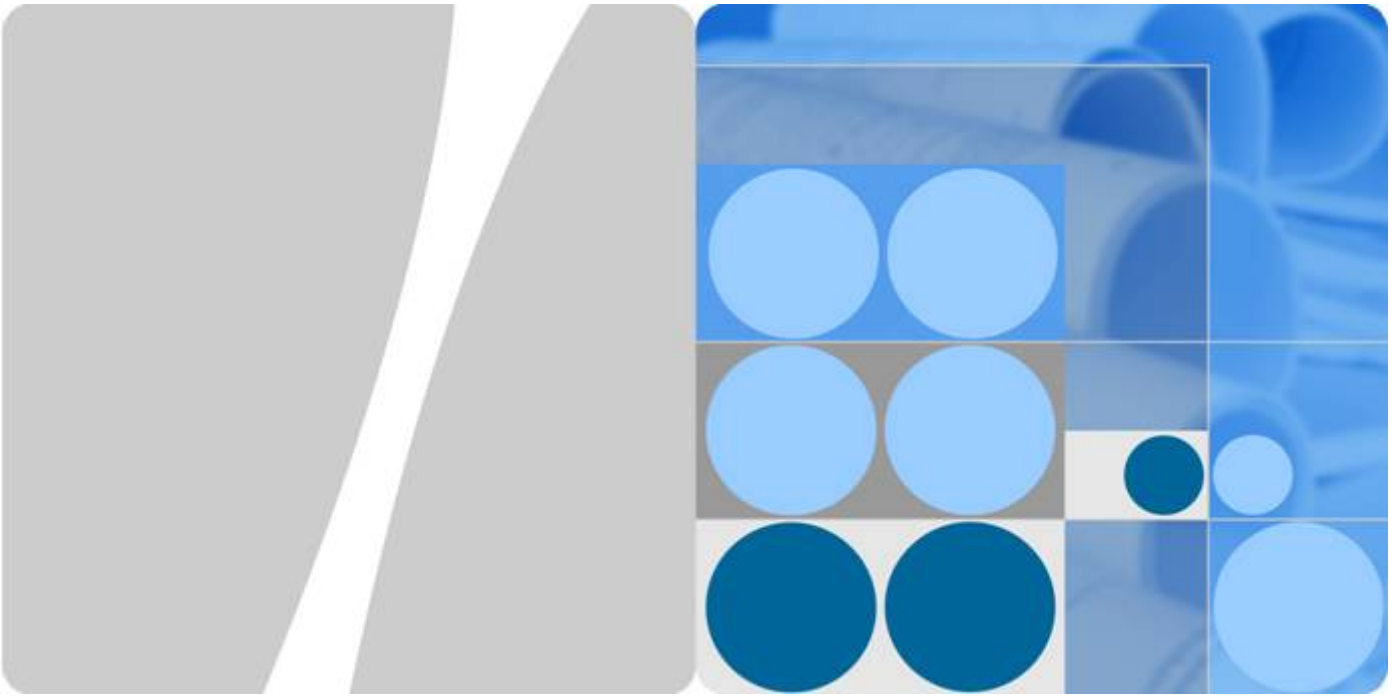


Huawei AR3200 系列企业路由器

V200R002C01

配置指南-基础配置

文档版本　01

发布日期　2012-04-20

华为技术有限公司

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默示的声明或保证。

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： http://www.huawei.com

客户服务邮箱： support@huawei.com

客户服务电话： 4008302118

前 言

读者对象

本文档介绍了 AR3200 中基础配置的基本概念、在不同应用场景中的配置过程和配置举例。

本文档提供了基础配置的配置方法。

本文档主要适用于以下工程师：

- 数据配置工程师
- 调测工程师
- 网络监控工程师
- 系统维护工程师

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
危险	以本标志开始的文本表示有高度潜在危险，如果不能避免，会导致人员死亡或严重伤害。
警告	以本标志开始的文本表示有中度或低度潜在危险，如果不能避免，可能导致人员轻微或中等伤害。
注意	以本标志开始的文本表示有潜在风险，如果忽视这些文本，可能导致设备损坏、数据丢失、设备性能降低或不可预知的结果。
窍门	以本标志开始的文本能帮助您解决某个问题或节省您的时间。
说明	以本标志开始的文本是正文的附加信息，是对正文的强调和补充。

命令行格式约定

格式	意义
粗体	命令行关键字（命令中保持不变、必须照输的部分）采用**加粗**字体表示。
斜体	命令行参数（命令中必须由实际值进行替代的部分）采用*斜体*表示。
[ ]	表示用“[ ]”括起来的部分在命令配置时是可选的。
{ x | y | ... }	表示从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&前面的参数可以重复 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。

修订记录

修改记录累积了每次文档更新的说明。最新版本的文档包含以前所有文档版本的更新内容。

文档版本 01 (2012-04-20)

第一次正式发布。

目 录

1 首次登录系统

关于本章

用户通过 Console 口、Mini USB 口首次登录一台新的路由器，实现对新设备的基本配置。

1.1 首次登录系统简介
当用户需要为第一次上电的设备进行配置时，必须通过 Console 口、MiniUSB 口登录设备。

1.2 通过 Console 口登录路由器
通过 Console 口连接终端与路由器，搭建配置环境。

1.3 通过 MiniUSB 口登录路由器
通过 MiniUSB 口连接终端与路由器，搭建配置环境。

1.1 首次登录系统简介

当用户需要为第一次上电的设备进行配置时，必须通过 Console 口、MiniUSB 口登录设备。

一块主控板提供一个 Console 口（端口类型为 EIA/TIA-232 DCE）、一个 MiniUSB 口。通过将用户终端的串行端口与设备 Console 口直接连接，或者将用户终端的 USB 口与设备 MiniUSB 口直接连接，实现对设备的本地配置。

说明

- 在通过 MiniUSB 口登录设备前，需要在用户终端安装 MiniUSB 接口的驱动程序。
- 同一时刻，MiniUSB 端口和 Console 口只有一个可以使用。

1.2 通过 Console 口登录路由器

通过 Console 口连接终端与路由器，搭建配置环境。

1.2.1 建立配置任务

在进行通过 Console 口登录路由器配置前了解此特性的应用环境、配置此特性的前置任务和数据准备，有助于快速、准确地完成配置任务。

应用环境

当路由器第一次上电，需要对此路由器进行配置和管理时，可以通过 Console 口登录。

前置任务

在配置通过 Console 口配置路由器之前，需要完成以下任务：

- PC 已安装终端仿真程序（如 Windows XP 的超级终端）
- 准备好 Console 通信电缆

数据准备

在通过 Console 口配置路由器之前，需要准备以下数据。

序号	数据
1	终端通信参数（包括波特率、数据位、奇偶校验、停止位和流量控制）

说明

首次登录路由器，终端通信参数均使用路由器的缺省值。

1.2.2 建立物理连接

使用配置电缆将路由器的 Console 口与终端 COM 口进行物理连接。

操作步骤

步骤 1 所有设备上电，自检正常。

步骤 2 使用配置电缆将 PC 的 COM 口和路由器的 Console 口连接。

----结束

1.2.3 登录路由器

通过 Console 口从 PC 登录设备，实现对第一次上电的设备进行配置和管理。

背景信息

用户需要根据设备上所配置的 Console 口的物理属性（包括传输速率、数据位、校验方式、停止位、流控方式），来配置终端登录时的相关参数。由于是首次登录设备，终端属性的各参数值均为设备的缺省值。

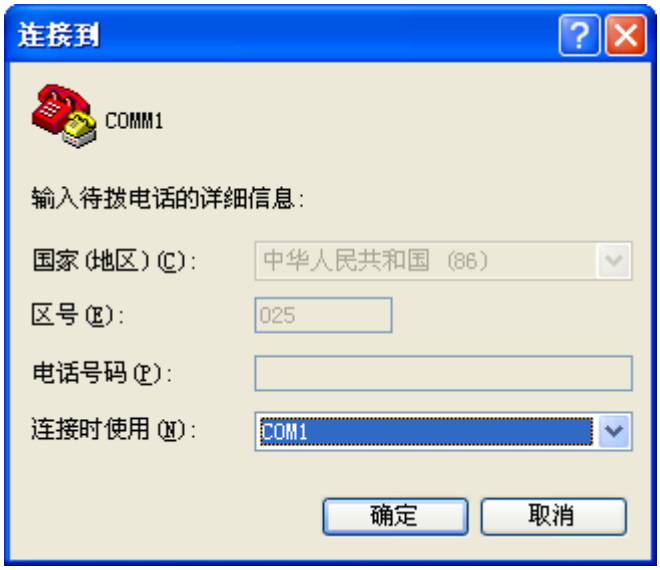
操作步骤

步骤 1 在 PC 上打开终端仿真程序（如 Windows XP 的超级终端），如图 1-1 新建一个连接。

图 1-1 新建连接

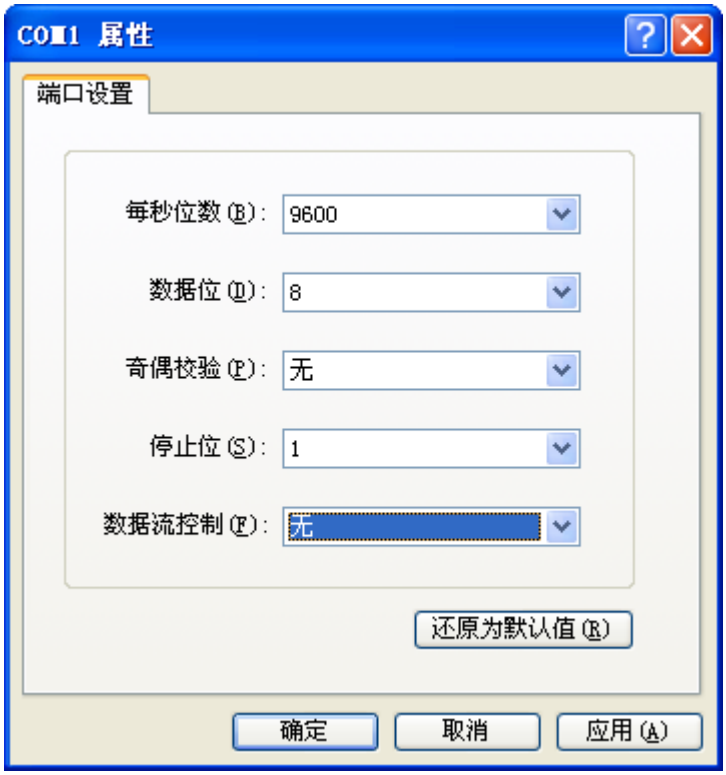
步骤 2 设置连接端口，如图 1-2。

图 1-2 连接端口设置



步骤 3 设置端口通信参数，与设备的缺省值保持一致，如图 1-3。

图 1-3 端口通信参数设置



步骤 4 按 Enter 键，直到系统出现如下显示，提示用户配置验证密码，系统会自动保存此密码配置。

```
Please configure the login password (maximum length 16)
Enter Password:
Confirm Password:
```

说明

- 如果设备出厂时已有初始密码，请输入初始密码“Admin@huawei.com”进入系统，但此密码不是安全密码，请及时修改，修改方法请参见 **4.2.5 配置 Console 用户界面的用户验证方式**。
- 用户界面密码配置成功后，当用户采用密码验证方式通过此界面再次登录系统时，用户验证密码即为初次登录时所配置的验证密码。
- 用户通过 Console 口登录新出厂（或没有启动配置文件）的 AR3200 时，系统会提示：“Auto-Config is working. Before configuring the device, stop Auto-Config. If you perform configurations when Auto-Config is running, the DHCP, routing, DNS, and VTY configurations will be lost. Do you want to stop Auto-Config? [y/n]:”，
  - 如果需要进行 Auto-Config，选择 n，并回车；
  - 如果不需要进行 Auto-Config，选择 y，并回车；

注意

如果不需要进行 Auto-Config，但选择的是 n，会导致后续配置的 dhcp、路由、dns 和 vty 用户配置丢失。

----结束

1.3 通过 MiniUSB 口登录路由器

通过 MiniUSB 口连接终端与路由器，搭建配置环境。

1.3.1 建立配置任务

在进行通过 MiniUSB 口登录路由器配置前了解此特性的应用环境、配置此特性的前置任务和数据准备，有助于快速、准确地完成配置任务。

应用环境

当路由器第一次上电进行配置和管理时，若 PC 端没有 COM 接口，无法通过路由器的 Console 口登录，您可以使用 MiniUSB 口登录路由器。

前置任务

在配置通过 MiniUSB 口配置路由器之前，需要完成以下任务：

- PC 已安装终端仿真程序（如 Windows XP 的超级终端）
- 准备好 MiniUSB 线缆

数据准备

在通过 MiniUSB 口配置路由器之前，需要准备以下数据。

序号	数据
1	终端通信参数（包括波特率、数据位、奇偶校验、停止位和流量控制）

1.3.2 建立物理连接

使用 MiniUSB 线缆将路由器的 MiniUSB 口与 PC 的 USB 口建立物理连接。

操作步骤

步骤 1 所有设备上电，自检正常。

步骤 2 使用 MiniUSB 线缆将 PC 的 USB 口和路由器的 MiniUSB 口连接。

----结束

1.3.3 安装路由器驱动程序

在 PC 端安装路由器驱动程序，使 PC 端可以发现并识别 AR3200。

背景信息

此驱动程序仅支持 Windows XP/VISTA/7 操作系统。

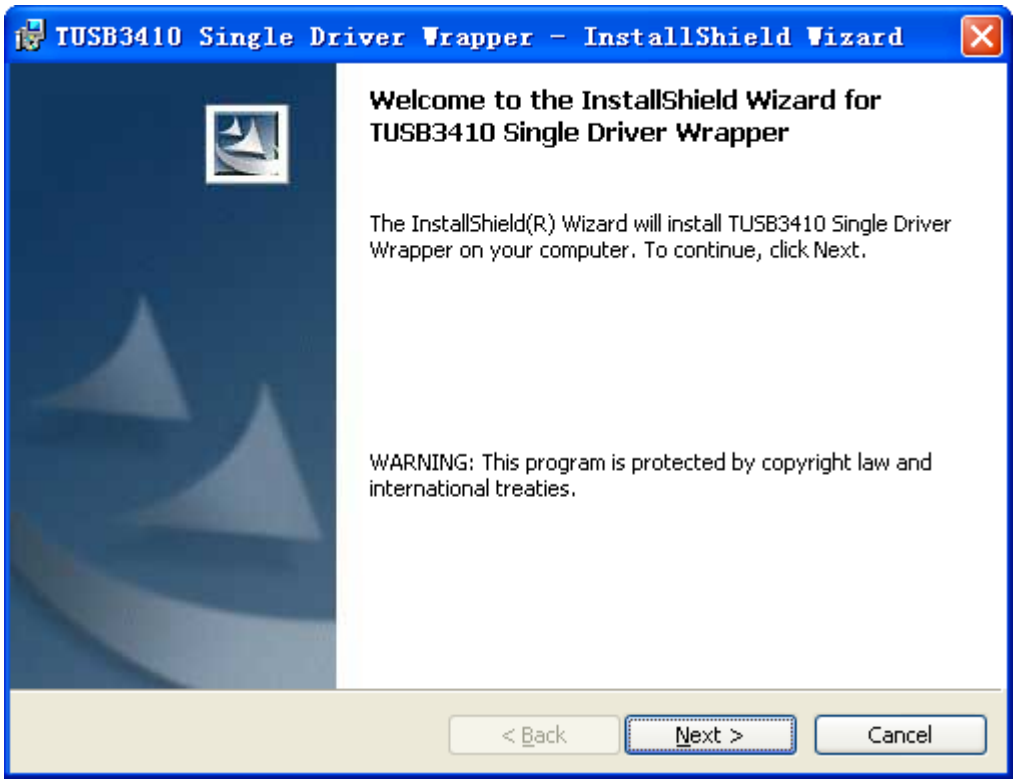
说明

请从“华为技术支持网站（**http://support.huawei.com**）>软件中心>版本软件>数通>路由器>AR1200&2200&3200>AR3200>AR3200 V200R001C01SPC200”路径下获取驱动程序**AR_MiniUSB_driver_1_0**。

操作步骤

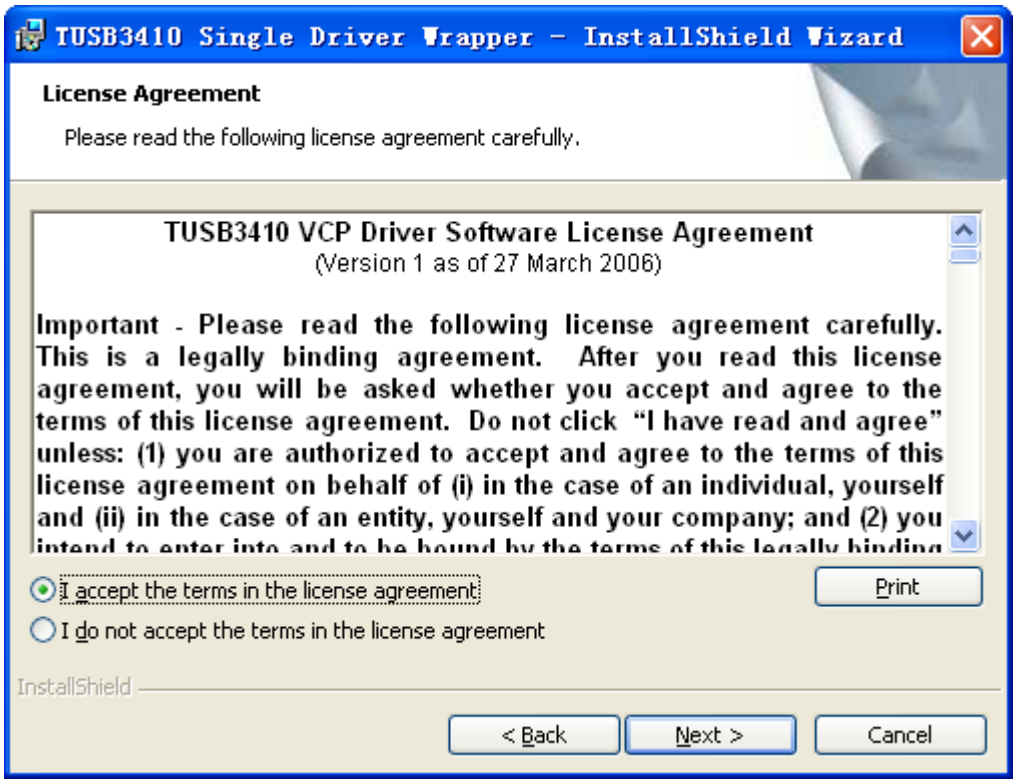
步骤 1 在 PC 端双击驱动程序的安装文件并点击“Next”，如图 1-4 所示。

图 1-4 PC 端运行驱动程序



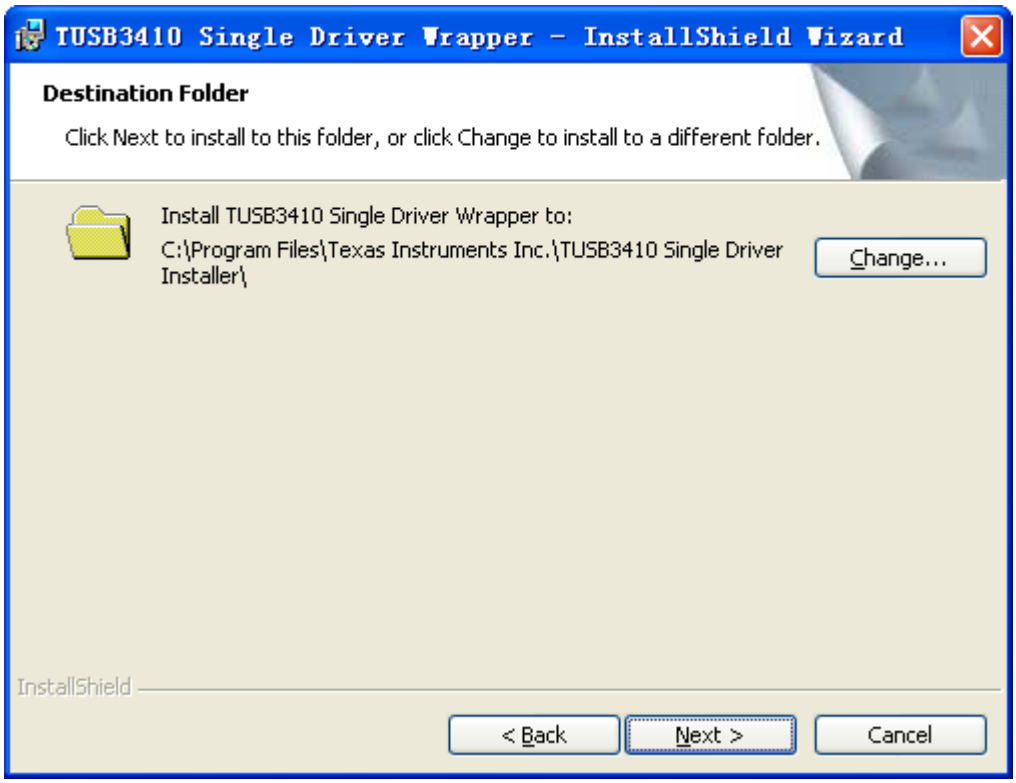
步骤 2 选择“I accept the terms in the license agreement”并点击“Next”，如图 1-5。

