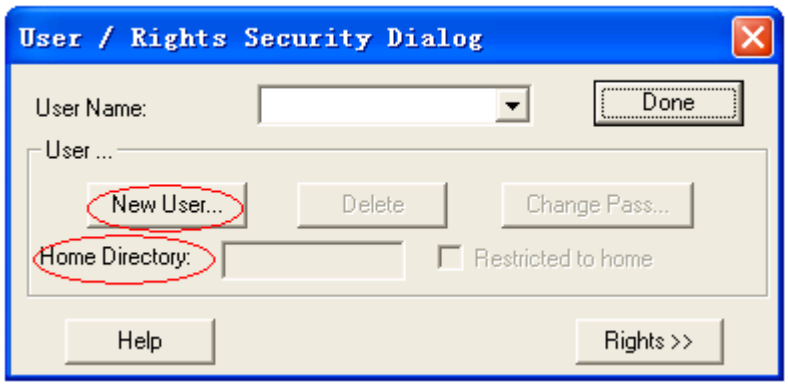
操作步骤

步骤1 设置PC为FTP服务器，并将设备的系统软件拷贝至FTP工作目录。

配置FTP服务器的IP地址、用户名、密码及工作目录。

如图11-2所示，在PC上运行FTP Server程序（以wftpd32为例介绍），依次选择菜单“Security”->“Users/rights...”。在弹出的对话框中单击“New User...”设置用户名为**user**和密码**huawei**。在“Home Directory:”处设置PC上FTP的工作目录为D:\BootLoad。然后单击“Done”按钮完成设置并关闭对话框。配置PC的IP地址为192.168.1.6，掩码为255.255.255.0。

图 11-2 配置 FTP 服务器



将系统软件上传至FTP服务器的工作目录D:\BootLoad上（上传步骤略），例如上传的系统软件为S5732-H-V200R022C00.cc。

步骤2 重启设备，待界面出现如下显示信息时，按下Ctrl+B，输入密码后，进入BootLoad菜单。

您可以在《S系列交换机缺省帐号与密码》（**企业网**、**运营商**）文档中获取各种缺省帐号与密码信息。获取该文档需要权限，如需升级权限，请查看网站帮助。

```
Press Ctrl+B to enter BootLoad menu : 2

Password:      //输入BootLoad密码
      BootLoad Menu

   1. Boot with default mode
   2. Enter startup submenu
   3. Enter ethernet submenu
   4. Enter filesystem submenu
   5. Enter password submenu
   6. Clear password for console user
   7. Reboot
  (Press Ctrl+E to enter diag menu)

Enter your choice(1-7):
```

步骤3 设置设备的FTP参数，建立FTP连接。

在BootLoad主菜单下选择3，进入以太网子菜单。

```
      BootLoad Menu

   1. Boot with default mode
   2. Enter startup submenu
   3. Enter ethernet submenu
   4. Enter filesystem submenu
   5. Enter password submenu
   6. Clear password for console user
   7. Reboot
  (Press Ctrl+E to enter diag menu)

Enter your choice(1-7): 3

      ETHERNET  SUBMENU

   1. Download file to Flash through ethernet interface
   2. Modify ethernet interface boot parameter
   3. Return to main menu
```

```
Enter your choice(1-3):
```

在以太网子菜单下，选择2，进入修改以太网参数菜单。

```
      ETHERNET  SUBMENU

    1. Download file to Flash through ethernet interface
    2. Modify ethernet interface boot parameter
    3. Return to main menu

Enter your choice(1-3): 2

      BOOTLINE  SUBMENU

    1. Set TFTP protocol parameters
    2. Set FTP protocol parameters
    3. Set SFTP protocol parameters
    4. Return to ethernet menu

Enter your choice(1-4):
```

在修改以太网参数菜单下选择2，进入FTP协议参数设置菜单，配置网络参数和需要下载的系统软件名。

```
      BOOTLINE  SUBMENU

    1. Set TFTP protocol parameters
    2. Set FTP protocol parameters
    3. Set SFTP protocol parameters
    4. Return to ethernet menu

Enter your choice(1-4): 2

'.' = clear field;  '-' = go to previous field;  'Ctrl+D' = quit

Load File name      : S5732-HV200R022C00.cc   //输入待上传的系统软件
Switch IP address   : 192.168.1.2   //输入设备的管理网口IP地址
Server IP address   : 192.168.1.6   //输入FTP服务器的IP地址
FTP User Name       : user   //输入FTP服务器的用户名
FTP User Password   :   //输入FTP服务器的登录密码
```

步骤4 参数修改完成后，退出修改以太网参数菜单。在以太网子菜单中选择1，将需要加载的系统软件加载到Flash中。

```
      BOOTLINE  SUBMENU

    1. Set TFTP protocol parameters
    2. Set FTP protocol parameters
    3. Set SFTP protocol parameters
    4. Return to ethernet menu

Enter your choice(1-4): 4

      ETHERNET  SUBMENU

    1. Download file to Flash through ethernet interface
    2. Modify ethernet interface boot parameter
    3. Return to main menu

Enter your choice(1-3): 1

Use ftp to download file : S5732-HV200R022C00.cc , please wait for a moment.
.................
Download file successfully.
```

步骤5 退出以太网子菜单，在BootLoad主菜单中选择“2. Enter startup submenu”，设置加载的系统软件为设备的启动文件。

```
      ETHERNET  SUBMENU

    1. Download file to Flash through ethernet interface
```



```
    2. Modify ethernet interface boot parameter
    3. Return to main menu

Enter your choice(1-3): 3

      BootLoad Menu

    1. Boot with default mode
    2. Enter startup submenu
    3. Enter ethernet submenu
    4. Enter filesystem submenu
    5. Enter password submenu
    6. Clear password for console user
    7. Reboot
   (Press Ctrl+E to enter diag menu)

Enter your choice(1-7): 2

      Startup Configuration Submenu

    1. Display startup configuration
    2. Modify startup configuration
    3. Return to main menu

Enter your choice(1-3): 2

Note: startup file field can not be cleared
'.'=clear field; '^D'=quit; Enter=use current configuration

startup type(1: Flash)
  current: 1
  new    :  //无需设置，直接回车

Flash startup file (can not be cleared)
  current: s5732-h-V200R022C00SPC100B310.cc
  new    : s5732-hV200R022C00.cc    //设置为下次启动的系统软件

patch package
  current:
  new    :  //无需设置，直接回车
```

步骤6 退出启动配置信息菜单，在BootLoad主菜单中选择“1. Boot with default mode”，启动设备。

```
      Startup Configuration Submenu

    1. Display startup configuration
    2. Modify startup configuration
    3. Return to main menu

Enter your choice(1-3): 3

      BootLoad Menu

    1. Boot with default mode
    2. Enter startup submenu
    3. Enter ethernet submenu
    4. Enter filesystem submenu
    5. Enter password submenu
    6. Clear password for console user
    7. Reboot
   (Press Ctrl+E to enter diag menu)

Enter your choice(1-7): 1
```

步骤7 检查配置结果。

设备启动完成后，在命令行界面使用**display version**命令查看设备是否升级到目标版本。

从回显中可以看出，当前设备的系统软件版本为**V200R022C00**，配置成功。

----结束