图 1-5 接受软件协议条款



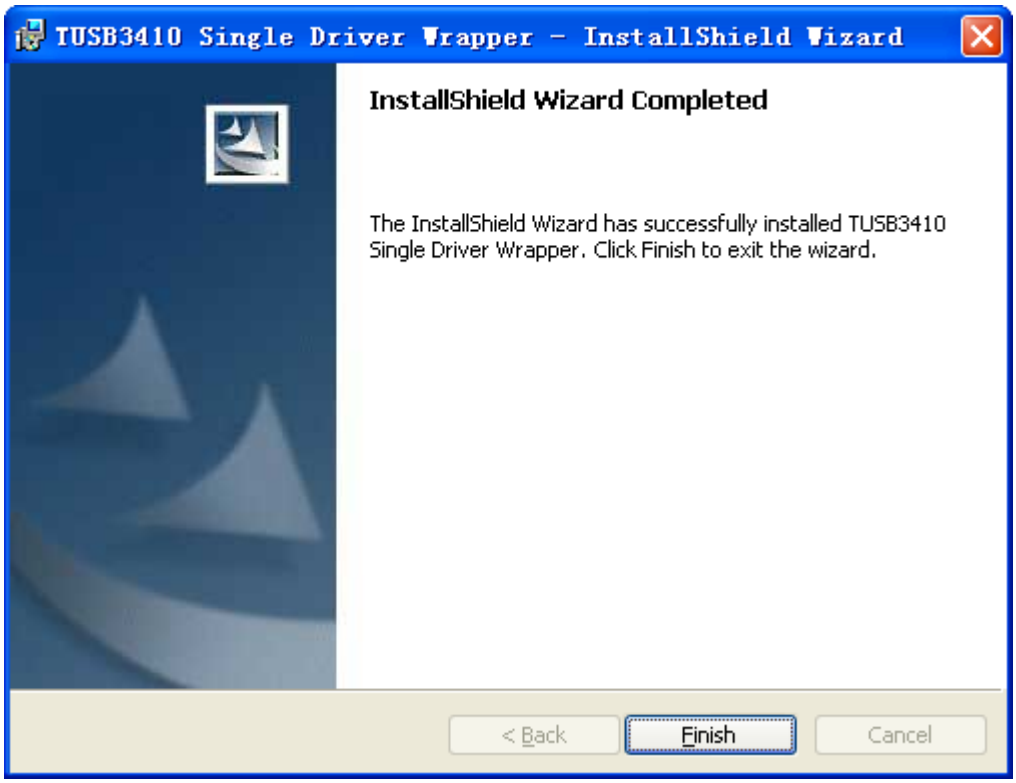
步骤 3 点击“Change”可以更改驱动解压的路径，然后点击“Next”，如图 1-6 所示。

图 1-6 选择驱动解压路径



步骤 4 点击“Install”后进行解压，完成后点击“Finish”结束解压，如图 1-7 所示。

图 1-7 完成驱动的解压



步骤 5 在刚才指定的解压路径下找到“DISK1”文件夹，进入找到“setup.exe”图标并双击。

步骤 6 点击“下一步”，选择“我接受许可证协议中的条款”项并点击“下一步”进入驱动安装。

步骤 7 点击“完成”结束驱动程序的安装。

步骤 8 鼠标右键点击“我的电脑”，单击“管理”->“设备管理器”->“端口（COM 和 LPT）”，可以看到一个“TUSB3410 Device (COM3)”的设备即为路由器。

说明

如果在设备管理器中没有找过“TUSB3410 Device (COM3)”的设备，请重新安装驱动或者更换 MiniUSB 线缆重新连接。

----结束

1.3.4 登录路由器

通过 MiniUSB 口从 PC 登录设备，实现对第一次上电的设备进行配置和管理。

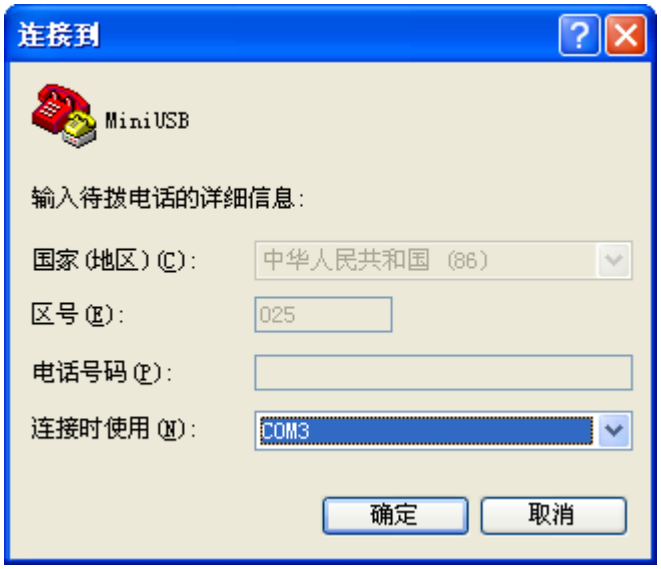
操作步骤

步骤 1 在 PC 上打开终端仿真程序（如 Windows XP 的超级终端），如图 1-8 新建一个连接。

图 1-8 新建连接

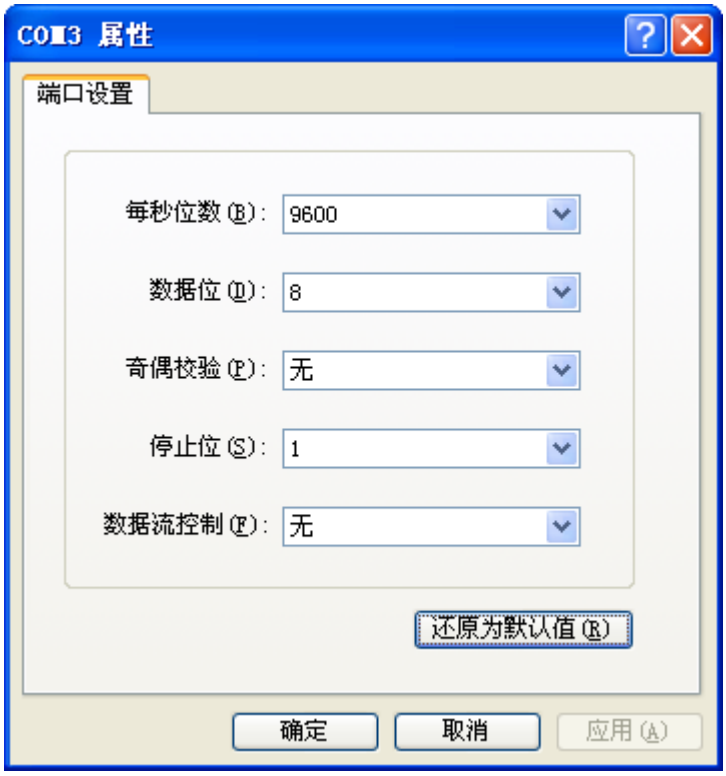
步骤 2 设置连接端口，MiniUSB 口请选择“COM3”，如图 1-9。

图 1-9 连接端口设备



步骤 3 设置端口通信参数，点击“还原为默认值”保持参数与路由器的缺省配置一致，如图 1-10。

图 1-10 端口通信参数设置



步骤 4 按 Enter 键，直到系统出现如下显示，提示用户配置验证密码，系统会自动保存此密码配置。

```
Please configure the login password (maximum length 16)
Enter Password:
Confirm Password:
```

说明

- 如果设备出厂时已有初始密码，请输入初始密码“Admin@huawei.com”进入系统，但此密码不是安全密码，请及时修改，修改方法请参见 **4.2.5 配置 Console 用户界面的用户验证方式**。
- 用户界面密码配置成功后，当用户采用密码验证方式通过此界面再次登录系统时，用户验证密码即为初次登录时所配置的验证密码。
- 用户通过 Console 口登录新出厂（或没有启动配置文件）的 AR3200 时，系统会提示：“Auto-Config is working. Before configuring the device, stop Auto-Config. If you perform configurations when Auto-Config is running, the DHCP, routing, DNS, and VTY configurations will be lost. Do you want to stop Auto-Config? [y/n]:”，
  - 如果需要进行 Auto-Config，选择 n，并回车；
  - 如果不需要进行 Auto-Config，选择 y，并回车；

注意

如果不需要进行 Auto-Config，但选择的是 n，会导致后续配置的 dhcp、路由、dns 和 vty 用户配置丢失。

----结束

2 熟悉命令行

关于本章

用户通过命令行对设备下发各种命令来实现对设备的配置与日常维护操作。

2.1 命令行简介
用户登录到路由器出现命令行提示符后，即进入命令行接口 CLI（Command Line Interface），命令行接口是用户与路由器进行交互的常用工具。

2.2 在线帮助
当用户在输入命令行或进行配置业务时，可以使用在线帮助以获取在配置手册之外的实时帮助。

2.3 命令行特性
命令行提供以下特性，可以帮助用户灵活方便地使用命令行。

2.4 快捷键
用户可以通过使用系统快捷键或者自定义的快捷键，完成对应命令的输入，简化操作。

2.5 配置举例
通过举例，您可以了解到命令行的基本使用。

2.1 命令行简介

用户登录到路由器出现命令行提示符后，即进入命令行接口 CLI（Command Line Interface），命令行接口是用户与路由器进行交互的常用工具。

2.1.1 命令行接口

通过命令行接口输入命令，用户可以对路由器进行配置和管理。

命令行接口有如下特性：

- 允许通过 Console 口进行本地配置。
- 允许通过 Telnet、SSH 进行本地或远程配置。
- 用 **telnet** 命令直接登录并管理其它路由器。
- 提供 FTP 服务，方便用户上传、下载文件。
- 提供 User-interface 视图，管理各种终端用户的特定配置。
- 命令分级保护，不同级别的用户只能执行相应级别的命令。
- 提供 password 和 AAA 验证方式，确保未授权用户无法侵入路由器，保证系统的安全。
- 用户可以随时键入“?”而获得在线帮助。
- 命令行解释器提供不完全匹配和上下文关联等多种智能命令解析方法，方便用户输入。
- 提供网络测试命令，如 **tracert**、**ping** 等，迅速诊断网络是否正常。
- 提供种类丰富、内容详尽的调试信息，帮助诊断网络故障。
- 提供类似 DosKey 的功能，可以执行某条历史命令。

说明

- 系统可正确执行的命令长度最大为 512 个字符，包括使用不完整格式的情况。不完整格式是指不用输入命令的完整格式，只需输入命令的首个或首几个字符，但要确保输入的不完整格式的命令系统只能匹配到唯一一条命令。比如 **display current-configuration** 命令，可以在命令行中输入 **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。
- 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 512 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。

2.1.2 命令级别

为了设备的安全性，系统将命令进行分级管理，设备管理员可以为不同的用户设置与命令级别相对应的用户级别，从而实现对各个用户的访问权限的限制。

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 2-1 所示。

表 2-1 命令级别

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）、部分 display 命令等。
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，比如管理配置文件中的 display current-configuration 命令和 display saved-configuration 命令是 3 级管理级。各命令的级别请参见《*Huawei AR3200 系列 企业路由器 命令参考*》手册。
2	0、1、2	配置级	业务配置命令，包括路由、各个网络层次的命令，向用户提供直接网络服务。
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、配置文件切换命令、备板控制命令、用户管理命令、命令级别设置命令、系统内部参数设置命令；用于业务故障诊断的 debugging 命令等。

说明

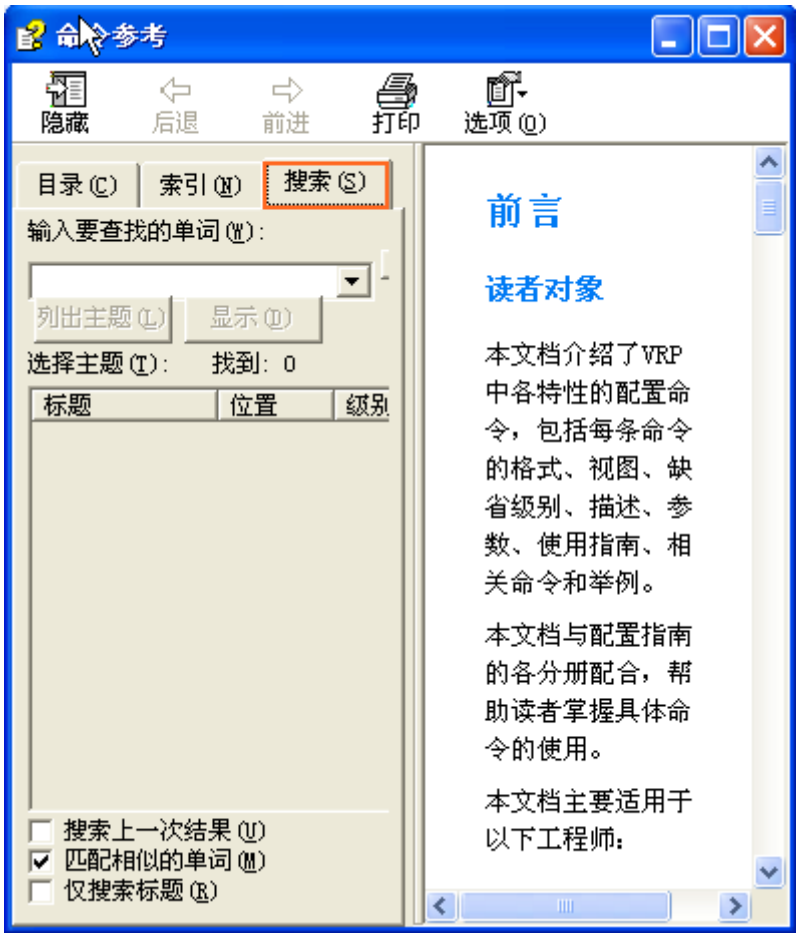
- 实际实现中，根据命令的重要程度，有可能出现某些命令的缺省级别要高于本命令按照命令规则定义所对应的级别。
- 用户可以执行命令的级别由用户的级别决定。
- 登录用户划分为 16 级，与命令级别对应。不同级别的用户登录后，只能使用等于或低于自己级别的命令。可以使用 **user privilege level** *level* 命令设置用户级别。

按级别搜索命令

为了方便使用，用户可以通过命令级别进行命令搜索，即找出同一命令级别下对应的所有命令行信息。具体操作步骤如下：

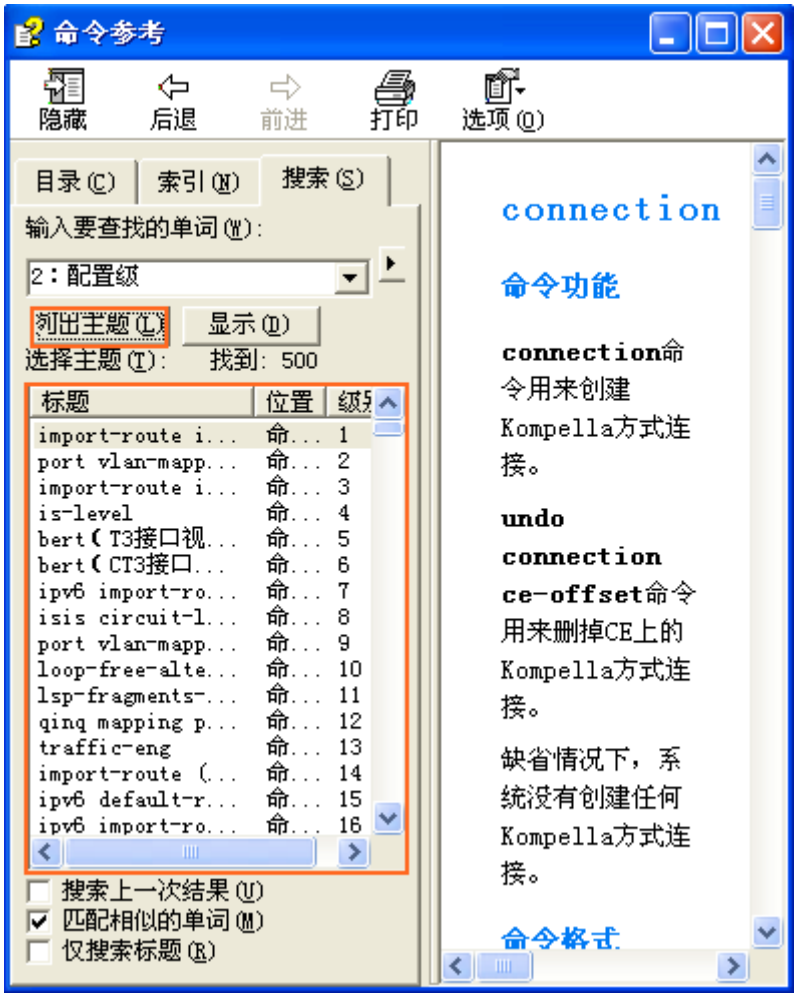
1. 打开命令参考 CHM 文档。
2. 点击“搜索”，并进入搜索页面，详细如图 2-1 所示。

图 2-1 进入搜索页面



3. 在“输入要查找的单词”框中输入需要查找的命令级别，并点击“列出主题”按钮，即可搜索出同一命令级别下对应的所有命令行，详细如图 2-2 所示。

图 2-2 按级别进行命令行搜索



2.1.3 命令视图

命令行接口分为若干个命令视图，所有命令都注册在某个（或某些）命令视图下。通常情况下，必须先进入命令所在的视图才能执行该命令。

下面分别以进入用户视图、系统以及 aaa 视图为例。

与路由器建立连接，如果此路由器是缺省配置，则进入用户视图。

```
<Huawei>
```

键入 **system-view** 后回车，进入系统视图。

```
<Huawei> system-view
[Huawei]
```

在系统视图下键入 **aaa**，则可进入 AAA 视图。

```
[Huawei] aaa
[Huawei-aaa]
```

说明

- 命令行提示符“Huawei”是缺省的主机名。
- 通过提示符可以判断当前所处的视图，例如：“<HUAWEI>”表示用户视图，“[HUAWEI-ui-console0]”表示 Console 用户界面视图。

有些在系统视图下实现的命令，在其它视图下也可以实现，但实现的功能与命令视图密切相关。

2.2 在线帮助

当用户在输入命令行或进行配置业务时，可以使用在线帮助以获取在配置手册之外的实时帮助。

2.2.1 完全帮助

当用户输入命令时，如果不记得此命令的关键字或参数，可以使用命令行的完全帮助获取全部关键字或参数的提示。

操作步骤

- 命令行的完全帮助可以通过以下三种方式获取。
  - 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。

```
<Huawei> ?
User view commands:
arp-ping                        ARP-ping
autosave                        <Group> autosave command group
backup                          Backup  information
cd                              Change current directory
clock                           Specify the system clock
cls                             Clear screen
...
...
```

  - 键入一命令，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] interface ?
Bridge-if                       Bridge-if interface
Cellular                        Cellular interface
...
...
```

    其中“Bridge-if”、“Cellular”是关键字，“Bridge-if interface”和“Cellular interface”是对关键字的分别描述。

  - 键入一命令，后接以空格分隔的“?”，如果该位置为参数，则列出参数取值的说明和参数作用的描述。举例如下：

```
[Huawei] ftp timeout  ?
  INTEGER<1-35791>  The value of FTP timeout (in 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 (in minutes)”是对参数作用的简单描述，<cr>表示该位置无参数，在紧接着的下一个命令行该命令被复述，直接键入回车即可执行。

----结束

2.2.2 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。

操作步骤

- 命令行的部分帮助可以通过以下三种方式获取。
  - 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。

```
<Huawei> d?
debugging                       <Group> debugging command group
delete                          Delete a file
dialer                          Dialer
dir                             List files on a filesystem
display                         Display information
```

  - 键入一命令，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。

```
<Huawei> display b?
  bfd                             Specify BFD(Bidirectional Forwarding Detection
                                  ) configuration information
  bgp                             BGP information
  bootp                           Bootstrap Protocol
  bridge                          <Group> bridge command group
```

  - 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。

----结束

2.2.3 命令行错误信息

所有用户键入的命令，如果通过语法检查，则正确执行，否则系统将会向用户报告错误信息。

常见错误信息参见表 2-2。

表 2-2 命令行常见错误信息表

英文错误信息	错误原因
Error: Unrecognized command found at '^' position.	没有查找到命令
	没有查找到关键字
Error: Wrong parameter found at '^' position.	参数类型错
	参数值越界
Error:Incomplete command found at '^' position.	输入命令不完整
Error: Too many parameters found at "^" position.	输入参数太多
Error:Ambiguous command found at '^' position.	输入命令不明确

2.3 命令行特性

命令行提供以下特性，可以帮助用户灵活方便地使用命令行。

2.3.1 编辑特性

命令行编辑功能有助于用户利用某些特定的键进行命令的编辑或者获得帮助。

AR3200 的命令行接口提供基本的命令编辑功能，支持多行编辑，每条命令最大长度为 512 个字符。

一些常用的编辑功能如表 2-3 所示。

表 2-3 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。
Tab 键	输入不完整的关键字后按下 Tab 键，系统自动执行部分帮助： ● 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； ● 对于不匹配或者匹配的关键字不唯一的情况，首先显示前缀，继续按 Tab 键循环翻词，此时光标距词尾不空格，按空格键输入下一个单词； ● 如果输入错误关键字，按 Tab 键后，换行显示，输入的关键字不变。

2.3.2 显示特性

所有的命令行有共同的显示特性，并且可以根据用户的需求，灵活构建显示方式。

设备上命令行接口提供如下显示特性：

- 在一次显示信息超过一屏时，提供暂停功能，在暂停显示时用户可以有三种选择，如表 2-4 所示。

表 2-4 显示功能表

功能键	功能
键入<Ctrl_C>	停止显示或命令执行。
键入空格键	继续显示下一屏信息。

功能键	功能
键入回车键	继续显示下一行信息。

2.3.3 正则表达式

正则表达式描述了一种字符串匹配的模式，由普通字符（例如字符 a 到 z）和特殊字符（或称“元字符”）组成。正则表达式作为一个模板，将某个字符模式与所搜索的字符串进行匹配。用户可以使用正则表达式来过滤显示信息，方便快速查找到所需要的信息。

正则表达式一般具有以下功能：

- 检查字符串中符合某个规则的子字符串，并可以获取该子字符串。
- 根据匹配规则对字符串进行替换操作。

正则表达式的语法规则

正则表达式由普通字符和特殊字符组成。

- 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、标点符号以及一些特殊符号。例如：a 匹配 abc 中的 a，202 匹配 202.113.25.155，@匹配 xxx@xxx.com 中的@。
- 特殊字符

  特殊字符配合普通字符匹配复杂或特殊的字符串组合。表 2-5 是对特殊字符及其语法意义的使用描述。

表 2-5 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、……

特殊字符	功能	举例
+	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。	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
[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
_	匹配一个逗号（,）、左花括号（{）、右花括号（}）、左圆括号、右圆括号。 匹配输入字符串的开始位置。 匹配输入字符串的结束位置。 匹配一个空格。	_2008_可以匹配 2008、空格 2008 空格、空格 2008、2008 空格、，2008,、{2008}、(2008)、{2008)、(2008}

说明

除非特别说明，上表中涉及到的字符指的是可以打印的字符。

- 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，以上正则表达式包括括号“（）”内包含的子正则表达式。

- 普通字符与特殊字符的组合使用

  实际应用中，往往不是一个普通字符加上一个特殊字符配合使用，而是由多个普通字符和特殊字符组合，匹配某些特征的字符串。

在命令中指定过滤方式

注意

Huawei AR3200 系列采用正则表达式实现管道符的过滤功能。并非所有 display 命令均支持管道符。当显示信息内容很多时，此 display 命令支持管道符；当显示信息内容很少时，此 display 命令不支持管道符。

按过滤条件进行查询时，显示内容的第一行信息中，以包含该字符串的整条信息作为起始，而非过滤字符串作为起始。

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。
- | **exclude** *regular-expression*：输出不匹配指定正则表达式的所有行。
- | **include** *regular-expression*：只输出匹配指定正则表达式的所有行。

说明

regular-expression 为字符串形式，长度范围是 1 ~ 255。且 *regular-expression* 中不能含有“_”。

2.3.4 历史命令

命令行接口提供类似 Doskey 功能，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，可以调用命令行接口保存的历史命令，并重复执行，方便了用户的操作。

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，反而影响了效率。

对历史命令的操作如表 2-6 所示。

表 2-6 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**	显示用户键入的历史命令。
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，否则清空命令，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，这时可以用组合键<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：

- AR3200 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，AR3200 的历史命令中只保留最早的一次。但如果执行时输入的形式不同，将作为不同的命令对待。

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

2.4 快捷键

用户可以通过使用系统快捷键或者自定义的快捷键，完成对应命令的输入，简化操作。

2.4.1 快捷键的分类

在使用快捷键时，会接触到两类快捷键，自定义的快捷键和系统快捷键。了解了分类后，用户可以更快速和准确的使用快捷键。

系统中的快捷键分成两类：

- 提供给用户可以自由定义的快捷键：共有 4 个，包括 CTRL_G、CTRL_L、CTRL_O 和 CTRL_U。用户可以根据自己的需要将这 4 个快捷键与任意命令进行关联，当使用快捷键时，系统自动执行它所对应的命令。定义此类快捷键的方法请参见 **2.4.2 定义快捷键**。
- 系统快捷键：是系统中固定的。这种快捷键不由用户定义，代表固定功能。系统包括的主要快捷键如**表 2-7** 所示。

说明

由于不同的终端软件对于某些键的解释不同，具体终端上实际可用的快捷键与本节所列举的按键组合可能略有差异。

表 2-7 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。
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_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_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（word）。
ESC_D	删除光标右侧的一个字（word）。
ESC_F	将光标向右移动一个字（word）。

2.4.2 定义快捷键

如果用户经常性地使用某一个或某几个命令时，可以将这些命令定义成快捷键，方便用户操作，提升效率。只有管理级用户有定义快捷键的权限。

请在系统视图下进行下列配置。

操作	命令
定义快捷键	**hotkey** { **CTRL_G** | **CTRL_L** | **CTRL_O** | **CTRL_U** } *command-text*

CTRL_G、CTRL_L、CTRL_O 三个快捷键的默认值如下：

- CTRL_G：对应命令 **display current-configuration**
- CTRL_L：对应命令 **undo idle-timeout**
- CTRL_O：对应命令 **undo debugging all**

CTRL_U 快捷键默认值为空。

定义快捷键时，对于由多个命令字组成的命令，即命令中间有空格，需要使用双引号标识。对于单个命令字的命令，即命令中没有空格，不需要使用双引号。

说明

可通过 **undo hotkey** 命令恢复系统的快捷键缺省值。

2.4.3 快捷键的使用

在任何允许输入命令的地方都可以键入快捷键，系统执行时，会将该快捷键对应的命令显示在屏幕上，如同输入了完整的命令一样。

- 如果用户已经输入了命令的一部分，但是还没有键入回车以确认，此时键入快捷键将会把以前输入的字符全部清空，并将该快捷键对应的命令显示在屏幕上，效果与用户删除所有的输入，然后重新敲入完整的命令一样。
- 快捷键的执行与命令一样，也会将命令原形记录在命令缓冲区和日志中以备问题定位和查询。

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路由器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。

可以在任意视图下执行以下命令。

操作	命令
查看快捷键的使用情况	**display hotkey**

2.5 配置举例

通过举例，您可以了解到命令行的基本使用。

2.5.1 Tab 键使用示例

Tab 键使用的示例。在本例中，当用户输入不完整的关键字后按下 Tab 键，可以获得所有相关的关键字，或者检查关键字是否正确。

背景信息

用户一般不需要输入完整的命令关键字，只需要输入关键字的前一个或前几个字符，使用 Tab 键就可以将此关键字补全。方便用户查找以及使用所需要的命令。

操作步骤

- 关于 Tab 键的使用，有如下 3 种情况，分别举例如下：
  - 如果与不完整关键字匹配的关键字唯一
    1. 输入不完整的关键字。

       ```
       [Huawei] info-
       ```

2. 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
   ```

- 如果不匹配或者匹配的关键字不唯一

  # 关键字 **info-center** 后面可以跟如下 3 个前缀是“log”的关键字。

  ```
  [Huawei] info-center log?
    logbuffer                      Setting of log buffer configuration
    logfile                        <Group> logfile command group
    loghost                        Setting of logging host configuration
  ```

  1. 输入不完整的关键字。

     ```
     [Huawei] info-center log
     ```

  2. 按下 Tab 键。

     则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 logbuffer
     ```

     继续按 Tab 键循环翻词，此时光标距词尾不空格。

     ```
     [Huawei] info-center logfile
     [Huawei] info-center loghost
     ```

     如果找到所需要的关键字 **logfile** 后，则停止按 Tab 键。

  3. 按空格键，然后输入下一个关键字 **path**。

     ```
     [Huawei] info-center logfile path
     ```

- 输入错误的关键字后按下 Tab 键（检查关键字是否正确）

  1. 输入不完整的关键字 **loglog**。

     ```
     [Huawei] info-center loglog
     ```

  2. 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。

----结束

2.5.2 定义快捷键示例

自定义快捷键的示例。在本例中，将常用的命令自定义为快捷键，输入命令时只需使用相应的快捷键，方便操作，提升效率。

背景信息

如果登录的路由器上定义了快捷键，那么所有的用户均可以使用，不区分用户级别。

操作步骤

步骤 1 定义快捷键 CTRL_U，与命令 **display local-user** 进行关联，并执行。

```
<Huawei> system-view
[Huawei] hotkey ctrl_u "display local-user"
```

说明

定义快捷键时，对于由多个命令字组成的命令，即命令中间有空格，需要使用双引号标识。对于单个命令字的命令，即命令中没有空格，不需要使用双引号。

步骤 2 在提示符[Huawei]下键入快捷键“Ctrl+U”即显示。

```
[Huawei] display local-user
------------------------------------------------------------------------------
  User-name                      State  AuthMask  AdminLevel
  ------------------------------------------------------------------------------
  admin                          A      H         -
  root                           A      A         -
  ------------------------------------------------------------------------------
  Total 2 user(s)
```

----结束

3 进行基本配置

关于本章

用户登录路由器后，可以对路由器进行基本配置，以符合用户使用习惯或是实际环境的需求。

3.1 配置系统基本环境
用户根据自己的需求，配置以下系统基本环境。

3.2 显示系统基本信息
当用户需要查看当前系统的基本配置信息时，可以使用相应的 display 命令。

3.1 配置系统基本环境

用户根据自己的需求，配置以下系统基本环境。

3.1.1 建立配置任务

在进行系统的基本环境配置前了解此特性的应用环境、配置此特性的前置任务和数据准备，有助于快速、准确地完成配置任务。

应用环境

在配置业务前，用户需要进行系统的基本环境配置，以便符合实际环境的要求。比如系统的时间、设备名称等。

前置任务

在配置系统环境之前，需要完成以下任务：

- 路由器上电自检正常

数据准备

在配置系统环境之前，需要准备以下数据。

序号	数据
1	系统时间
2	主机名称
3	登录信息
4	命令级别

3.1.2 设置设备名称

当网络上有多个设备需要管理时，用户可以为每个设备设置特定的名称，以便于用户登录后识别不同的设备。

背景信息

设备名称更改后立即生效。

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 **sysname** *host-name*，设置设备名称。

缺省情况下，路由器主机名为 Huawei。

设备名称会出现在命令提示符中，用户可以根据需要更改设备名称。

----结束

3.1.3 设置系统时钟

为了保证网络中的设备在同一时钟下协调工作，用户需要准确设置系统时钟。

背景信息

系统时钟是系统信息时间戳显示的时间。由于地域的不同，用户可以根据本国或本地区的规定，自由设置系统时钟。

系统时钟=UTC（Universal Time Coordinated）通用协调时间+时区偏移+夏令时偏移

为了保证与其他设备正常协调工作，用户需要将系统时钟设置准确。

请在用户视图下执行以下操作。

操作步骤

步骤 1 执行命令 **clock datetime** *HH:MM:SS YYYY-MM-DD*，设置当前时间和日期。

说明

当时区为 0 时，通过本命令设置的时间将被认为是 UTC 时间。建议设置当前时间时，务必清楚所在时区，设置正确的 UTC 时间，以保证本地时间正确。

步骤 2 执行命令 **clock timezone** *time-zone-name* { **add** | **minus** } *offset*，设置所在的时区。

- **add** 将在 UTC 标准时间的基础上增加指定的时区偏移量。即，在系统默认的 UTC 时区的基础上，加上 *offset*，就可以得到 *time-zone-name* 所标识的时区时间。
- **minus** 将在 UTC 标准时间的基础上减去指定的时区偏移量。即，在系统默认的 UTC 时区的基础上，减去 *offset*，就可以得到 *time-zone-name* 所标识的时区时间。

步骤 3 执行命令 **clock daylight-saving-time** *time-zone-name* **one-year** *start-time start-date end-time end-date offset* 或 **clock daylight-saving-time** *time-zone-name* **repeating** *start-time* { { **first** | **second** | **third** | **fourth** | **last** } *weekday month* | *start-date* } *end-time* { { **first** | **second** | **third** | **fourth** | **last** } *weekday month* | *end-date* } *offset* [*start-year* [*end-year*]]，设置夏令时。

缺省情况下，系统没有设置夏令时。

配置周期夏令时，夏令时开始时间和结束时间支持日期+日期、星期+星期、日期+星期、星期+日期四种配置方式。配置方法请参考 **clock daylight-saving-time** 命令。

说明

当当前时间处在夏令时时，执行命令 **clock timezone** *time-zone-name* { **add** | **minus** } *offset* 设置时区名是可以成功的。但此时执行命令 **display clock** 显示的时区名为夏令时名，当夏令时结束之后，就会显示之前设置的时区名。

----结束

系统时钟显示

系统时钟由 **clock datetime**、**clock timezone**、**clock daylight-saving-time** 三条命令联合决定。

- 如果以上三条命令都不配置，则执行命令 **display clock** 将显示的是原系统时钟。
- 如果以上三条命令任意组合进行配置，配置后的系统时间如**表 3-1** 所示。

表中举例原系统时间是 2010 年 1 月 1 日 08:00:00。

- 1：表示执行 **clock datetime** 命令，配置了当前时间和日期是 *date-time*。
- 2：表示执行 **clock timezone** 命令，配置了时区参数，时间偏移量是 *zone-offset*。
- 3：表示执行 **clock daylight-saving-time** 命令，配置了夏令时参数，时间偏移量是 *offset*。
- [1]：表示 **clock datetime** 命令是可选配置。

表 3-1 系统时钟配置示例表

操作	配置后的系统时间	举例
1	*date-time*	配置：clock datetime 8:0:0 2011-11-12 配置后的系统时间： 2011-11-12 08:00:03 Saturday Time Zone(DefaultZoneName) : UTC
2	原系统时间±*zone-offset*	配置：clock timezone BJ add 8 配置后的系统时间： 2010-01-01 16:00:20+08:00 Friday Time Zone(BJ) : UTC+08:00
1、2	*date-time*±*zone-offset*	配置：clock datetime 8:0:0 2011-11-12 和 clock timezone BJ add 8 配置后的系统时间： 2011-11-12 16:00:13+08:00 Saturday Time Zone(BJ) : UTC+08:00
[1]、2、1	*date-time*	配置：lock timezone NJ add 8 和 clock datetime 9:0:0 2011-11-12 配置后的系统时间： 2011-11-12 09:00:02+08:00 Saturday Time Zone(NJ) : UTC+08:00
3	原系统时间不在夏令时段内，则为原系统时间	配置：clock daylight-saving-time BJ one-year 6:0 2011-8-1 6:0 2011-10-01 1 配置后的系统时间： 2010-01-01 08:00:51 Friday Time Zone(DefaultZoneName) : UTC Daylight saving time : Name : BJ Repeat mode : one-year Start year : 2011 End year : 2011 Start time : 08-01 06:00:00 End time : 10-01 06:00:00 Saving time : 01:00:00

操作	配置后的系统时间	举例
	原系统时间在夏令时段内，则为原系统时间+*offset*	配置：clock daylight-saving-time BJ one-year 6:0 2011-1-1 6:0 2011-9-1 2 配置后的系统时间： 2010-01-01 10:00:34 DST Friday Time Zone(BJ) : UTC Daylight saving time : Name : BJ Repeat mode : one-year Start year : 2011 End year : 2011 Start time : 01-01 06:00:00 End time : 09-01 06:00:00 Saving time : 02:00:00
1、3	*date-time* 不在夏令时段内，则为 *date-time*	配置 clock datetime 9:0:0 2011-11-12 和 clock daylight-saving-time BJ one-year 6:0 2012-8-1 6:0 2012-10-01 1 配置后的系统时间： 2011-11-12 09:00:26 Saturday Time Zone(DefaultZoneName) : UTC Daylight saving time : Name : BJ Repeat mode : one-year Start year : 2012 End year : 2012 Start time : 08-01 06:00:00 End time : 10-01 06:00:00 Saving time : 01:00:00
	date-time 在夏令时段内，则为 *date-time* +*offset*	配置 clock datetime 9:0:0 2011-11-12 和 clock daylight-saving-time BJ one-year 9:0 2011-11-12 6:0 2011-12-01 2 配置后的系统时间： 2011-11-12 11:02:21 DST Saturday Time Zone(BJ) : UTC Daylight saving time : Name : BJ Repeat mode : one-year Start year : 2011 End year : 2011 Start time : 11-12 09:00:00 End time : 12-01 06:00:00 Saving time : 02:00:00

操作	配置后的系统时间	举例
[1]、3、1	*date-time* 不在夏令时段内，则为 *date-time*	配置 clock daylight-saving-time BJ one-year 6:0 2012-8-1 6:0 2012-10-01 1 和 clock datetime 9:0 2011-11-12 配置后的系统时间： 2011-11-12 09:00:02 Saturday Time Zone(DefaultZoneName) : UTC Daylight saving time : Name : BJ Repeat mode : one-year Start year : 2012 End year : 2012 Start time : 08-01 06:00:00 End time : 10-01 06:00:00 Saving time : 01:00:00
	date-time 在夏令时段内，则为 *date-time*	配置 clock daylight-saving-time BJ one-year 1:0 2011-1-1 1:0 2011-9-1 2 和 clock datetime 3:0 2011-1-1 配置后的系统时间： 2011-01-01 03:00:19 DST Saturday Time Zone(BJ) : UTC Daylight saving time : Name : BJ Repeat mode : one-year Start year : 2011 End year : 2011 Start time : 01-01 01:00:00 End time : 09-01 01:00:00 Saving time : 02:00:00
2、3 或者 3、2	如果原系统时间±*zone-offset* 的值不在夏令时段内，则为原系统时间±*zone-offset*	配置：clock timezone BJ add 8 和 clock daylight-saving-time BJ one-year 6:0 2011-1-1 6:0 2011-9-1 2 配置后的系统时间： 2010-01-01 16:01:29+08:00 Friday Time Zone(BJ) : UTC+08:00 Daylight saving time : Name : BJ Repeat mode : one-year Start year : 2011 End year : 2011 Start time : 01-01 06:00:00 End time : 09-01 06:00:00 Saving time : 02:00:00

操作	配置后的系统时间	举例
	如果原系统时间±*zone-offset* 的值在夏令时段内，则为原系统时间±*zone-offset*±*offset*	配置：clock daylight-saving-time BJ one-year 1:0 2010-1-1 1:0 2010-9-1 2 和 clock timezone BJ add 8 配置后的系统时间： 2010-01-01 18:05:31+08:00 DST Friday Time Zone(BJ) : UTC+08:00 Daylight saving time : Name : BJ Repeat mode : one-year Start year : 2010 End year : 2010 Start time : 01-01 01:00:00 End time : 09-01 01:00:00 Saving time : 02:00:00
1、2、3 或者 1、3、2	如果 *date-time*±*zone-offset* 的值不在夏令时段内，则为 *date-time*±*zone-offset*	配置：clock datetime 8:0:0 2011-11-12、clock timezone BJ add 8 和 clock daylight-saving-time BJ one-year 6:0 2012-1-1 6:0 2012-9-1 2 配置后的系统时间： 2011-11-12 16:01:40+08:00 Saturday Time Zone(BJ) : UTC+08:00 Daylight saving time : Name : BJ Repeat mode : one-year Start year : 2012 End year : 2012 Start time : 01-01 06:00:00 End time : 09-01 06:00:00 Saving time : 02:00:00
	如果 *date-time*±*zone-offset* 的值在夏令时段内，则为 *date-time*±*zone-offset*+*offset*	配置：clock datetime 8:0:0 2011-1-1、clock daylight-saving-time BJ one-year 6:0 2011-1-1 6:0 2011-9-1 2 和 clock timezone BJ add 8 配置后的系统时间： 2011-01-01 18:00:43+08:00 DST Saturday Time Zone(BJ) : UTC+08:00 Daylight saving time : Name : BJ Repeat mode : one-year Start year : 2011 End year : 2011 Start time : 01-01 06:00:00 End time : 09-01 06:00:00 Saving time : 02:00:00

操作	配置后的系统时间	举例
[1]、2、3、1 或者 [1]、3、2、1	*date-time* 不在夏令时段内，则为 *date-time*	配置：clock daylight-saving-time BJ one-year 6:0 2012-1-1 6:0 2012-9-1 2、clock timezone BJ add 8 和 clock datetime 8:0:0 2011-11-12 配置后的系统时间： 2011-11-12 08:00:03+08:00 Saturday Time Zone(BJ) : UTC+08:00 Daylight saving time : Name : BJ Repeat mode : one-year Start year : 2012 End year : 2012 Start time : 01-01 06:00:00 End time : 09-01 06:00:00 Saving time : 02:00:00
	date-time 在夏令时段内，则为 *date-time*	配置：clock timezone BJ add 8、clock daylight-saving-time BJ one-year 1:0 2011-1-1 1:0 2011-9-1 2 和 clock datetime 3:0:0 2011-1-1 配置后的系统时间： 2011-01-01 03:00:03+08:00 DST Saturday Time Zone(BJ) : UTC+08:00 Daylight saving time : Name : BJ Repeat mode : one-year Start year : 2011 End year : 2011 Start time : 01-01 01:00:00 End time : 09-01 01:00:00 Saving time : 02:00:00

3.1.4 设置标题文本

如果用户需要对登录路由器的用户提供警示或说明信息，可以设置登录时或登录成功后的标题文本。

背景信息

标题文本是用户在连接到路由器、进行登录验证以及开始交互配置时系统显示的一段提示信息。

需要为用户登录提供明确的指示信息时，可以使用此配置。

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 **header login** { **information** *text* | **file** *file-name* }，设置登录时的标题文本。

步骤 3 执行命令 **header shell** { **information** *text* | **file** *file-name* }，设置登录成功后的标题文本。

需要在终端连接被激活但用户尚未通过认证时显示标题信息，使用参数 **login**。

需要在用户成功登录后显示标题信息，使用参数 **shell**。

说明

- 标题信息文本以一个英文字符作为起始符，且以相同的字符作为结束符。输入一个英文字符后回车会进入交互过程，输入所需的信息后再输入相同的英文字符，系统自动退出交互过程。
- 使用参数 **file** 时，需要将指定标题所使用的文件存放在默认存储介质的根目录。如果放在其他目录下，请使用全路径，否则将无法配置成功。
- 如果在客户端使用 SSH1.X 版本登录路由器，则用户登录时不显示参数 **login** 设置的标题信息，但可以显示参数 **shell** 设置的信息。
- 如果在客户端使用 SSH2.0 版本登录路由器，则设置的登录时和登录成功后的标题信息都可以显示。

----结束

3.1.5 设置命令级别

为保证设备的安全性或满足低级别用户具有使用高级别命令的需要，可以设置命令级别。缺省情况下，命令按 0 ～ 3 级进行注册，如果用户需要实现权限的精细管理，可以将命令级别提升到 0 ～ 15 级。

背景信息

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。

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 **command-privilege level** *level* **view** *view-name command-key*，设置指定视图内命令的级别。

command-privilege level 命令可以一次指定多条命令（*command-key*）的级别及所在视图。

所有的命令都有默认的视图和优先级，一般不需要用户进行重新设置。

----结束

3.1.6 允许 undo 命令到上一级视图执行

当用户在某个视图下执行非本视图注册的 **undo** 命令时，系统将自动跳转到上一级视图搜索该 undo 命令。如果搜索成功，则 **undo** 命令生效。当上级视图没有该 **undo** 命令时，系统会向更上一级视图进行搜索，一直搜索到系统视图，不再向上搜索。

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 **matched upper-view**，允许 **undo** 命令到上一级视图执行。

缺省情况下，**undo** 命令不自动到上一级视图执行。

说明

- **matched upper-view** 命令只对执行此命令的当前登录用户有效。
- 非必要，不推荐配置 **undo** 自动匹配上一级视图特性。

----结束

3.2 显示系统基本信息

当用户需要查看当前系统的基本配置信息时，可以使用相应的 display 命令。

背景信息

利用 display 命令可以收集系统状态信息，根据功能可以划分为以下几类：

- 显示系统配置信息的 display 命令
- 显示系统运行状态的 display 命令
- 显示系统诊断信息的 display 命令

有关各协议和各种接口的 display 命令请参见相关章节。下面只介绍一些有关系统的 display 命令。

可在所有视图下进行下面的操作。

3.2.1 显示系统配置信息

当用户需要查看系统配置信息时，可以使用以下命令查看到系统版本、系统时钟、起始配置信息、当前配置信息等信息。

操作步骤

- 执行命令 **display version**，显示系统版本。
- 执行命令 **display clock**，显示系统时钟。
- 执行命令 **display saved-configuration**，显示起始配置信息。
- 执行命令 **display current-configuration**，显示当前配置信息。

  说明

  - 用户通过查看版本信息可以获知系统当前使用的软件版本、机架类型、主控板及接口板的相关信息。
  - 起始配置信息是设备上电时进行设备初始化工作的配置文件的信息。当前配置信息是设备运行过程中正在生效的配置信息。具体配置请参见《*Huawei AR3200 系列 企业路由器 配置指南-基础配置*》中“**配置系统启动**”部分。

----结束

3.2.2 显示系统运行状态

当用户需要查看系统运行状态时，可以使用以下命令查看当前视图的运行配置等信息。

操作步骤

- 执行命令 **display this**，显示当前视图的运行配置。

----结束

3.2.3 收集系统诊断信息

用户可以使用系统诊断信息命令收集当前系统所有模块的信息。

背景信息

在系统出现故障或日常维护时，为了便于问题定位，需要收集很多的信息，但相应的 **display** 命令很多，很难一次把信息收集全，这时可以使用 **display diagnostic-information** 命令进行系统当前各个模块的运行信息收集。

操作步骤

- 执行命令 **display diagnostic-information**，显示系统诊断信息。

  display diagnostic-information 命令一次性收集了如下命令执行后的终端显示的信息，包括：**display clock**、**display version** 等。

----结束

4 配置用户界面

关于本章

当用户通过 Console 口、TTY 方式、Telnet 或 SSH 方式登录路由器时，系统会分配相应的用户界面，用来管理当前用户与路由器之间的会话。

4.1 用户界面简介
系统支持的用户界面有 Console 用户界面、TTY 用户界面和 VTY 用户界面。

4.2 配置 Console 用户界面
当用户通过 Console 口登录设备实现本地维护时，可以根据使用需求或对设备安全的考虑，配置相应的 Console 用户界面属性。

4.3 配置 VTY 用户界面
当用户通过 Telnet 或 SSH 方式登录路由器实现本地或远程维护时，可以根据用户使用需求以及对设备安全的考虑，配置 VTY 用户界面。

4.4 配置 TTY 用户界面
TTY（True Type Terminal，实体类型终端）用户界面视图是系统提供的一种命令行视图，用来配置和管理所有工作在异步交互方式下的物理接口。

4.5 配置举例
配置 Console 用户界面、VTY 用户界面、TTY 用户界面的示例。配置示例中包括组网需求、配置注意事项和配置思路等。

4.1 用户界面简介

系统支持的用户界面有 Console 用户界面、TTY 用户界面和 VTY 用户界面。

每个用户界面有对应的用户界面视图。用户界面（User-interface）视图是系统提供的一种命令行视图，用来配置和管理所有工作在异步交互方式下的物理接口和逻辑接口，从而达到统一管理各种用户界面的目的。

目前系统支持的用户界面

- Console（CON）

  控制口（Console Port）是一种通信串行端口，由设备的主控板提供。

  一块主控板提供一个 Console 口，端口类型为 EIA/TIA-232 DCE。用户终端的串行端口可以与设备 Console 口直接连接，实现对设备的本地访问。

- VTY

  虚拟类型终端（Virtual Type Terminal）是一种虚拟线路端口。

  用户通过终端与设备建立 Telnet 或 SSH 连接后，即建立了一条 VTY，即用户可以通过 VTY 方式登录设备进行本地或远程访问。最多支持 15 个用户同时通过 VTY 方式访问设备。

- TTY

  实体类型终端（True Type Terminal），用来管理和监控通过 TTY 方式登录的用户。

  TTY 方式是指异步串口的登录方式。

用户界面的编号

当用户登录设备时，系统会根据此用户的登录方式，自动分配一个当前空闲且编号最小的相应类型的用户界面给这个用户。用户界面的编号有两种方式：相对编号方式和绝对编号方式。

- 相对编号方式

  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，而不能跨类型操作。相对编号方式遵守的规则如下：

  - 控制口的编号：CON 0。
  - 异步工作方式串口（TTY）的编号：第一个为 TTY 1，第二个为 TTY 2，依此类推。
  - 虚拟线路的编号：第一个为 VTY 0，第二个为 VTY 1，依此类推。

- 绝对编号方式

  绝对编号可以唯一的指定一个用户界面或一组用户界面。

  绝对编号的起始编号是 0，并按照 CON、TTY、VTY 的顺序依次分配。

  每个主控板上 CON 口只有一个，但 VTY 类型的用户界面有 20 个（其中 0 ～ 14 用户提供给普通 Telnet/SSH 用户的用户接口，16 ～ 20 是预留给网管用户的接口），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。

  缺省情况下，CON、TTY、VTY 三种用户接口在系统中的绝对编号，如**表 4-1** 所示。

表 4-1 用户界面的绝对编号示例

绝对编号	用户界面
0	CON0
1	TTY1 第一个 TTY 类型用户界面
2	TTY2 第二个 TTY 类型用户界面
3	TTY3 第三个 TTY 类型用户界面
4	TTY4 第四个 TTY 类型用户界面
5	TTY5 第五个 TTY 类型用户界面
129	VTY0 第一个 VTY 类型用户界面
130	VTY1 第二个 VTY 类型用户界面
131	VTY2 第三个 VTY 类型用户界面
132	VTY3 第四个 VTY 类型用户界面
133	VTY4 第五个 VTY 类型用户界面

说明

不同的设备类型，TTY 和 VTY 类型的用户界面的绝对编号可能有所不同。

在上述例子中，编号范围 1 ～ 128 保留给 TTY 类型的用户界面使用。

可以使用 **display user-interface** 命令查看当前系统中的绝对编号。

用户界面的用户验证

配置用户界面的用户验证方式后，用户登录设备时，系统对用户的身份进行验证。

对用户的验证有两种方式：password 验证和 AAA 验证。这两种验证方式分别描述如下：

- Password 验证：只需要口令，不需要用户名。
- AAA 验证：需要用户提供用户名和口令，对 Telnet 用户一般采用 AAA 验证。

用户界面的用户优先级

系统支持对登录用户进行分级管理。

与命令的优先级一样，用户的优先级分为 16 个级别，级别标识为 0 ～ 15，标识越高则优先级越高。

用户所能访问命令的级别由用户的级别决定。

- 如果对用户采用 password 验证，登录到设备的用户所能访问的命令级别由登录时的用户界面级别决定。

- 如果对用户采用 AAA 验证，登录到设备的用户所能访问的命令级别由 AAA 配置信息中本地用户的优先级级别决定。

4.2 配置 Console 用户界面

当用户通过 Console 口登录设备实现本地维护时，可以根据使用需求或对设备安全的考虑，配置相应的 Console 用户界面属性。

4.2.1 建立配置任务

在进行 Console 用户界面的配置前了解此特性的应用环境、配置此特性的前置任务和数据准备，有助于快速、准确地完成配置任务。

应用环境

当用户需要通过 Console 口登录路由器对路由器进行本地维护时，可以配置相应的 Console 用户界面，包括 Console 用户界面的物理属性、终端属性、用户优先级以及用户验证方式等。但这些参数不是必须要配置的，因为路由器上有缺省值。用户可以根据使用需求以及出于对设备安全性的考虑配置相应的参数。

前置任务

在配置 Console 用户界面之前，需要完成以下任务：

- 通过终端可以登录路由器

数据准备

在配置 Console 用户界面之前，需要准备以下数据。

序号	数据
1	传输速率、流控方式、校验方式、停止位、数据位
2	流控方式、终端屏幕的显示行数、终端屏幕显示的列数、历史命令缓冲区大小
3	用户优先级
4	用户验证方式、用户名、口令

说明

以上数据除用户名、口令外路由器均有缺省值，一般不需要单独配置。

4.2.2 配置 Console 用户界面的物理属性

Console 用户界面的物理属性包括 Console 口的传输速率、流控方式、校验位、停止位和数据位。

背景信息

Console 口的物理属性在路由器上均有缺省值，一般不需要单独配置。

说明

当用户通过 Console 口登录路由器时，超级终端的下列属性要和路由器的物理属性保持一致，否则不能登录到路由器。

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 **user-interface console** *interface-number*，进入用户界面视图。

步骤 3 执行命令 **speed** *speed-value*，设置传输速率。

缺省情况下，传输速率为 9600bit/s。

步骤 4 执行命令 **flow-control** { **hardware** | **none** }，设置流控方式。

缺省情况下，流控方式为 None。

步骤 5 执行命令 **parity** { **even** | **none** | **odd** }，设置校验位。

缺省情况下，校验位为 None。

步骤 6 执行命令 **stopbits** { **1.5** | **1** | **2** }，设置停止位。

缺省情况下，停止位为 1bit。

步骤 7 执行命令 **databits** { **5** | **6** | **7** | **8** }，设置数据位。

缺省情况下，数据位为 8。

----结束

4.2.3 配置 Console 用户界面的终端属性

用户可以配置 Console 用户界面的终端属性，包括用户超时断连功能、终端屏幕的显示行数或列数以及历史命令缓冲区大小。

背景信息

Console 用户界面的终端属性在路由器上均有缺省值。用户可以根据需求，重新配置相应的属性。

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 **user-interface console** *interface-number* ，进入用户界面视图。

步骤 3 执行命令 **shell**，启动终端服务。

步骤 4 执行命令 **idle-timeout** *minutes* [*seconds*]，设置用户超时断连功能。

在设定的时间内，如果连接始终处于空闲状态，系统将自动断开该连接。

缺省情况下，用户界面断连的超时时间为 10 分钟。

步骤 5 执行命令 **screen-length** *screen-length* [**temporary**]，设置终端屏幕每屏显示的行数。

使用参数 **temporary** 可以指定终端屏幕的临时显示行数。

缺省情况下，终端屏幕显示的行数为 24 行。

说明

设备可以自动根据终端的屏幕宽度调整输出信息的宽度，无需手工设置。

步骤 6 执行命令 **history-command max-size** *size-value*，设置历史命令缓冲区大小。

缺省情况下，用户界面历史命令缓冲区大小为 10 条历史命令。

----结束

4.2.4 配置 Console 用户界面的用户优先级

用户可以配置用户优先级，实现对不同用户访问路由器权限的限制，增加路由器管理的安全性。

背景信息

- 与命令的优先级一样，用户的优先级分为 16 个级别，级别标识为 0 ～ 15，标识越高则优先级越高。
- 用户的优先级和命令的优先级是相对应的，即用户只能使用等于或低于自己级别的命令。

命令优先级请参见**命令级别**。

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 **user-interface console** *interface-number*，进入 console 用户界面视图。

步骤 3 执行命令 **user privilege level** *level*，设置用户的优先级。

说明

- 缺省情况下，Console 口用户界面对应的默认命令访问级别是 15，而其他用户界面对应的默认级别是 0。
- 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级别为准。

----结束

4.2.5 配置 Console 用户界面的用户验证方式

系统提供 AAA 验证、密码验证两种方式。配置用户验证方式可以增加路由器的安全性。

背景信息

系统提供如**表 4-2** 所示两种验证方式。

表 4-2 验证方式

验证方式	优点	缺点
AAA 验证	AAA 验证基于用户认证，安全性高。 需要保存好登录的用户名和密码，登录设备时需要首先输入登录用户名和密码才能登录。	配置相对复杂，需要创建 AAA 用户及登录密码。
密码验证	密码验证基于 VTY 通道，配置较简单，有安全保证，只需创建登录密码即可。	相对 AAA 验证，安全性较低。 只要有登录设备的密码，所有用户均可登录设备。

注意

如果 Console 用户界面的验证方式为 password 或 AAA，必须配置密码或用户名，否则将无法登录。

操作步骤

- 设置 AAA 验证
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **user-interface console** *interface-number*，进入 Console 用户界面视图。
  3. 执行命令 **authentication-mode aaa**，设置用户验证方式为 AAA 验证。
  4. 执行命令 **aaa**，进入 AAA 视图。
  5. 执行命令 **local-user** *user-name* **password** *password*，配置本地用户名和密码。
  6. 执行命令 **local-user** *user-name* **service-type** *terminal*，配置本地用户的接入类型为 Console 用户。
  7. 执行命令 **quit**，退出 AAA 视图。
- 设置密码验证
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **user-interface console** *interface-number*，进入 Console 用户界面视图。
  3. 执行命令 **authentication-mode password**，设置用户验证方式为密码验证，并同时配置验证密码。
  4. （可选）执行命令 **set authentication password cipher** *password*，修改用户界面的验证密码。

     通过此命令可修改密码为明文或密文密码，但要确保当前用户界面的验证方式是密码验证，才可执行此命令。

----结束

4.2.6 检查配置结果

Console 用户界面配置成功后，可以查看到用户界面的使用信息、物理属性和配置、本地用户列表和在线用户等内容。

前提条件

已完成 Console 用户界面的相关配置。

操作步骤

- 使用 **display users** [**all**]命令显示用户界面的使用信息。
- 使用 **display user-interface console** *ui-number1* [**summary**]命令显示用户界面的物理属性和配置。
- 使用 **display local-user** 命令查看本地用户列表。

----结束

任务示例

执行命令 **display users**，可以查看当前用户界面的使用信息。

```
<Huawei> display users
  User-Intf   Delay     Type   Network Address     AuthenStatus    AuthorcmdFlag
  0   CON 0   00:00:44
Username : Unspecified
```

执行命令 **display user-interface console** *ui-number1* [**summary**]，查看用户界面的物理属性和配置。

```
<Huawei> display user-interface console 0
  Idx  Type     Tx/Rx      Modem Privi ActualPrivi Auth  Int
  0    CON 0    9600       -     3     -           N     -
  +    : Current UI is active.
  F    : Current UI is active and work in async mode.
  Idx  : Absolute index of UIs.
  Type : Type and relative index of UIs.
  Privi: The privilege of UIs.
  ActualPrivi: The actual privilege of user-interface.
  Auth : The authentication mode of UIs.
      A: Authenticate use AAA.
      N: Current UI need not authentication.
      P: Authenticate use current UI's password.
  Int  : The physical location of UIs.
```

执行命令 **display local-user**，可以查看本地用户列表。

```
<Huawei> display local-user
------------------------------------------------------------------------------
  User-name                      State  AuthMask  AdminLevel
  ------------------------------------------------------------------------------
  admin                          A      H         -
  ftp                            A      F         -
  guest                          A      A         15
  ------------------------------------------------------------------------------
  Total 3 user(s)
```

4.3 配置 VTY 用户界面

当用户通过 Telnet 或 SSH 方式登录路由器实现本地或远程维护时，可以根据用户使用需求以及对设备安全的考虑，配置 VTY 用户界面。

4.3.1 建立配置任务

在进行 VTY 用户界面的配置前了解此特性的应用环境、配置此特性的前置任务和数据准备，有助于快速、准确地完成配置任务。

应用环境

当用户需要通过 Telnet 或 SSH 方式本地或远程配置和管理路由器时可以配置相应的 VTY 用户界面，包括 VTY 用户界面的最大个数、呼入呼出限制、终端属性、用户优先级以及用户验证方式等。用户可以根据使用需求以及出于对设备安全性的考虑配置相应的参数。

前置任务

在配置 VTY 用户界面之前，需要完成以下任务：

- 通过终端可以登录路由器

数据准备

在配置 VTY 用户界面之前，需要准备以下数据。

序号	数据
1	VTY 类型用户界面的最大个数
2	（可选）对 VTY 类型用户界面呼入呼出进行限制的 ACL 号
3	终端用户超时断开时间、终端屏幕的显示的行数、终端屏幕显示的列数和历史命令缓冲区大小
4	用户优先级
5	用户验证方式、用户名、口令

说明

以上各数据除对 VTY 类型用户界面呼入呼出进行限制的 ACL 号、用户名和口令、用户验证方式外路由器均有缺省值，一般不需要单独配置。

4.3.2 配置 VTY 用户界面的最大个数

用户可以配置同时登录到路由器的 VTY 类型用户界面的最大个数，实现对登录用户量的限制。

背景信息

VTY 用户界面的最大个数是当前登录路由器的 Telnet 用户和 SSH 用户的总和。

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 **user-interface maximum-vty** *number*，配置可以同时登录到路由器的 VTY 类型用户界面的最大个数，缺省值为 5。

注意

当配置 VTY 用户界面最大个数为 0 时，任何用户（包括网管用户）都无法通过 VTY 登录到路由器。

如果要配置的 VTY 用户接口的最大数小于当前在线用户数量，系统则会提示用户配置失败。

如果要配置的 VTY 用户接口的最大数量大于当前的最大数量，就必须为新增加的用户接口配置验证方式。因为对于新增用户接口系统默认为无验证方式。

例如：当前允许最多 5 个 VTY 用户同时在线，现在配置为允许 15 个 VTY 用户同时在线，那么 VTY 用户接口 5 ～ 14 就必须使用 **authentication-mode** 命令配置验证方式。

----结束

4.3.3 （可选）配置 VTY 用户界面的呼入呼出限制

用户可以通过访问控制列表（ACL），实现对 VTY 用户界面的呼入呼出进行限制。

背景信息

在配置 VTY 用户界面的呼入呼出限制前，需要先在系统视图下执行 acl 命令创建一个访问控制列表并进入 ACL 视图，然后执行 rule 命令增加相应访问控制列表的规则。

说明

- 用户界面支持基本访问控制列表（2000 ~ 2999）和高级访问控制列表（3000 ~ 3999）。
- 关于 ACL 配置的更多内容，请参见安全配置《*Huawei AR3200 系列 企业路由器 配置指南-安全配置*》。

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 **user-interface vty** *first-ui-number* [*last-ui-number*]，进入 VTY 用户界面视图。

步骤 3 执行命令 **acl** *acl-number* { **inbound** | **outbound** }，配置 VTY 类型用户界面的呼入呼出限制。

- 当需要限制某个地址或地址段的用户登录到路由器时，使用 **inbound**。
- 当需要限制已经登录的用户登录到其它路由器时，使用 **outbound**。

----结束

4.3.4 配置 VTY 用户界面的终端属性

用户可以配置 VTY 用户界面的终端属性。包括用户超时断连功能、终端屏幕的显示行数或列数以及历史命令缓冲区的大小。

背景信息

VTY 用户界面的终端属性在路由器上均有缺省值。用户可以根据需求，重新配置相应的属性。

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 **user-interface vty** *first-ui-number* [*last-ui-number*]，进入 VTY 用户界面视图。

步骤 3 执行命令 **shell**，启用 VTY 终端服务。

步骤 4 执行命令 **idle-timeout** *minutes* [*seconds*]，设置用户超时断连功能。

在设定的时间内，如果连接始终处于空闲状态，系统将自动断开该连接。

缺省情况下，超时时间为 10 分钟。

步骤 5 执行命令 **screen-length** *screen-length* [**temporary**]，设置终端屏幕每屏显示的行数。

使用参数 **temporary** 可以指定终端屏幕的临时显示行数。

缺省情况下，终端屏幕显示的行数为 24 行。

说明

设备可以自动根据终端的屏幕宽度调整输出信息的宽度，无需手工设置。

步骤 6 执行命令 **history-command max-size** *size-value*，设置历史命令缓冲区的大小。

缺省情况下，存放 10 条历史命令。

----结束

4.3.5 配置 VTY 用户界面的用户优先级

用户可以配置用户优先级，实现对不同用户访问路由器权限的限制，增加路由器管理的安全性。

背景信息

- 与命令的优先级一样，用户的优先级分为 16 个级别，级别标识为 0 ～ 15，标识越高则优先级越高。
- 用户的优先级和命令的优先级是相对应的，即用户只能使用等于或低于自己级别的命令。

命令优先级请参见命令级别。

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 **user-interface vty** *first-ui-number* [*last-ui-number*]，进入 VTY 用户界面视图。

步骤 3 执行命令 **user privilege level** *level*，设置用户优先级。

缺省情况下，VTY 用户界面对应的默认命令访问级别是 0。

说明

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级别为准。

----结束

4.3.6 配置 VTY 用户界面的用户验证方式

系统提供 AAA 验证、密码验证两种方式。配置用户验证方式可以增加路由器的安全性。

背景信息

系统提供如表 4-3 所示两种验证方式。

表 4-3 验证方式

验证方式	优点	缺点
AAA 验证	AAA 验证基于用户认证，安全性高。 需要保存好登录的用户名和密码，登录设备时需要首先输入登录用户名和密码才能登录。	配置相对复杂，需要创建 AAA 用户及登录密码。
密码验证	密码验证基于 VTY 通道，配置较简单，有安全保证，只需创建登录密码即可。	相对 AAA 验证，安全性较低。 只要有登录设备的密码，所有用户均可登录设备。

操作步骤

- 设置 AAA 验证
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **user-interface vty** *first-ui-number* [*last-ui-number*]，进入 VTY 用户界面视图。
  3. 执行命令 **authentication-mode aaa**，设置用户验证方式为 AAA 验证。
  4. 执行命令 **quit**，退出 VTY 用户界面视图。
  5. 执行命令 **aaa**，进入 AAA 视图。
  6. 执行命令 **local-user** *user-name* **password** *password*，配置本地用户名和密码。
  7. 执行命令 **local-user** *user-name* **service-type** *telnet*，配置本地用户的接入类型为 Telnet。
- 设置密码验证
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **user-interface vty** *first-ui-number* [*last-ui-number*]，进入 VTY 用户界面视图。
  3. 执行命令 **authentication-mode password**，设置用户验证方式为密码验证，并同时配置验证密码。
  4. （可选）执行命令 **set authentication password cipher** *password*，修改用户界面的验证密码。

     通过此命令可修改密码为明文或密文密码，但要确保当前用户界面的验证方式是密码验证，才可执行此命令。

----结束

4.3.7 检查配置结果

VTY 用户界面配置成功后，可以查看到用户界面的使用信息、VTY 类型用户界面的最大个数以及物理属性和配置等内容。

前提条件

已完成 VTY 用户界面的所有配置。

操作步骤

- 使用 **display users** [**all**]命令查看用户界面的使用信息。
- 使用 **display user-interface maximum-vty** 命令查看 VTY 类型用户界面的最大个数。
- 使用 **display user-interface** [[*ui-type*] *ui-number1* | *ui-number*] [**summary**]命令查看用户界面的物理属性和配置。
- 使用 **display local-user** 命令查看本地用户列表。
- 使用 **display vty mode** 命令查看 VTY 模式。

----结束

任务示例

执行命令 **display users**，可以查看当前用户界面的使用信息。

```
<Huawei> display users
  User-Intf    Delay     Type   Network Address     AuthenStatus    AuthorcmdFlag
  34  VTY 0    00:00:12  TEL    10.138.77.38
 Username : Unspecified
+ 35  VTY 1    00:00:00  TEL    10.138.77.57
 Username : Unspecified
```

执行命令 **display user-interface maximum-vty**，可以查看 VTY 类型用户界面的最大个数。

```
<Huawei> display user-interface maximum-vty
 Maximum of VTY user:15
```

执行命令 **display user-interface vty** [*ui-number1* | *ui-number*] [**summary**]，可以查看用户界面的物理属性和配置。

```
<Huawei> display user-interface vty 0
  Idx  Type     Tx/Rx      Modem Privi ActualPrivi Auth  Int
+ 34   VTY 0               -     14    14          N     -
  +    : Current UI is active.
  F    : Current UI is active and work in async mode.
  Idx  : Absolute index of UIs.
  Type : Type and relative index of UIs.
  Privi: The privilege of UIs.
  ActualPrivi: The actual privilege of user-interface.
  Auth : The authentication mode of UIs.
      A: Authenticate use AAA.
      N: Current UI need not authentication.
      P: Authenticate use current UI's password.
  Int  : The physical location of UIs.
```

执行命令 **display local-user**，可以查看本地用户列表。

```
<Huawei> display local-user
------------------------------------------------------------------------------
  User-name                      State  AuthMask  AdminLevel
  ------------------------------------------------------------------------------
```

```
admin                           A      H         -
ftp                             A      F         -
guest                           A      A         15
------------------------------------------------------------------------------
Total 3 user(s)
```

执行命令 **display vty mode**，可以看到使能了机机接口的提示信息。例如：

```
<Huawei> display vty mode
current VTY mode is Machine-Machine interface
```

4.4 配置 TTY 用户界面

TTY（True Type Terminal，实体类型终端）用户界面视图是系统提供的一种命令行视图，用来配置和管理所有工作在异步交互方式下的物理接口。

4.4.1 建立配置任务

在进行 TTY 用户界面的配置前了解此特性的应用环境、配置此特性的前置任务和数据准备，有助于快速、准确地完成配置任务。

应用环境

当用户需要通过异步串口登录路由器对路由器进行本地维护时，可以配置相应的 TTY 用户界面，包括 TTY 用户界面的物理属性、终端属性、用户优先级等。但这些参数不是必须要配置的，因为路由器上有缺省值。用户可以根据使用需求以及出于对设备安全性的考虑配置相应的参数。

前置任务

在配置 TTY 用户界面之前，需要完成以下任务：

- 通过终端可以登录路由器

数据准备

在配置 TTY 用户界面之前，需要准备以下数据。

序号	数据
1	传输速率、流控方式、校验方式、停止位、数据位
2	流控方式、终端屏幕的显示行数、历史命令缓冲区大小
3	用户优先级

说明

以上数据除用户名、口令外路由器均有缺省值，一般不需要单独配置。

4.4.2 配置 TTY 用户界面的物理属性

TTY 用户界面的物理属性包括异步串口的传输速率、流控方式、校验位、停止位和数据位。

背景信息

异步串口的物理属性在路由器上均有缺省值，一般不需要单独配置。

说明

- 当用户需要通过异步串口登录路由器时，需要在设备上配备 SA 或者 AS 单板，如果是 SA 单板上，需要将 SA 单板上的接口模式设置为异步模式。
- 当用户通过异步串口登录路由器时，超级终端的下列属性要和路由器的物理属性保持一致，否则不能登录到路由器。

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 **user-interface tty** *tty-number*，进入 TTY 用户界面视图。

当单板注册成功，且串口工作在异步模式时，设备会随机生成 *tty-number*，可以通过 **display user-interface** 命令查看。

步骤 3 执行命令 **speed** *speed-value*，设置传输速率。

缺省情况下，传输速率为 9600bit/s。

步骤 4 执行命令 **flow-control** { **hardware** | **none** }，设置流控方式。

缺省情况下，流控方式为 None。

步骤 5 执行命令 **parity** { **even** | **none** | **odd** }，设置校验位。

缺省情况下，校验位为 None。

步骤 6 执行命令 **stopbits** { **1.5** | **1** | **2** }，设置停止位。

缺省情况下，停止位为 1bit。

步骤 7 执行命令 **databits** { **5** | **6** | **7** | **8** }，设置数据位。

缺省情况下，数据位为 8。

----结束

4.4.3 配置 TTY 用户界面的终端属性

用户可以配置 TTY 用户界面的终端属性，包括用户超时断连功能、终端屏幕的显示行数以及历史命令缓冲区大小。

背景信息

TTY 用户界面的终端属性在路由器上均有缺省值。用户可以根据需求，重新配置相应的属性。

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 **user-interface tty** *interface-number* ，进入 TTY 用户界面视图。

步骤 3 执行命令 **shell**，启动终端服务。

步骤 4 执行命令 **idle-timeout** *minutes* [*seconds*]，设置用户超时断连功能。

在设定的时间内，如果连接始终处于空闲状态，系统将自动断开该连接。

缺省情况下，用户界面断连的超时时间为 10 分钟。

步骤 5 执行命令 **screen-length** *screen-length* [**temporary**]，设置终端屏幕每屏显示的行数。

使用参数 **temporary** 可以指定终端屏幕的临时显示行数。

缺省情况下，终端屏幕显示的行数为 24 行。

说明

设备可以自动根据终端的屏幕宽度调整输出信息的宽度，无需手工设置。

步骤 6 执行命令 **history-command max-size** *size-value*，设置历史命令缓冲区大小。

缺省情况下，用户界面历史命令缓冲区大小为 10 条历史命令。

----结束

4.4.4 配置 TTY 用户界面的用户优先级

用户可以配置用户优先级，实现对不同用户访问路由器权限的限制，增加路由器管理的安全性。

背景信息

- 与命令的优先级一样，用户的优先级分为 16 个级别，级别标识为 0 ～ 15，标识越高则优先级越高。
- 用户的优先级和命令的优先级是相对应的，即用户只能使用等于或低于自己级别的命令。

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 **user-interface tty** *interface-number*，进入 TTY 用户界面视图。

步骤 3 执行命令 **user privilege level** *level*，设置用户的优先级。

说明

- 缺省情况下，TTY 口用户界面对应的默认命令访问级别是 3，而其他用户界面对应的默认级别是 0。
- 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级别为准。

----结束

4.4.5 检查配置结果

TTY 用户界面配置成功后，可以查看到用户界面的使用信息、物理属性和配置、本地用户列表和在线用户等内容。

前提条件

已完成 TTY 用户界面的相关配置。

操作步骤

- 使用 **display users** [**all**]命令显示用户界面的使用信息。
- 使用 **display user-interface tty** *ui-number1* [**summary**]命令显示用户界面的物理属性和配置。

----结束

任务示例

执行命令 **display users**，可以查看当前用户界面的使用信息。

```
<Huawei> display users
  User-Intf   Delay     Type   Network Address     AuthenStatus    AuthorcmdFlag
  0   TTY 0   00:00:44
Username : Unspecified
```

执行命令 **display user-interface tty** *ui-number1* [**summary**]，查看用户界面的物理属性和配置。

```
<Huawei> display user-interface tty 17
Idx  Type     Tx/Rx      Modem Privi ActualPrivi Auth  Int
  17   TTY 17   9600       -     0     -           N     2/0/0
  +    : Current UI is active.
  F    : Current UI is active and work in async mode.
  Idx  : Absolute index of UIs.
  Type : Type and relative index of UIs.
  Privi: The privilege of UIs.
  ActualPrivi: The actual privilege of user-interface.
  Auth : The authentication mode of UIs.
      A: Authenticate use AAA.
      N: Current UI need not authentication.
      P: Authenticate use current UI's password.
  Int  : The physical location of UIs.
```

4.5 配置举例

配置 Console 用户界面、VTY 用户界面、TTY 用户界面的示例。配置示例中包括组网需求、配置注意事项和配置思路等。

4.5.1 配置 Console 用户界面示例

在本示例中，通过配置 Console 用户界面的物理属性、终端属性、用户优先级、验证方式和验证密码，实现通过 Console 口使用 Password 方式登录路由器。

组网需求

在初始化空配置路由器或本地维护路由器时，用户需要通过 Console 用户界面登录并进行配置。设备管理员可以根据使用需求或出于对设备安全性的考虑，配置 Console 用户界面的相关属性。

对从 Console 登录的用户进行 Password 验证，用户登录时需要输入密码“huawei” 。

登录后，如果用户超过 30 分钟未对路由器进行操作，将断开与路由器的连接。

配置思路

采用如下的思路配置登录路由器：

1. 进入用户界面视图，配置 Console 用户界面的物理属性。
2. 配置 Console 用户界面的终端属性。
3. 配置 Console 用户界面的用户优先级。
4. 配置 Console 用户界面的验证方式和验证密码。

数据准备

为完成此配置举例，需准备如下的数据：

- Console 用户界面的传输速率为 9600bit/s。
- Console 用户界面的流控方式为 None。
- Console 用户界面的校验位为 even。
- Console 用户界面的停止位为 2。
- Console 用户界面的数据位为 8。
- Console 用户界面断开连接的时间为 30。
- Console 用户界面的终端屏幕每屏显示的行数为 30。
- Console 用户界面的历史命令缓冲区大小为 20。
- Console 用户界面的用户优先级为 15。
- Console 用户界面的用户验证方式为 password 和验证密码为 huawei。

操作步骤

步骤 1 配置 Console 用户界面的物理属性

```
<Huawei> system-view
[Huawei] user-interface console 0
[Huawei-ui-console0] speed 9600
[Huawei-ui-console0] flow-control none
[Huawei-ui-console0] parity even
[Huawei-ui-console0] stopbits 2
[Huawei-ui-console0] databits 8
```

步骤 2 配置 Console 用户界面的终端属性

```
[Huawei-ui-console0] idle-timeout 30
[Huawei-ui-console0] screen-length 30
[Huawei-ui-console0] history-command max-size 20
```

步骤 3 配置 Console 用户界面的用户优先级

```
[Huawei-ui-console0] user privilege level 15
```

步骤 4 配置 Console 用户界面的用户验证方式为密码验证

```
[Huawei-ui-console0] authentication-mode password
Please configure the login password (maximum length 16):huawei
[Huawei-ui-console0] quit
```

Console 用户界面配置完成后，用户可以通过 Console 口使用 Password 方式登录路由器，实现对路由器的本地维护。用户登录路由器的具体过程请参见配置用户登录。

----结束

配置文件

```
#
 sysname Huawei
#
user-interface con 0
```

```
 authentication-mode password
 user privilege level 15
 set authentication password cipher Hb(c;\@iU'@X,k6.E\Z,*.S#
 history-command max-size 20
 idle-timeout 30 0
 screen-length 30
 databits 8
 parity even
 stopbits 2
 speed 9600
#
return
```

4.5.2 配置 VTY 用户界面示例

配置 VTY 用户界面的示例。在本示例中，通过配置 VTY 用户界面的最大个数、呼入呼出限制、终端属性、验证方式和验证密码，实现通过 Telnet 方式使用 Password 验证登录路由器。

组网需求

用户使用 Telnet 协议或 SSH 协议从 VTY 通道登录远程路由器。设备管理员可以根据使用需求或出于对设备安全性的考虑，配置 VTY 用户界面的相关属性。

配置 VTY 用户界面的用户优先级为 15，对从 VTY 登录的用户进行 Password 验证，用户登录时需要输入密码“huawei”。同时需要限制 IP 地址为 10.1.1.1 的用户登录路由器。

登录后，如果用户超过 30 分钟未对路由器进行操作，将断开与路由器的连接。

配置思路

采用如下的思路配置登录路由器：

1. 进入用户接口视图，配置 VTY 用户界面的最大个数为 15。
2. 配置 VTY 用户界面的呼入呼出限制，实现限制某一 IP 地址或地址段的用户登录路由器。
3. 配置 VTY 用户界面的终端属性。
4. 配置 VTY 用户界面的用户优先级。
5. 配置 VTY 用户界面的验证方式和验证密码。

数据准备

为完成此配置举例，需准备如下的数据：

- VTY 用户界面的最大个数为 15。
- VTY 用户界面呼入限制的 ACL 号为 2000。
- VTY 用户界面断开连接的时间为 30 分钟。
- VTY 用户界面的终端屏幕每屏显示的行数为 30。
- VTY 用户界面的历史命令缓冲区大小为 20。
- VTY 用户界面的用户优先级为 15。
- VTY 用户界面的用户验证方式为 password，验证密码为 huawei。

缺省情况下，在所有的用户界面上启动终端服务。如果终端服务关闭，执行命令 **shell** 使能终端服务接入系统。

操作步骤

步骤 1 配置 VTY 用户界面的最大个数

```
<Huawei> system-view
[Huawei] user-interface maximum-vty 15
```

步骤 2 配置 VTY 用户界面的呼入呼出限制类型

```
[Huawei] acl 2000
[Huawei-acl-basic-2000] rule deny source 10.1.1.1 0
[Huawei-acl-basic-2000] rule permit source any
[Huawei-acl-basic-2000] quit
[Huawei] user-interface vty 0 14
[Huawei-ui-vty0-14] acl 2000 inbound
```

步骤 3 配置 VTY 用户界面的终端属性

```
[Huawei-ui-vty0-14] shell
[Huawei-ui-vty0-14] idle-timeout 30
[Huawei-ui-vty0-14] screen-length 30
[Huawei-ui-vty0-14] history-command max-size 20
```

步骤 4 配置 VTY 用户界面的用户优先级

```
[Huawei-ui-vty0-14] user privilege level 15
```

步骤 5 配置 VTY 用户界面的用户验证方式为密码验证

```
[Huawei-ui-vty0-14] authentication-mode password
Please configure the login password (maximum length 16):huawei
[Huawei-ui-vty0-14] quit
```

VTY 用户界面配置完成后，用户可以通过 Telnet 或 SSH（STelnet）使用 Password 方式登录路由器，实现对路由器的本地或者远程维护。用户登录路由器的具体过程请参见*《Huawei AR3200 系列 企业路由器 配置指南-基础配置》*中“**配置用户登录**”部分。

----结束

配置文件

```
#
 sysname Huawei
#
acl number 2000
 rule 5 deny source 10.1.1.1 0
 rule permit source any
#
user-interface maximum-vty 15
user-interface vty 0 14
 acl 2000 inbound
 user privilege level 15
 authentication-mode password
 set authentication password cipher %$%$%%eM1O&JQOsq%;YWL7f*"RI@,O#LL>N0OC&*1C..Z'CDqXOJ%$%$
 history-command max-size 20
 idle-timeout 30 0
 screen-length 30
#
return
```

4.5.3 配置 TTY 用户界面示例

在本示例中，介绍了 TTY 用户界面的物理属性、终端属性和用户优先级的配置。

组网需求

在初始化路由器或本地维护路由器时，用户需要通过 TTY 用户界面登录并进行配置。设备管理员可以根据使用需求或出于对设备安全性的考虑，配置 TTY 用户界面的相关属性。

登录后，如果用户超过 30 分钟未对路由器进行操作，将断开与路由器的连接。

配置思路

采用如下的思路配置登录路由器：

1. 进入用户接口视图，配置 TTY 用户界面的物理属性。
2. 配置 TTY 用户界面的终端属性。
3. 配置 TTY 用户界面的用户优先级。

数据准备

为完成此配置举例，需准备如下的数据：

- TTY 用户界面的传输速率为 4800bit/s。
- TTY 用户界面的流控方式为 None。
- TTY 用户界面的校验位为 even。
- TTY 用户界面的停止位为 2。
- TTY 用户界面的数据位为 6。
- TTY 用户界面断开连接的时间为 30。
- TTY 用户界面的终端屏幕每屏显示的行数为 30。
- TTY 用户界面的历史命令缓冲区大小为 20。

缺省情况下，在所有的用户界面上启动终端服务。如果终端服务关闭，执行命令 **shell** 使能终端服务接入系统。

操作步骤

步骤 1 配置 TTY 用户界面的物理属性

```
<Huawei> system-view
[Huawei] user-interface tty 1
[Huawei-ui-tty1] speed 4800
[Huawei-ui-tty1] flow-control none
[Huawei-ui-tty1] parity even
[Huawei-ui-tty1] stopbits 2
[Huawei-ui-tty1] databits 6
```

步骤 2 配置 TTY 用户界面的终端属性

```
[Huawei-ui-tty1] shell
[Huawei-ui-tty1] idle-timeout 30
[Huawei-ui-tty1] screen-length 30
[Huawei-ui-tty1] history-command max-size 20
```

步骤 3 配置 TTY 用户界面的用户优先级

```
[Huawei-ui-tty1] user privilege level 15
```

----结束

配置文件

```
#
 sysname Huawei
#
user-interface TTY 1
 user privilege level 15
 history-command max-size 20
 idle-timeout 30 0
 screen-length 30
 databits 6
 parity even
 stopbits 2
 speed 4800
#
return
```

5 配置用户登录

关于本章

用户可以通过 Console 口、Telnet 或 SSH（STelnet）方式登录路由器，实现对路由器本地或远程维护。

5.1 用户登录简介
用户只有成功登录到设备，才能实现对设备的管理与维护。用户登录设备的方式有：Console 口、Telnet 或 STelnet。

5.2 配置用户通过 Console 口登录系统
当用户需要配置第一次上电的路由器或在本地维护路由器时，可以通过 Console 口登录。

5.3 配置用户通过 Telnet 登录系统
如果网络中有一台或多台路由器需要配置和管理，用户无需为每一台路由器连接用户终端进行本地维护。此时可以通过 Telnet 方式从用户终端登录到路由器，实现对网络中路由器的远程维护，极大地方便了用户的操作。

5.4 配置用户通过 STelnet 登录系统
STelnet 协议实现在不安全网络上提供安全的远程访问。客户端和服务器之间经过协商，建立安全连接，用户可以像操作 Telnet 一样登录路由器。

5.5 登录后的常用操作
登录路由器后，用户可以根据需求进行如下的操作，如切换用户级别、锁定用户终端界面等。

5.6 配置举例
配置用户通过 Console 口、Telnet、STelnet 登录系统的示例。请结合配置流程图了解配置过程。配置示例中包括组网需求、配置注意事项和配置思路等。

5.1 用户登录简介

用户只有成功登录到设备，才能实现对设备的管理与维护。用户登录设备的方式有：Console 口、Telnet 或 STelnet。

用户可通过如表 5-1 所示几种方式登录设备，对设备进行配置和管理。

表 5-1 用户登录方式

登录方式	应用场景	说明
配置用户通过 Console 口登录系统	使用终端通过连接设备的 Console 口登录设备，进行第一次上电和配置。 ● 当用户无法进行远程访问设备时，可通过 Console 进行本地登录。 ● 当设备系统无法启动时，可通过 console 口进行诊断或进入 BootRom 进行系统升级。	缺省情况下，用户可以直接通过 Console 口本地登录设备，登录时需要配置验证密码，命令访问级别是 3。
配置用户通过 Telnet 登录系统	通过终端连接到网络上，使用 Telnet 方式登录设备，进行本地或远程的配置，目标设备根据配置的登录参数对用户进行验证。 Telnet 登录方式便于对设备进行远程管理和维护。	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，必须先通过 Console 口本地登录设备，并完成以下配置： ● 配置设备管理网口的 IP 地址，确保终端和登录的设备之间路由可达（缺省情况下，设备上没有配置 IP 地址）。 ● 配置 VTY 用户界面的用户认证方式（缺省情况下，VTY 用户界面无认证方式的配置，需要网络管理员手动配置认证方式。）。 ● 配置 VTY 用户界面的用户级别（缺省情况下，VTY 用户界面的用户级别是 0）。 ● 使能 Telnet 服务器功能（缺省情况下，设备的 Telnet 服务功能是开启的）。

登录方式	应用场景	说明
配置用户通过 STelnet 登录系统	通过终端连接到网络上，如果网络安全性不高，SSH（Secure Shell）可提供安全的信息保障和强大认证功能，保护设备系统不受 IP 欺骗、明文密码截取等攻击。 STelnet 登录能更大限度的保证数据信息交换的安全。	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，必须先通过 Console 口本地登录设备，并完成以下配置： ● 配置设备管理网口的 IP 地址，确保终端和登录的设备之间路由可达（缺省情况下，设备上没有配置 IP 地址）。 ● 配置 VTY 用户界面的用户认证方式（缺省情况下，VTY 用户界面无认证方式的配置，需要网络管理员手动配置认证方式。）。 ● 配置 VTY 用户界面的用户级别（缺省情况下，VTY 用户界面的用户级别是 0）。 ● 配置 VTY 用户界面支持 SSH 协议（缺省情况下，VTY 类型用户界面支持的协议是 Telnet）。 ● 使能 STelnet 服务器功能（缺省情况下，设备的 STelnet 服务功能是关闭的）。

说明

Telnet 缺少安全的认证方式，而且传输过程采用 TCP 进行明文传输，存在很大的安全隐患。与 Telnet 相比，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。SSH 协议支持 STelnet，即安全 Telnet。

SSH 协议的介绍请参见《*Huawei AR3200 系列 企业路由器 特性描述 基础配置*》。

5.2 配置用户通过 Console 口登录系统

当用户需要配置第一次上电的路由器或在本地维护路由器时，可以通过 Console 口登录。

5.2.1 建立配置任务

在进行用户通过 Console 口登录系统的配置前了解此特性的应用环境、配置此特性的前置任务和数据准备，有助于快速、准确地完成配置任务。

应用环境

用户可以在本地通过 Console 口登录设备，特别是设备第一次上电时只能采用此方式登录。

- 当用户无法进行远程访问设备时，可通过 Console 进行本地登录。
- 当设备系统无法启动时，可通过 console 口进行诊断或进入 BootRom 进行系统升级。

前置任务

在配置用户通过 Console 口登录设备之前，需要完成以下任务：

- 准备好 Console 通信电缆
- PC 已安装终端仿真程序（如 Windows XP 的超级终端）

数据准备

在配置用户通过 Console 口登录设备之前，需要准备以下数据。

序号	数据
1	● 传输速率、流控方式、校验方式、停止位、数据位、流控方式 ● 终端屏幕的显示的行数、终端屏幕显示的列数、历史命令缓冲区大小 ● 用户优先级 ● 用户验证方式、用户名、口令

5.2.2 用户通过 Console 口登录系统

用户通过 Console 口连接终端与设备，实现从用户终端登录设备。

背景信息

- 用户终端的通信参数必须与设备上 Console 用户界面的物理属性参数保持一致。
- 必须给 Console 用户界面设置用户验证放置，用户必须通过验证后才能登录设备，增加了设备的安全性。

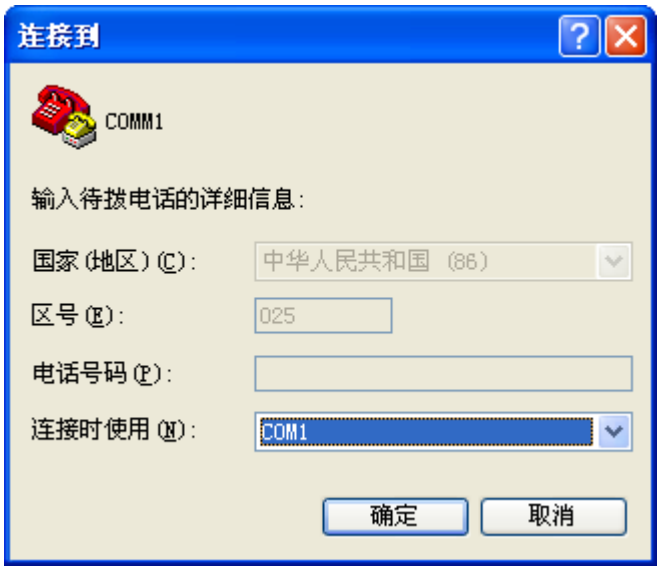
操作步骤

步骤 1 在 PC 上打开终端仿真程序（如 Windows XP 的超级终端），如图 5-1 新建一个连接。

图 5-1 新建连接

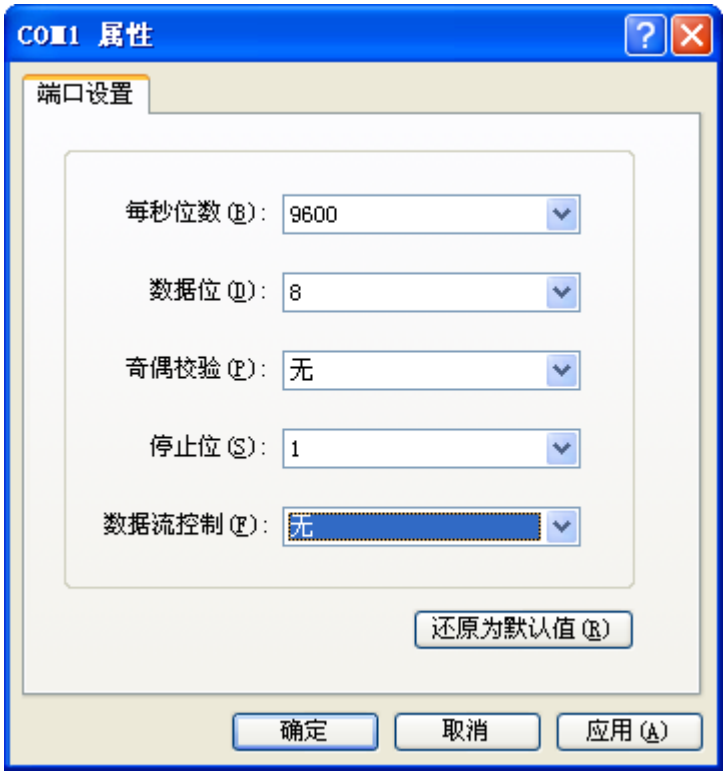
步骤 2 设置连接端口，如图 5-2。

图 5-2 连接端口设置



步骤 3 设置端口通信参数，与设备的缺省值保持一致，如图 5-3。

图 5-3 端口通信参数设置



步骤 4 按 Enter 键，直到系统出现如下显示，提示用户配置验证密码，系统会自动保存此密码配置。

```
Please configure the login password (maximum length 16)
Enter Password:
Confirm Password:
```

说明

- 如果设备出厂时已有初始密码，请输入初始密码“Admin@huawei.com”进入系统，但此密码不是安全密码，请及时修改，修改方法请参见 **4.2.5 配置 Console 用户界面的用户验证方式**。
- 用户界面密码配置成功后，当用户采用密码验证方式通过此界面再次登录系统时，用户验证密码即为初次登录时所配置的验证密码。
- 用户通过 Console 口登录新出厂（或没有启动配置文件）的 AR3200 时，系统会提示：“Auto-Config is working. Before configuring the device, stop Auto-Config. If you perform configurations when Auto-Config is running, the DHCP, routing, DNS, and VTY configurations will be lost. Do you want to stop Auto-Config? [y/n]:”，
  - 如果需要进行 Auto-Config，选择 n，并回车；
  - 如果不需要进行 Auto-Config，选择 y，并回车；

注意

如果不需要进行 Auto-Config，但选择的是 n，会导致后续配置的 dhcp、路由、dns 和 vty 用户配置丢失。

----结束

5.2.3 （可选）配置 Console 用户界面

当用户通过 Console 口登录设备实现本地维护时，可以根据使用需求或对设备安全的考虑，配置相应的 Console 用户界面属性。

背景信息

Console 用户界面的属性在设备上都有缺省值，用户一般不需要另外配置。但是用户可以根据使用需求以及对设备安全的考虑，配置相关属性，比如用户界面的终端属性以及用户验证方式等。

如需配置 Console 用户界面，请参见**配置 Console 用户界面**。

说明

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

5.2.4 检查配置结果

用户通过 Console 口登录系统配置成功后，可以查看到用户界面的使用信息、物理属性和配置、本地用户列表和在线用户等内容。

前提条件

已完成用户通过 Console 口登录系统的相关配置。

操作步骤

- 使用 **display users** [**all**]命令显示用户界面的使用信息。
- 使用 **display user-interface console** *ui-number1* [**summary**]命令显示用户界面的物理属性和配置。
- 使用 **display local-user** 命令查看本地用户列表。

----结束

任务示例

执行命令 **display users**，可以查看当前用户界面的使用信息。

```
<Huawei> display users
  User-Intf   Delay     Type   Network Address     AuthenStatus    AuthorcmdFlag
  0   CON 0   00:00:44
Username : Unspecified
```

执行命令 **display user-interface console** *ui-number1* [**summary**]，查看用户界面的物理属性和配置。

```
<Huawei> display user-interface console 0
  Idx  Type     Tx/Rx      Modem Privi ActualPrivi Auth  Int
  0    CON 0    9600       -     3     -           N     -
  +    : Current UI is active.
  F    : Current UI is active and work in async mode.
  Idx  : Absolute index of UIs.
  Type : Type and relative index of UIs.
  Privi: The privilege of UIs.
  ActualPrivi: The actual privilege of user-interface.
  Auth : The authentication mode of UIs.
      A: Authenticate use AAA.
      N: Current UI need not authentication.
      P: Authenticate use current UI's password.
  Int  : The physical location of UIs.
```

执行命令 **display local-user**，可以查看本地用户列表。

```
<Huawei> display local-user
------------------------------------------------------------------------------
  User-name                      State  AuthMask  AdminLevel
  ----------------------------------------------------------------------------
  admin                          A      H         -
  ftp                            A      F         -
  guest                          A      A         15
  ----------------------------------------------------------------------------
  Total 3 user(s)
```

5.3 配置用户通过 Telnet 登录系统

如果网络中有一台或多台路由器需要配置和管理，用户无需为每一台路由器连接用户终端进行本地维护。此时可以通过 Telnet 方式从用户终端登录到路由器，实现对网络中路由器的远程维护，极大地方便了用户的操作。

5.3.1 建立配置任务

在进行用户通过 Telnet 登录系统的配置前了解此特性的应用环境、配置此特性的前置任务和数据准备，有助于快速、准确地完成配置任务。

应用环境

如果已知待登录设备的 IP 地址，用户可以通过 Telnet 方式从用户终端登录设备，对设备进行远程配置。用户可以通过此方式在一台用户终端上维护网络中的多台设备，极大地方便了用户的操作。

前置任务

在配置用户通过 Telnet 登录设备之前，必须通过 Console 口登录设备，更改设备的缺省配置，以便用户能够通过 Telnet 方式远程登录设备并实现管理和维护。更改的缺省配置如下：

- 配置设备管理网口的 IP 地址，确保终端和登录的设备之间路由可达。
- **配置 VTY 用户界面的用户验证方式和优先级**，实现远程管理和维护设备。
- **使能 Telnet 服务器功能**，以便用户能够通过 Telnet 方式远程登录设备。

数据准备

在配置用户通过 Telnet 登录系统之前，需要准备以下数据。

序号	数据
1	● 用户优先级 ● 用户验证方式、用户名、口令 ● （可选）VTY 类型用户界面的最大个数 ● （可选）对 VTY 类型用户界面呼入呼出进行限制的 ACL 号 ● （可选）终端用户超时断开时间、终端屏幕的显示行数、终端屏幕显示的列数和历史命令缓冲区大小
2	远端设备的 IPv4/IPv6 地址或主机名
3	远端设备提供 Telnet 服务的 TCP 端口号、VPN 实例名

5.3.2 配置 VTY 用户界面的用户级别和验证方式

缺省情况下，VTY 用户界面的用户级别是 0，为了实现通过 Telnet 方式远程登录设备维护和管理设备，必须先通过 Console 口登录设备，更改用户级别并配置用户验证方式。

背景信息

VTY 用户界面的其他属性在设备上都有缺省值，用户一般不需要另外配置。但是可以根据用户使用需求，配置相关属性。具体配置请参见**配置 VTY 用户界面**。

以下配置无顺序关系，但是都必须配置。

操作步骤

- 配置 VTY 用户界面的用户优先级
  1. 执行命令 **system-view**，进入系统视图。

2. 执行命令 **user-interface vty** *first-ui-number* [*last-ui-number*]，进入 VTY 用户界面视图。
3. 执行命令 **user privilege level** *level*，设置用户优先级。

   缺省情况下，VTY 用户界面的用户级别是 0。VTY 用户界面的用户级别和命令级别对应关系如表 5-2 所示。

表 5-2 用户级别和命令级别对应关系表

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，比如管理配置文件中的 display current-configuration 命令和 display saved-configuration 命令是 3 级管理级。各命令的级别请参见《*Huawei AR3200 系列 企业路由器 命令参考*》手册。
2	0、1、2	配置级	业务配置命令，包括路由、各个网络层次的命令，向用户提供直接网络服务。
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、配置文件切换命令、备板控制命令、用户管理命令、命令级别设置命令、系统内部参数设置命令；用于业务故障诊断的 debugging 命令等。

说明

- 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，从而保证了设备的安全性。
- 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级别为准。

- 配置 VTY 用户界面的验证方式

  系统提供密码验证和 AAA 验证两种方式。用户可根据需要任意选择一种方式。

  - 密码验证

    1. 执行命令 **system-view**，进入系统视图。
    2. 执行命令 **user-interface vty** *first-ui-number* [*last-ui-number*]，进入 VTY 用户界面视图。
    3. 执行命令 **authentication-mode password**，设置用户验证方式为密码验证，并同时配置验证密码。
    4. （可选）执行命令 **set authentication password cipher** *password*，修改用户界面的验证密码。

       通过此命令可修改密码为明文或密文密码，但要确保当前用户界面的验证方式是密码验证，才可执行此命令。

- AAA 验证

  用户界面验证方式配置为 AAA 验证时，必须指定本地用户的接入类型。

  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **aaa**，进入 AAA 视图。
  3. 执行命令 **local-user** *user-name* **password** *password*，配置本地用户名和密码。
  4. 执行命令 **local-user** *user-name* **service-type telnet**，配置本地用户的接入类型为 Telnet。
  5. 执行命令 **quit**，退出 AAA 视图。
  6. 执行命令 **user-interface vty** *first-ui-number* [*last-ui-number*]，进入 VTY 用户界面视图。
  7. 执行命令 **authentication-mode aaa**，设置用户验证方式为 AAA 验证。

----结束

5.3.3 使能 Telnet 服务器功能

用户终端建立与路由器的 Telnet 连接之前，需要首先开启路由器 Telnet 服务器功能。

背景信息

缺省情况下，路由器的 Telnet 服务功能是开启的。

请在作为 Telnet 服务器的路由器上进行如下的配置。

操作步骤

步骤 1 使能 Telnet 服务。根据网络协议基于 IPv4 还是 IPv6，选择执行如下步骤之一。

- 网络协议基于 IPv4
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **telnet server enable**，使能 Telnet 服务。
- 网络协议基于 IPv6
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **telnet ipv6 server enable**，使能 Telnet 服务。

     说明

     - 执行命令 **undo telnet [ipv6] server enable** 关闭 Telnet 服务器时，如果当前有通过 telnet 登录的用户在线，该命令执行不成功。
     - 关闭 Telnet 服务功能后，将不能通过 Telnet 方式登录设备，只能通过 SSH 或异步串口等其他方式登录设备。

----结束

5.3.4 用户通过终端 Telnet 登录到系统

当通过 Console 口登录设备完成相关配置后，用户可以使用 Telnet 协议从终端登录到远端设备，实现对设备的远程维护。

背景信息

从终端通过 Telnet 访问系统，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。

请在用户终端上进行以下配置。

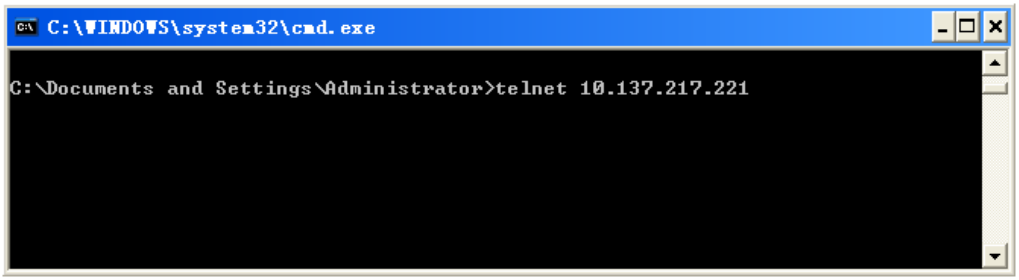
操作步骤

步骤 1 进入 Windows 的命令行提示符。

步骤 2 执行 Windows 命令 **telnet** *ip-address*，通过 Telnet 方式登录设备。

1. 键入 Telnet 服务器的 IP 地址。

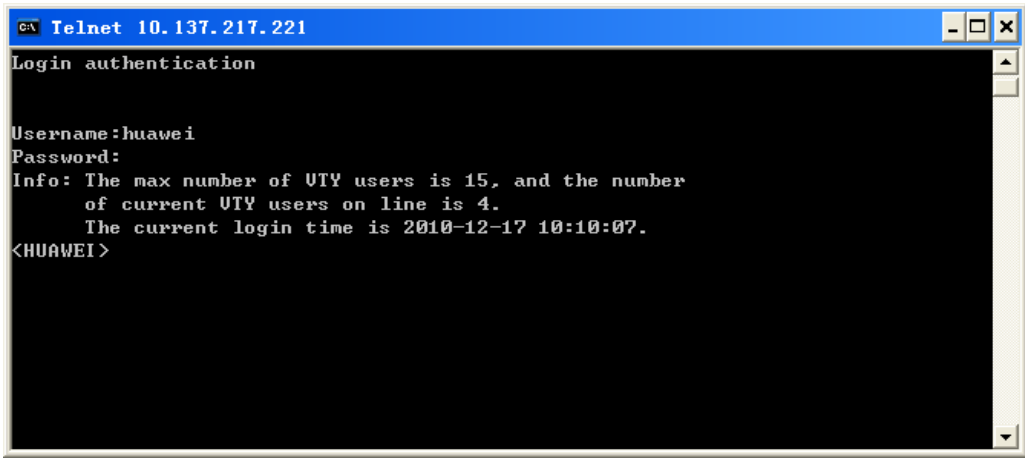
图 5-4 Windows 的命令行提示符



2. 按 Enter 键，出现用户视图的命令行提示符，如<HUAWEI>，至此用户登录到了 Telnet 服务器。

   如果设备配置了密码认证方式或 AAA 认证方式，设备将要求用户输入登录的用户名和密码，正确输入用户名和密码并按 Enter 键后，将出现用户视图的命令行提示符，如图 5-5 所示。

图 5-5 登录示意图



----结束

5.3.5 检查配置结果

用户通过 Telnet 登录系统配置成功后，可以查看到当前用户界面连接情况、每个用户界面连接情况、以及当前建立的所有 TCP 连接情况等内容。

前提条件

已完成用户通过 Telnet 登录系统的所有配置。

操作步骤

- 使用 **display users [all]**命令查看用户界面连接情况。
- 使用 **display tcp status** 命令查看当前建立的所有 TCP 连接情况。
- 使用 **display telnet server status** 命令查看 Telnet 服务器的状态和配置信息。

----结束

任务示例

执行命令 **display users**，可以查看当前用户界面的使用信息。

```
<Huawei> display users
  User-Intf   Delay     Type   Network Address     AuthenStatus    AuthorcmdFlag
  34  VTY 0   00:00:12  TEL    10.138.77.38
Username : Unspecified
+ 35  VTY 1   00:00:00  TEL    10.138.77.57
Username : Unspecified
```

执行命令 **display tcp status**，可以看到 TCP 连接状态。**Established** 表示一个 TCP 连接已经建立。

```
<Huawei> display tcp status
TCPCB      Tid/Soid     Local Add:port         Foreign Add:port      VPNID    State
39952df8   36 /1509     0.0.0.0:0              0.0.0.0:0             0        Closed
32af9074   59 /1        0.0.0.0:21             0.0.0.0:0             14849    Listening
34042c80   73 /17       10.164.39.99:23        10.164.6.13:1147      0        Established
```

执行命令 **display telnet server status**，可以看到 Telnet 服务器的状态和配置信息。

```
<Huawei> display telnet server status
TELNET IPV4 server                      :Enable
TELNET server port                      :23
```

5.4 配置用户通过 STelnet 登录系统

STelnet 协议实现在不安全网络上提供安全的远程访问。客户端和服务器之间经过协商，建立安全连接，用户可以像操作 Telnet 一样登录路由器。

5.4.1 建立配置任务

在进行用户通过 STelnet 登录系统的配置前了解此特性的应用环境、配置此特性的前置任务和数据准备，有助于快速、准确地完成配置任务。

应用环境

Telnet 缺少安全的认证方式，而且传输过程采用 TCP 进行明文传输，存在很大的安全隐患。与 Telnet 相比，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。SSH 协议支持 STelnet、Sftp。

STelnet 是一种安全的 Telnet 服务，SSH 用户可以像使用 Telnet 服务一样操作 STelnet 服务。

前置任务

在配置用户通过 STelnet 登录系统之前，必须通过 Console 口登录设备，更改设备的缺省配置，以便用户能够通过 Telnet 方式远程登录设备并实现管理和维护。更改的缺省配置如下：

- 配置设备管理网口的 IP 地址，确保终端和登录的设备之间路由可达。
- **配置 VTY 用户界面的用户验证方式和优先级**，实现远程管理和维护设备。
- **配置 VTY 用户界面支持 SSH 协议**、、**配置 SSH 用户并指定服务方式包含 STelnet**
  使能 STelnet 服务器功能，以便用户能够通过 STelnet 方式远程登录设备。

数据准备

在配置用户通过 STelnet 登录系统之前，需准备以下数据。

序号	数据
1	用户验证方式、用户名、密码、（可选）VTY 类型用户界面的最大个数、（可选）对 VTY 类型用户界面呼入呼出进行限制的 ACL 号、（可选）终端用户超时断开时间、（可选）终端屏幕的显示行数和历史命令缓冲区大小
2	SSH 用户的用户名和密码、认证方式、服务方式、为 SSH 用户分配的对端 RSA 公钥名
3	（可选）SSH 服务器名称、SSH 服务器当前监听的端口号、STelnet 客户端到 SSH 服务器端的首选加密算法、SSH 服务器端到 STelnet 客户端的首选加密算法、STelnet 客户端到 SSH 服务器端的首选 HMAC 算法、SSH 服务器端到 STelnet 客户端的首选 HMAC 算法、首选密钥交换算法、出接口名称、源地址

5.4.2 配置 VTY 用户界面的用户级别和验证方式

缺省情况下，VTY 用户界面的用户级别是 0，为了实现通过 STelnet 方式远程登录设备维护和管理设备，必须先通过 Console 口登录设备，更改用户级别并配置用户验证方式。

背景信息

VTY 用户界面的其他属性在设备上都有缺省值，用户一般不需要另外配置。但是可以根据用户使用需求，配置相关属性。具体配置请参见**配置 VTY 用户界面**。

以下配置无顺序关系，但是都必须配置。

操作步骤

- 配置 VTY 用户界面的用户优先级
  1. 执行命令 **system-view**，进入系统视图。

2. 执行命令 **user-interface vty** *first-ui-number* [*last-ui-number*]，进入 VTY 用户界面视图。
3. 执行命令 **user privilege level** *level*，设置用户优先级。

   缺省情况下，VTY 用户界面的用户级别是 0。VTY 用户界面的用户级别和命令级别对应关系如表 5-3 所示。

表 5-3 用户级别和命令级别对应关系表

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，比如管理配置文件中的 display current-configuration 命令和 display saved-configuration 命令是 3 级管理级。各命令的级别请参见《*Huawei AR3200 系列 企业路由器 命令参考*》手册。
2	0、1、2	配置级	业务配置命令，包括路由、各个网络层次的命令，向用户提供直接网络服务。
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、配置文件切换命令、备板控制命令、用户管理命令、命令级别设置命令、系统内部参数设置命令；用于业务故障诊断的 debugging 命令等。

说明

- 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，从而保证了设备的安全性。
- 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级别为准。

- 配置 VTY 用户界面的验证方式
  - AAA 验证

    用户界面验证方式配置为 AAA 验证时，必须指定本地用户的接入类型。

    1. 执行命令 **system-view**，进入系统视图。
    2. 执行命令 **aaa**，进入 AAA 视图。
    3. 执行命令 **local-user** *user-name* **password** *password*，配置本地用户名和密码。
    4. 执行命令 **local-user** *user-name* **service-type ssh**，配置本地用户的接入类型为 SSH。
    5. 执行命令 **quit**，退出 AAA 视图。
    6. 执行命令 **user-interface vty** *first-ui-number* [*last-ui-number*]，进入 VTY 用户界面视图。
    7. 执行命令 **authentication-mode aaa**，设置用户验证方式为 AAA 验证。

----结束

5.4.3 配置 VTY 用户界面支持 SSH 协议

当用户通过 STelnet 方式登录设备时，需要配置 VTY 用户界面支持 SSH 协议。

背景信息

缺省情况下，用户界面支持的协议是 Telnet。如果不配置某个或某几个用户界面支持 SSH 协议，则用户不能通过 STelnet 方式登录设备。

说明

如果配置用户界面支持的协议是 SSH，必须设置 VTY 用户界面验证方式为 AAA 验证，否则 **protocol inbound ssh** 将不能配置成功。

请在作为 SSH 服务器的设备上进行如下的配置。

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 **user-interface vty** *first-ui-number* [*last-ui-number*]，进入 VTY 用户界面视图。

步骤 3 执行命令 **authentication-mode aaa**，设置验证方式为 AAA 验证。

步骤 4 执行命令 **protocol inbound ssh**，配置 VTY 支持 SSH 协议。

----结束

5.4.4 配置 SSH 用户并指定服务方式包含 STelnet

通过 STelnet 方式登录路由器时，必须要配置 SSH 用户、产生本地 RSA 密钥对、设置用户验证方式以及指定 SSH 用户的服务方式。

背景信息

- SSH 支持 RSA、password、password-rsa 和 all 四种认证方式。需要在 AAA 视图下创建同名的本地用户。
- 产生本地 RSA 密钥对是成功完成 SSH 登录的首要操作。如果 SSH 用户使用 password 验证，则需要在 SSH 服务器端生成本地 RSA 密钥。如果 SSH 用户使用 RSA 验证，则在服务器端和客户端都需要生成本地 RSA 密钥。

说明

password-rsa 认证需要同时满足 password 认证和 RSA 认证，all 认证是指 password 认证和 RSA 认证方式满足其中一种即可。

请在作为 SSH 服务器的路由器上进行如下的配置。

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 **aaa**，进入 AAA 视图。

步骤 3 执行命令 **local-user** *user-name* **password** *password*，配置本地用户名和密码。

步骤 4 执行命令 **quit**，退出 AAA 视图。

步骤 5 执行命令 **rsa local-key-pair create**，产生本地 RSA 密钥对。

说明

- 在进行其它 SSH 配置之前，必须完成 **rsa local-key-pair create** 配置，生成本地密钥对。
- 密钥对生成后，可以执行 **display rsa local-key-pair public** 命令查看本地密钥对中的公钥部分信息。

步骤 6 执行命令 **ssh user** *user-name* **authentication-type** { **password** | **rsa** | **password-rsa** | **all** }，配置 SSH 用户的认证方式。

根据实际配置需要，选择如下操作之一：

- 配置对 SSH 用户进行 Password 验证
  - 执行命令 **ssh user** *user-name* **authentication-type password**，对 SSH 用户配置 Password 验证。
- 配置对 SSH 用户进行 RSA 验证

1. 执行命令 **ssh user** *user-name* **authentication-type rsa**，对 SSH 用户配置 RSA 验证。
2. 执行命令 **rsa peer-public-key** *key-name*，进入公共密钥视图。
3. 执行命令 **public-key-code begin**，进入公共密钥编辑视图。
4. 输入 *hex-data*，编辑公共密钥。

   说明

   - 进入公共密钥编辑视图后，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 的客户端软件随机生成。具体操作参见相应的 SSH 客户端软件的帮助文档。
   - 进入公共密钥编辑视图后，即可将客户端上产生的 RSA 公钥传送到服务器端。请采用拷贝粘贴方式将 RSA 公钥配置到作为 SSH 服务器的路由器上。
5. 执行命令 **public-key-code end**，退出公共密钥编辑视图。
   - 如果未输入合法的密钥编码 *hex-data*，执行 **peer-public-key end** 后，将无法生成密钥。
   - 如果步骤 b 中指定的密钥 *key-name* 已经在别的窗口下被删除，再执行 **peer-public-key end** 时，系统会提示：密钥已经不存在，此时直接退到系统视图。
6. 执行命令 **peer-public-key end**，退出公共密钥视图，回到系统视图。
7. 执行命令 **ssh user** *user-name* **assign rsa-key** *key-name*，为 SSH 用户分配公钥。

步骤 7（可选）配置 SSH 用户基本验证信息

1. 执行命令 **ssh server rekey-interval** *interval*，设置服务器密钥的更新时间。

   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。
2. 执行命令 **ssh server auth-timeout** *timeout_interval*，设置 SSH 认证超时时间。

   缺省情况下，SSH 连接认证超时时间为 60 秒。
3. 执行命令 **ssh server authentication-retries** *auth-times*，设置 SSH 验证重试次数。

   缺省情况下，SSH 连接的验证重试次数为 3。

----结束

5.4.5 使能 STelnet 服务器功能

缺省情况下，STelnet 服务器功能未使能。用户终端通过 STelnet 登录设备之前，必须通过 Console 口登录设备，开启设备的 STelnet 服务器功能。

背景信息

缺省情况下，设备的 STelnet 服务器功能没有使能，只有使能了此功能后，客户端才能以 STelnet 方式与设备建立连接。

请在作为 SSH 服务器的设备上进行如下的配置。

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 **stelnet server enable**，使能 STelnet 服务器功能。

缺省情况下，STelnet 服务器功能未使能。

----结束

5.4.6 用户通过终端 STelnet 登录到系统

当通过 Console 口登录设备完成相关配置后，用户可以使用 SSH 协议从终端登录到远端设备，实现对设备的远程维护。

背景信息

从终端通过 STelnet 登录设备，可以选择使用第三方软件。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。

在用户终端上安装 OpenSSH 软件后，请在用户终端上进行以下配置。

说明

OpenSSH 软件的安装请参考该软件的安装说明。

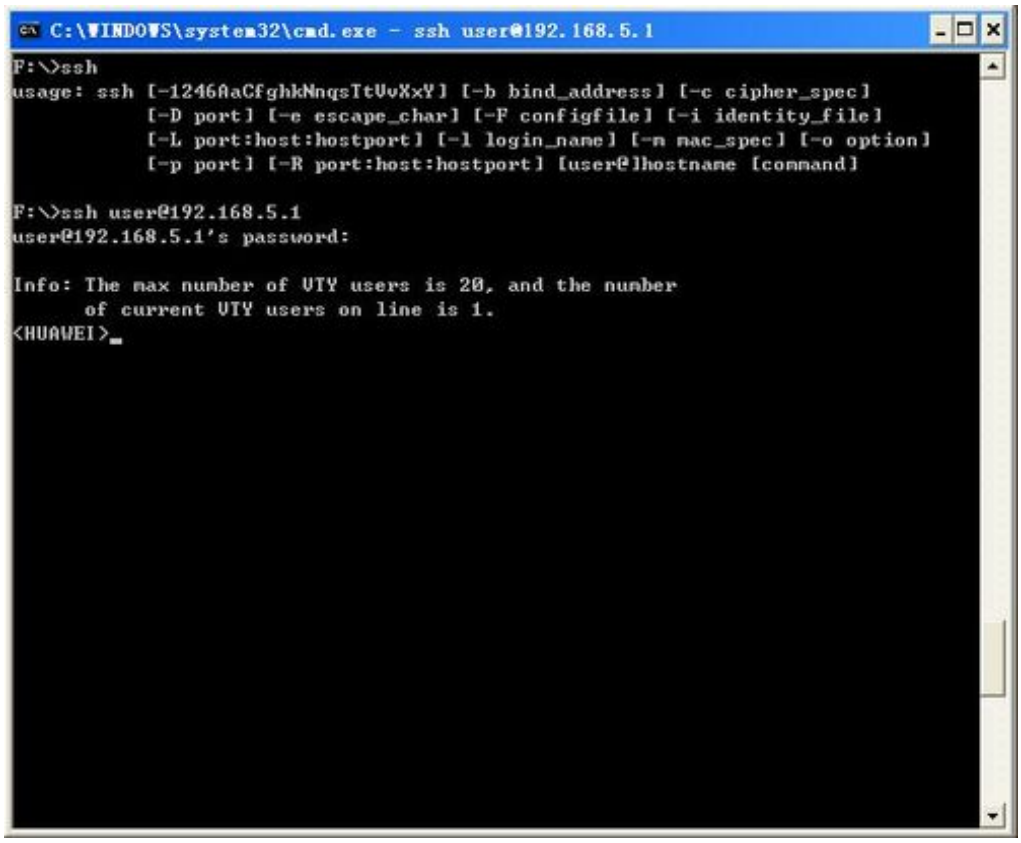
使用 OpenSSH 软件从终端通过 STelnet 登录到系统时，需要使用 OpenSSH 的命令，命令的使用可以参见该软件的帮助文档。

操作步骤

步骤 1 进入 Windows 的命令行提示符。

步骤 2 执行 OpenSSH 命令，通过 STelnet 方式登录设备。

图 5-6 通过 STelnet 方式登录设备示意图



----结束

5.4.7 （可选）配置 STelnet 服务器参数

用户可以配置是否使能兼容低版本 SSH 协议，配置或变更 SSH 服务器监听端口号以及配置服务器密钥对更新时间、指定源接口。

背景信息

服务器参数如表 5-4 所示。

表 5-4 服务器参数

服务器参数	说明
兼容低版本 SSH 协议	SSH 协议有 SSH1.X（SSH2.0 之前的版本）和 SSH2.0 版本。SSH2.0 协议相比 SSH1.X 协议来说，在结构上做了扩展，可以支持更多的认证方法和密钥交换方法，同时提高了服务能力（如 SFTP）。AR3200 支持大于等于 1.3 且小于等于 2.0 之间的 SSH 协议版本。

服务器参数	说明
监听端口号	缺省情况下，SSH 服务器端监听端口号是 22，此时登录路由器可以不指定端口号。但如果使用标准的监听端口号，可能会有攻击者不断访问此端口，导致带宽和服务器性能的下降，造成其他正常用户无法访问。所以可以重新配置 SSH 服务器的监听端口号，攻击者不知道 SSH 监听端口号的更改，有效防止了攻击者对 SSH 服务标准端口的访问，确保了安全性。
服务器密钥对更新时间	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。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 配置 SSH 服务器参数，根据需要，可执行如表 5-5 中的一个或多个操作。

表 5-5 配置服务器参数

服务器参数	操作
使能兼容低版本功能	执行命令 **ssh server compatible-ssh1x enable** 缺省情况下，SSH2.0 协议的服务器是兼容 SSH1.X 服务器功能的。如果不允许 SSH1.3 ～ SSH1.99（SSH 的协议版本号大于等于 1.3 且小于等于 1.99）的客户端登录，则执行 **undo ssh server compatible-ssh1x enable**，去使能兼容低版本功能。
配置 SSH 服务器监听端口号	执行命令 **ssh server port** *port-number* 如果配置了新的监听端口号，SSH 服务器端先断开当前已经建立的所有 STelnet 和 SFTP 连接，然后使用新的端口号开始监听。缺省情况下，SSH 服务器端监听端口号是 22。
配置服务器密钥对更新时间	执行命令 **ssh server rekey-interval** *rekey-interval* 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。

----结束

5.4.8 检查配置结果

用户通过 STelnet 登录系统配置成功后，可以查看到 SSH 服务器的全局配置信息等内容。

前提条件

已完成用户通过 STelnet 登录系统的所有配置。

操作步骤

- 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 服务器端查看与 SSH 客户端连接的会话信息。

----结束

任务示例

运行命令 **display ssh user-information** *username*，可以查看指定 SSH 用户的信息。

```
<Huawei> display ssh user-information client001
      Sftp-directory         : -
      Service-type           : sftp
------------------------------------------------------------------------------
 Username         Auth-type          User-public-key-name
 ------------------------------------------------------------------------------
 guest            password           null
 rsa              rsa                RsaKey001
 password         password           null
 ------------------------------------------------------------------------------
```

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。

运行命令 **display ssh server status**，可以查看 SSH 服务器全局配置信息。

```
<Huawei> 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                       :Enable
```

运行命令 **display ssh server session**，可以查看 SSH 服务器与客户端连接的会话信息。

```
<Huawei> display ssh server session
  ------------------------------------------------------------------
Conn    Ver   Encry     State  Auth-type        Username
------------------------------------------------------------------
VTY 0  1.5   BLOWFISH  run    password         john

------------------------------------------------------------------
```

5.5 登录后的常用操作

登录路由器后，用户可以根据需求进行如下的操作，如切换用户级别、锁定用户终端界面等。

5.5.1 建立配置任务

在进行登录后的常用操作前了解此特性的应用环境、配置此特性的前置任务和数据准备，有助于快速、准确地完成配置任务。

应用环境

为了保证操作用户能够安全管理路由器，可以配置用户级别切换、在用户界面间发送消息等。

前置任务

在进行登录后的常用操作之前，需要完成以下任务：

- 用户终端登录到路由器

数据准备

在进行登录后的常用操作之前，需要准备以下数据。

序号	数据
1	用户级别切换密码
2	用户界面类型和编号
3	要发送的消息内容

5.5.2 切换用户级别

如果用户以较低级别的身份登录到路由器后，需要切换到较高级别的用户身份进行操作，必须输入正确的级别切换口令。该口令需要事先配置。

背景信息

为了防止未授权用户的非法侵入，在从低级别用户切换到高级别用户时，要进行用户身份验证，即需要输入切换用户级别的口令。

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 **super password** [**level** *user-level*] **cipher** *password*，配置切换用户级别的口令。

设置了密码后，无法从系统取回。请妥善保管，以免遗忘或者遗失。

步骤 3 执行命令 **quit**，返回用户视图。

步骤 4 执行命令 **super** [*level*]，切换用户级别。

缺省情况下，切换的用户级别是 3 级。

步骤 5 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。

----结束

5.5.3 锁定用户终端界面

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。

背景信息

用户界面包括 Console 用户界面和 VTY 用户界面。

操作步骤

步骤 1 执行命令 **lock**，锁定用户终端界面。

步骤 2 根据系统提示，输入解除锁定的口令，并确认口令。

```
<Huawei> lock
Enter Password:
Confirm Password:
```

锁定成功后，系统将提示终端界面已经锁定。

锁定用户界面时，需要输入口令并确认。解除锁定时，必须输入正确的口令。

----结束

5.5.4 发送消息给其它用户界面

用户可以在当前的用户界面发送消息给其他用户界面，实现用户界面间的传递消息。

背景信息

当有多个用户登录路由器进行配置时，如果有用户想通知其他用户一些注意信息时，可以在当前用户界面发送消息给其他的用户界面。

操作步骤

步骤 1 执行命令 **send** { **all** | *ui-type ui-number* | *ui-number1* }，设置在用户界面间传递消息。

步骤 2 根据系统提示，输入要传递的消息。使用“Ctrl_Z”或回车键结束输入，使用“Ctrl_C”中止本次操作。

步骤 3 根据系统提示，选择是否需要发送消息。输入“Y”发送消息，输入“N”取消发送。

----结束

5.5.5 显示在线用户

用户登录系统后，可以查看在线用户的信息。

背景信息

用户信息包括用户的用户名、地址等登录信息，以及用户的验证和授权信息等。

操作步骤

- 使用 **display users [all]**命令显示用户界面的使用信息。

  参数 **all** 表示显示所有用户界面的用户登录信息。

----结束

5.6 配置举例

配置用户通过 Console 口、Telnet、STelnet 登录系统的示例。请结合配置流程图了解配置过程。配置示例中包括组网需求、配置注意事项和配置思路等。

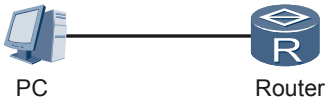
5.6.1 配置用户通过 Console 口登录系统示例

在本示例中，在 PC 端进行登录的设置，实现通过 Console 口登录路由器。

组网需求

如果用户修改了路由器 Console 用户界面配置参数的默认值，则用户下次通过 Console 口登录路由器时，必须在 PC 端进行相应参数的设置。

图 5-7 配置通过 Console 口登录组网图



配置思路

1. 通过 Console 口连接 PC 和路由器。
2. 在 PC 端进行登录的设置。
3. 登录路由器。

说明

本例中以超级终端为例介绍。

数据准备

终端通信参数（波特率为 4800bps、数据位为 7、奇偶校验为 even、停止位为 2 和流控方式为无）。

操作步骤

步骤 1 建立本地配置环境，只需将 PC（或终端）的串口通过标准 RS-232 配置电缆与路由器的 Console 口连接。

步骤 2 在 PC 上运行终端仿真程序。设置终端通信参数为 4800bps、7 位数据位、校验位 even、2 位停止位和无流控方式，如图 5-8 至图 5-10 所示。

图 5-8 新建连接

图 5-9 连接端口设置

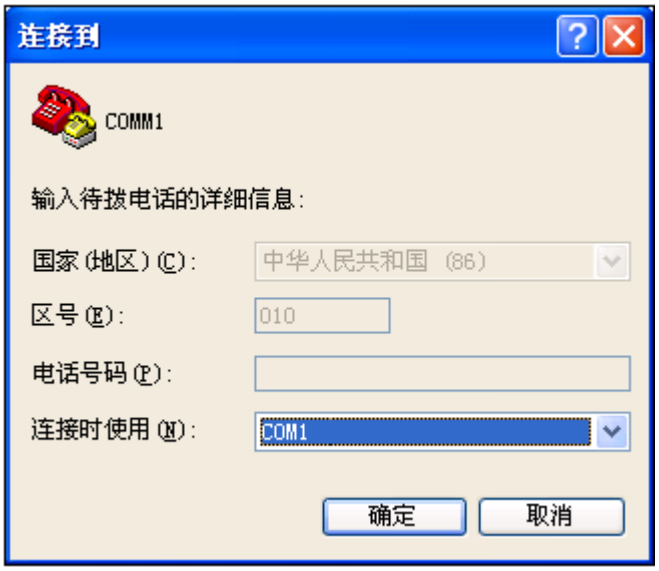
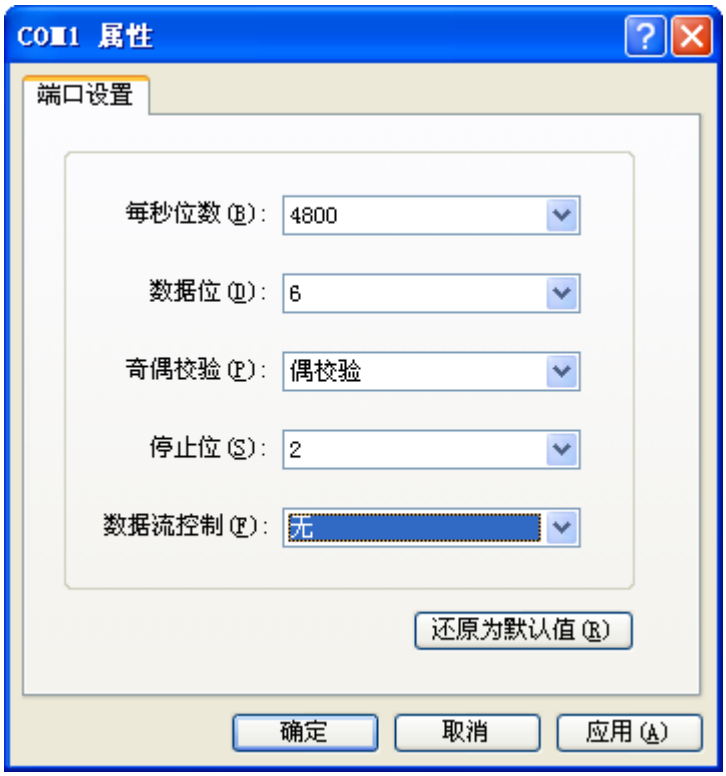


图 5-10 端口通信参数设置



步骤 3 路由器上电自检，系统自动进行配置，自检结束后提示用户键入回车，直到出现“Password: ”，用户输入正确的验证密码再次键入回车后，系统出现命令行提示符（如<Huawei>），表明用户已成功登录系统。

此时可以键入命令，查看路由器运行状态，或对路由器进行配置。

----结束

5.6.2 配置通过 Telnet 登录示例

在本示例中，通过配置用户登录参数，实现从客户端登录路由器。

组网需求

用户可以通过 PC 等配置终端登录到其它网段上的路由器，进行远程维护。

图 5-11 配置通过 Telnet 登录组网图

配置思路

1. 建立物理连接
2. 配置用户登录参数
3. 从客户端登录路由器

数据准备

- PC 的 IP 地址
- 待配置路由器以太网接口的 IP 地址
- Telnet 访问的用户信息（用户名、口令和验证方式）
- 确保 PC 与 Target 路由器之间路由可达

操作步骤

步骤 1 在 PC 端和路由器端分别和网络连接。

步骤 2 在 Target 路由器端配置登录用户参数。

配置登录地址

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ip address 202.38.160.92 255.255.0.0
[Huawei-GigabitEthernet1/0/0] quit
```

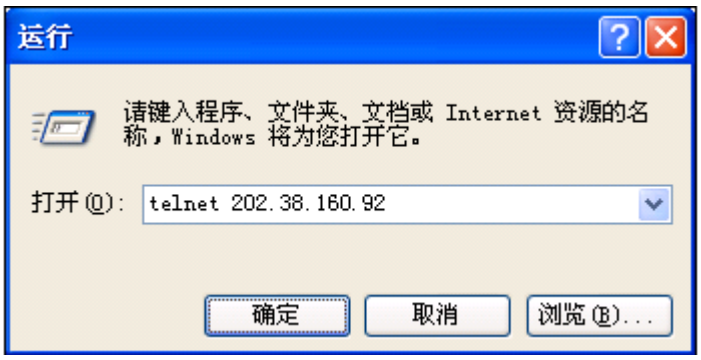
配置登录验证方式

```
[Huawei] aaa
[Huawei-aaa] local-user huawei password hello
[Huawei-aaa] local-user huawei service-type telnet
[Huawei-aaa] local-user huawei privilege level 3
[Huawei-aaa] quit
[Huawei] user-interface vty 0 4
[Huawei-ui-vty0-4] authentication-mode aaa
```

步骤 3 配置客户端登录

在 PC 上运行 Telnet（以 Windows 操作系统为例），如下图所示。

图 5-12 PC 上的 Telnet 界面



单击<确定>。

在登录窗口输入用户名和口令，验证通过后，出现用户视图的命令行提示符，如<Huawei>。至此用户进入了用户视图配置环境。

----结束

5.6.3 配置用户通过 STelnet 登录系统示例

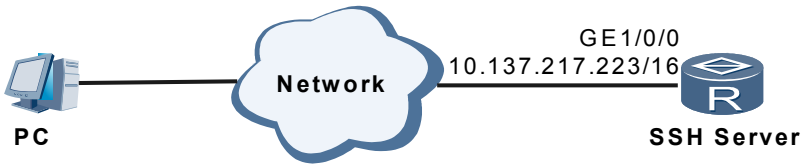
在本示例中，通过在 SSH 服务器端生成本地密钥对，并在 SSH 服务器端配置 SSH 用户的用户名和密码，使能 Stelnet 服务，实现 Stelnet 客户端连接 SSH 服务器。

组网需求

如图 5-13 所示，在作为 SSH 服务器的路由器上使能 STelnet 服务器功能后，STelnet 客户端 PC 可以通过 Password、RSA、password-rsa 或 all 认证的方式登录到 SSH 服务器端。

配置用户通过 password 认证方式登录 SSH Server。

图 5-13 配置用户通过 STelnet 登录系统组网图



配置思路

采用如下的思路配置 PC 作为 STelnet 客户端连接 SSH 服务器：

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，用户名和密码。
4. 在 SSH 服务器端使能 STelnet 服务器功能以及配置用户的服务类型。

数据准备

为完成此配置例，需准备如下的数据：

- SSH 用户的认证方式为 password，用户名为“client001”，密码为“huawei”。
- client001 的用户级别为 3。
- SSH 服务器端的 IP 地址为 10.137.217.223。

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] rsa local-key-pair create
The key name will be: Huawei_Host
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
```

```
      It will take a few minutes.
Input the bits in the modulus[default = 512]: 768
Generating keys...
.......++++++++++++
..........++++++++++++
.....................................++++++++
......++++++++
```

步骤 2 在服务器端配置 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
```

说明

若配置登录协议为 SSH，则 AR3200 设备将自动禁止 Telnet 功能。

步骤 3 在服务器端配置 SSH 用户的用户名和密码

```
[SSH Server] aaa
[SSH Server-aaa] local-user client001 password huawei
[SSH Server-aaa] local-user client001 privilege level 3
[SSH Server-aaa] local-user client001 service-type ssh
[SSH Server-aaa] quit
```

步骤 4 配置 SSH 用户的验证方式为 password

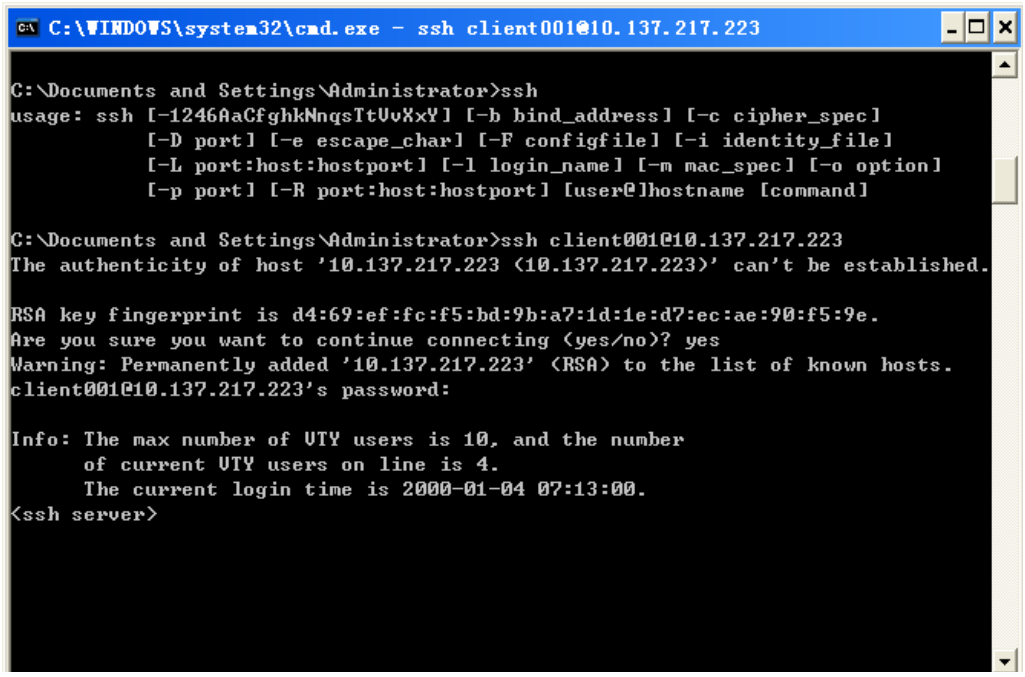
```
[SSH Server] ssh user client001 authentication-type password
```

步骤 5 使能 STelnet 服务器功能

```
[SSH Server]stelnet server enable
```

步骤 6 验证配置结果

通过 OpenSSH 软件实现访问 SSH 服务器



----结束

配置文件

- SSH 服务器的配置文件

```
#
 sysname SSH Server
#
aaa
 local-user client001 password N`C55QK<`=/Q=^Q`MAF4<1!!
 local-user client001 privilege level 3
 local-user client001 service-type ssh
#
interface GigabitEthernet1/0/0
 ip address 10.137.217.223 255.255.0.0
#
 ssh user client001 authentication-type password
#
user-interface vty 0 4
 authentication-mode aaa
 protocol inbound ssh
#
return
```

6 管理文件系统

关于本章

在路由器的存储设备中保存着路由器运行过程中所需要的文件，用户可以通过文件系统来管理路由器中的这些文件以及目录，实现对文件的显示、移动、删除等操作。

6.1 管理文件简介
路由器通过文件系统的方式有效地管理着设备上的所有文件。

6.2 通过登录系统进行文件操作
用户可以通过登录系统进行文件操作，包括管理存储设备、管理目录和管理文件。

6.3 通过 FTP 进行文件操作
用户可以使用 FTP 协议进行本地和远程主机之间的文件操作，尤其在进行版本升级、日志下载、文件传输和配置保存等业务操作中得到广泛应用。

6.4 通过 SFTP 进行文件操作
SFTP 使得用户可以从远端安全登录路由器进行文件管理，这样使远程系统升级等需要文件的传送的地方，增加了数据传输的安全性。

6.5 配置举例
配置用户通过登录系统、FTP、SFTP、FTPS 进行文件操作的示例。请结合配置流程图了解配置过程。配置示例中包括组网需求、配置注意事项和配置思路等。

6.1 管理文件简介

路由器通过文件系统的方式有效地管理着设备上的所有文件。

6.1.1 文件系统概述

文件系统是指对存储设备中文件、目录的管理，包括创建、删除、修改、更名文件和目录，以及显示文件的内容。

文件系统实现两类功能：管理存储设备、管理保存在存储设备中的文件。

登录系统进行文件操作

通过 Console 口、Telnet 或 STelnet 方式登录路由器后，可以对存储设备、目录和文件进行管理。

- 存储设备

  存储设备是存储信息的硬件设备。

  路由器目前支持的存储设备包括 Flash、U 盘和 SD 卡。
- 文件

  文件是系统存储信息，并对信息进行管理的一种机制。
- 目录

  目录是一种将整个文件集合进行组织的机制，是文件逻辑上的容器。

6.1.2 管理文件的主要方式

用户可以通过 FTP、SFTP、FTPS 等方式进行文件操作，实现对文件的管理。

通过 FTP 进行文件操作

FTP 协议是一种基于 TCP/IP 协议族的 Internet 标准应用协议，用于在远端服务器和本地客户端之间传输文件。FTP 采用两条 TCP 连接将一个文件从一个系统复制到另一个系统，连接通常是以客户－服务器的方式建立，这两条 TCP 连接分别是控制连接（服务器端为 21 号端口）和数据连接（服务器端为 20 号端口）。

- 控制连接：将命令从客户端传送到服务器端，并传回服务器的应答，IP 对控制连接的服务特点是最大限度地减少延迟。
- 数据连接：在客户和服务器之间传输数据，因此 IP 对数据连接的服务特点是最大限度地提高吞吐量。

FTP 有两种文件传输模式：

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

设备提供的 FTP 功能包括：

- 设备作为 FTP 客户端：用户在 PC 上通过终端仿真程序或 Telnet 程序连接到设备，执行 **ftp** 命令建立设备与远程 FTP 服务器的连接并访问远程主机上的文件，对远程主机上的文件进行操作。

- 设备作为 FTP 服务器：用户运行 FTP 客户端程序，登录设备并进行文件操作。
  用户登录前，网络管理员需要事先配置好 FTP 服务器的 IP 地址。

通过 SFTP 进行文件操作

SFTP 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送等操作，为数据传输提供了更高的安全保障。同时，由于设备支持作为客户端的功能，用户可以从本地设备安全登录到远程设备上，进行文件的安全传输。

当 SFTP 服务器端或是与客户端的连接存在故障时，客户端需要及时了解故障的存在，并主动断开连接。为了实现上述目标，客户端以 SFTP 方式登录服务器时，配置无数据接收时发送 Keepalive 报文的间隔时间和服务器端的无应答限制次数：

- 如果在指定时间间隔内未收到数据，客户端将发送 Keepalive 报文至服务器端。
- 如果服务端的无应答次数超过配置的次数，客户端将主动断开连接。

通过 FTPS 进行文件操作

FTPS 将 FTP 和 SSL 结合，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，从而实现了对设备的安全管理。

传统的 FTP 不具备安全机制，采用明文的形式传输数据。如果 FTP 服务器设置了登录用户名和密码，则 FTP 服务器可以验证客户端的身份，但是客户端不能验证服务器的身份，无法防止传输的数据被篡改等，存在很大的安全隐患。在 FTP 服务器上部署 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 可以为 FTP 服务器提供安全连接，从而很大程度上改善了 FTP 服务器安全性问题。

缺省情况下，用户不能通过 FTPS 方式直接登录设备。如果需要通过 FTPS 方式登录设备，必须完成以下操作：

- 先通过 Console 口本地登录设备，将数字证书上传到作为 FTPS 服务器的设备上，并拷贝到系统目录下名为 security 的子目录内。
- PC 上已经安装支持 SSL 的 FTP 客户端软件。

6.2 通过登录系统进行文件操作

用户可以通过登录系统进行文件操作，包括管理存储设备、管理目录和管理文件。

6.2.1 建立配置任务

在通过登录系统进行文件操作之前，完成前置任务和数据准备，有助于快速、准确地完成各项属性的配置任务。

应用环境

当路由器无法正常进行信息的存取，需要对异常的存储设备进行修复或用户需要对路由器上的文件或目录进行操作管理时，可以通过直接登录系统的方式实现以上需求。特别是对存储设备的操作需要通过此种方式。

前置任务

在通过登录系统进行文件操作之前，需要完成以下任务：

- 已正确连接客户端与服务器端，客户端可以登录服务器

数据准备

在配置通过登录系统进行文件操作之前，需要准备以下数据。

序号	数据
1	存储设备的名称
2	目录名
3	文件名

6.2.2 管理存储设备

当路由器的存储设备的文件系统出现异常时，可以通过修复或格式化来实现对存储设备的管理。

背景信息

当某存储设备上的文件系统出现异常时，路由器的终端会给出提示信息，建议修复异常。

说明

存储设备可以是 Flash，SD 卡或者 U 盘。缺省情况下，设备内置了 Flash 和一块 SD 卡（槽位号为 sd1）。

在缺省配置的情况下，用户最多可以再扩充两个 U 盘(槽位号分别为 usb0 和 usb1)。

请使用经过华为认证的存储设备。

当文件系统的异常无法修复或者确认不再需要存储设备上的所有数据时，可格式化存储设备。

注意

格式化存储设备，会导致数据无法恢复，请慎用。

操作步骤

- 执行命令 **fixdisk** *device-name*，修复文件系统异常的存储设备。

  说明

  执行此命令后，如果仍然收到系统建议修复的信息，则表示物理介质可能已经损坏。

- 执行命令 **format** *device-name*，格式化存储设备。

  说明

  如果执行 **format** *device-name* 命令后，存储设备仍然不可用，则可能是物理原因导致的存储设备不可用。

----结束

6.2.3 管理目录

用户可以通过管理目录在逻辑上将文件分级存放。

背景信息

对目录的管理包括：改变当前目录、显示当前目录、显示目录中的文件和子目录列表以及创建和删除目录。

操作步骤

- 执行命令 **cd** { *directory* | *device-name* }，改变当前所处的目录。
- 执行命令 **pwd**，查看当前所处的目录。
- 执行命令 **dir** [**/all**] [*filename*] [*device-name*]，显示目录中的文件和子目录的列表。
- 执行命令 **mkdir** { *directory* | *device-name* }，创建目录。
- 执行命令 **rmdir** { *directory* | *device-name* }，删除目录。

----结束

6.2.4 管理文件

如果用户需要查看、删除、重命名路由器上的文件时，可以通过文件系统对文件进行相应的操作。

背景信息

- 对文件的管理包括：显示文件的内容、拷贝文件、移动文件、重命名文件、压缩文件、删除文件以及恢复删除的文件、彻底删除回收站中的文件、运行批处理文件和配置文件系统提示方式。
- 当用户需要对某个文件进行操作时，可以执行 **cd** { *directory* | *device-name* }命令，改变当前目录到文件所处的目录。

操作步骤

- 执行命令 **more** [**/binary**] { *filename* | *device-name* } [*offset*] [**all**]，显示文件的内容。

  通过 **more** 命令的参数选择，可以实现对文档的灵活显示方式：

  - 执行 **more** *file-name* 命令，查看文件名为 *file-name* 的文件。此时分屏显示文本文件内容，在当前会话终端上不断输入空格键，可以把当前文件输出完。

    分屏显示的两个前提条件：

    - 用户执行 **screen-length** *screen-length* **temporary** 命令设置的终端屏幕的每屏行数必须大于 0。
    - 文件总行数目大于 *screen-length* 的值。
  - 执行 **more** *file-name offset* 命令，查看文件名为 *file-name* 的文件。此时从文档的 *offset* 字符开始分屏显示文本文件内容，在当前会话终端上不断输入空格键，可以把当前文件输出完。

    分屏显示的两个前提条件：

    - 用户执行 **screen-length** *screen-length* 命令设置的终端屏幕的每屏行数必须大于 0。

- 文件的字符数目减去 *offset* 参数指定的字符数目后，剩余字符行数目必须大于 *screen-length*。

- 执行 **more** *file-name* **all** 命令，查看文件名为 *file-name* 的文件。此时不分屏显示文本文件内容，一次把当前全部显示完。

- 执行命令 **copy** *source-filename destination-filename*，拷贝文件。
- 执行命令 **move** *source-filename destination-filename*，移动文件。
- 执行命令 **rename** *source-filename destination-filename*，重新命名文件。
- 执行命令 **zip** *source-filename destination-filename*，压缩文件。
- 执行命令 **delete** [**/unreserved**] [**/force**] {*filename* | *device-name* } [**all**]，删除文件。

注意

如果使用参数[**/unreserved**]，则删除后的文件不可恢复。

- 执行命令 **undelete** *filename*，恢复删除的文件。

  说明

  如果当前目录不是根目录，对文件的操作要使用绝对路径。

- 执行命令 **reset recycle-bin** [*filename*]，彻底删除回收站中的文件。

  当需要永久删除某一已丢弃的文件时，可以进行彻底删除回收站中的文件的操作。

- 运行批处理文件

  当需要对文件一次进行多项处理时，可以进行运行批处理文件的操作。编辑好的批处理文件要预先保存在路由器的存储设备中。

  如果已经建立好批处理文件，那么可以执行该文件，以实现执行固定任务的自动化。

  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **execute** *filename*，运行批处理文件。

- 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。

  1. 执行 **system-view** 命令，进入到系统视图。
  2. 执行 **file prompt** { **alert** | **quiet** }命令，配置文件系统提示方式。

     缺省情况下，提示方式为 **alert**。

     注意

     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

6.3 通过 FTP 进行文件操作

用户可以使用 FTP 协议进行本地和远程主机之间的文件操作，尤其在进行版本升级、日志下载、文件传输和配置保存等业务操作中得到广泛应用。

6.3.1 建立配置任务

在通过 FTP 进行文件操作配置前了解此特性的应用环境、配置此特性的前置任务和数据准备，有助于快速、准确地完成配置任务。

应用环境

将路由器作为 FTP 服务器。用户通过 FTP 客户端登录到路由器以后，可以在客户端与服务器之间实现远程传输文件。

前置任务

在配置通过 FTP 进行文件操作之前，需要完成以下任务：

- 客户端与路由器路由可达

数据准备

在配置通过 FTP 进行文件操作之前，需要准备以下数据。

序号	数据
1	FTP 用户名和口令、FTP 用户的授权工作目录
2	（可选）FTP 服务器指定监听端口号
3	（可选）FTP 服务器的源地址（或者源接口）、（可选）FTP 服务器的超时断开连接时间
4	FTP 服务器的 IP 地址或主机名

6.3.2 配置 FTP 类型的本地用户

用户可以配置 FTP 用户的验证信息、授权方式和授权目录，保证安全性，无权限的用户将不能访问某些目录。

背景信息

当用户通过 FTP 进行文件操作时，需要在作为 FTP 服务器的路由器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 访问路由器。

请在作为 FTP 服务器的路由器上进行如下的配置。

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 **set default ftp-directory** *directory*，配置 FTP 用户的缺省工作目录。

说明

该步骤只针对 TACACS 用户有效。

步骤 3 执行命令 **aaa**，进入 AAA 视图。

步骤 4 执行命令 **local-user** *user-name* **password** *password*，配置本地用户名和密码。

步骤 5 执行命令 **local-user** *user-name* **privilege level** *level*，配置本地用户级别。

说明

必须将用户级别配置在 3 级及 3 级以上。

步骤 6 执行命令 **local-user** *user-name* **service-type ftp**，配置本地用户的服务类型为 FTP。

步骤 7 执行命令 **local-user** *user-name* **ftp-directory** *directory*，配置 FTP 用户的授权目录。

----结束

6.3.3 （可选）指定 FTP 服务器端口号

用户可以变更 FTP 服务器的监听端口号。变更后，只有知道当前监听端口号的用户才能访问路由器，确保安全性。

背景信息

缺省情况下，FTP 服务器端监听端口号是 21，此时访问路由器可以不指定端口号。但如果使用标准的监听端口号，可能会有攻击者不断访问此端口，导致带宽和服务器性能的下降，造成其他正常用户无法访问。所以可以重新配置 FTP 服务器的监听端口号，攻击者不知道 FTP 监听端口号的更改，有效防止了攻击者对 FTP 服务标准端口的访问。

说明

如果 FTP 服务未使能，用户可以变更 FTP 服务器监听端口号。

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 server** 命令关闭 FTP 服务，再进行端口号变更。

请在作为 FTP 服务器的路由器上进行如下的配置。

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 **ftp** [**ipv6**] **server port** *port-number*，变更 FTP 服务器端口。

如果配置了新的监听端口号，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监听。

----结束

6.3.4 使能 FTP 服务器功能

用户通过 FTP 进行文件操作前需要使能路由器的 FTP 服务器功能。

背景信息

缺省情况下，路由器的 FTP 服务器功能是关闭的，所以使用 FTP 功能前必须要先使能 FTP 服务器的功能。

请在作为 FTP 服务器的路由器上进行如下的配置。

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 **ftp [ipv6] server enable**，启动 FTP 服务器。

说明

当客户端与路由器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，从而保证路由器的安全。

----结束

6.3.5 （可选）配置 FTP 服务器参数

FTP 服务器参数包括 FTP 服务器的源地址和 FTP 连接空闲时间。

背景信息

- 指定 FTP 服务器的源地址，从而限制客户端访问的目的地址，保证安全性。
- 配置 FTP 连接空闲时间，指定时间内没有操作的时候将释放 FTP 连接资源。

请在作为 FTP 服务器的路由器上进行如下的配置。

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 **ftp server-source** { **-a** *source-ip-address* | **-i** *interface-type interface-num* }，配置 FTP 服务器的源地址信息。

配置了 FTP 服务器的源地址信息后，再执行 **ftp** 命令登录服务器时，所输入的服务器源地址必须与该步骤中配置的一致，否则无法成功登录服务器。

步骤 3 执行命令 **ftp [ipv6] timeout** *minutes*，配置 FTP 服务器超时断连时间。

在设定的时间内，FTP 连接始终处于空闲状态时，系统将自动断开 FTP 连接。

缺省情况下，系统的连接空闲时间为 30 分钟。

----结束

6.3.6 （可选）配置 FTP 访问控制

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路由器。

背景信息

当路由器作为 FTP 服务器时，为提高安全性，可以通过配置 ACL 实现只允许满足匹配条件的客户端访问服务器。

请在作为 FTP 服务器的路由器上进行如下的配置。

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 **acl** *acl-number*，进入 ACL 视图。

步骤 3 执行命令 **rule** [*rule-id*] { **deny** | **permit** } [{ **fragment** | **none-first-fragment** } | **source** { *source-address source-wildcard* | **any** } | **time-range** *time-name* | **vpn-instance** *vpn-instance-name*] *，配置 ACL 规则。

说明

- 创建的 ACL 规则默认对所有报文进行 deny 操作。如果需要让报文正常通过，还需要在 ACL 规则中配置 permit 操作。例如，配置丢弃源 IP 为 10.1.1.10 的报文，那么 ACL 中应当定义两条规则：
  - **rule deny source 10.1.1.10 0**
  - **rule permit source any**

  如果没有定义 **rule permit source any**，其他源 IP 地址不是 10.1.1.10 的报文也会被丢弃。
- FTP 只支持基本访问控制列表。

步骤 4 执行命令 **quit**，返回系统视图。

步骤 5 执行命令 **ftp** [**ipv6**] **acl** *acl-number*，配置 FTP 基本访问控制列表。

----结束

6.3.7 用户通过 FTP 软件访问系统

当完成路由器的 FTP 服务器的相关设置后，用户可以通过 FTP 协议从 PC 访问路由器，实现对路由器上文件的管理。

背景信息

从终端通过 FTP 访问路由器，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。

请在 PC 上进行以下操作。

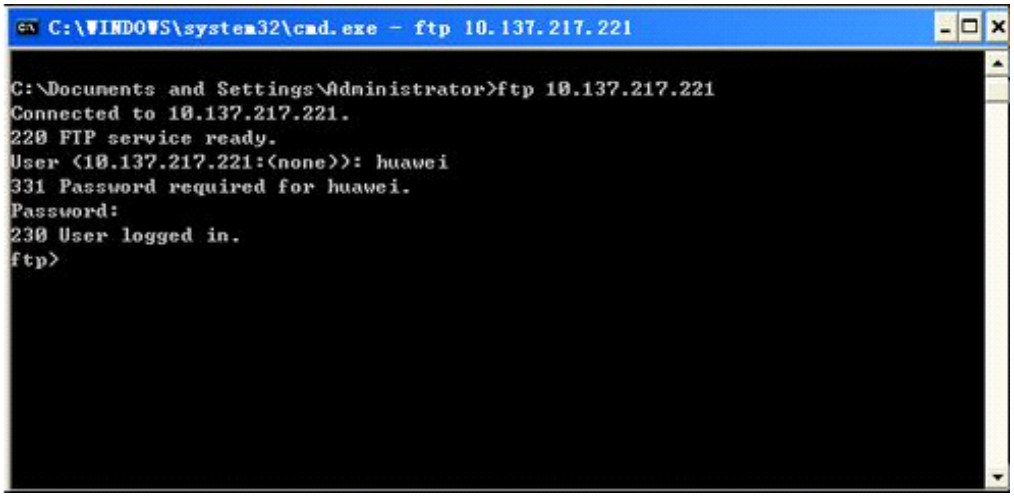
操作步骤

步骤 1 进入 Windows 的命令行提示符。

步骤 2 执行 Windows 命令 **ftp** *ip-address*，通过 FTP 方式登录路由器。

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。

图 6-1 FTP 登录示意图



----结束

6.3.8 用户使用 FTP 命令进行文件操作

当用户成功登录作为 FTP 服务器的路由器后，可以在路由器上执行传输文件、管理服务器目录等操作。

背景信息

用户登录 FTP 服务器后可以进行如下主要操作：

- 配置传输文件的数据类型。
- 将本地的文件上传到远程 FTP 服务器，也可以从 FTP 服务器下载文件并保存在本地。
- 在 FTP 服务器上进行创建、删除等管理目录的操作。
- 可以显示 FTP 服务器上指定远程目录或文件的信息，或者删除 FTP 服务器上的指定文件。

当用户登录 FTP 服务器进入 FTP 客户端视图后，即可在用户终端进行以下一种或几种操作。

操作步骤

- 配置传输文件的数据类型。
  - 执行命令 **ascii** 或 **binary**，配置传输的文件的数据类型为 ASCII 码或者二进制。

    说明

    FTP 支持 ASCII 码、二进制文件类型。二者的区别是:

    - ASCII 传输使用 ASCII 字符，把回车键和换行符分开。
    - 二进制不用转换或格式化就可传字符。

    FTP 传输模式由客户端进行选择，系统默认 ASCII 方式。客户端可使用模式切换命令进行切换（ASCII 和 Binary）。传输文本文件使用 ASCII 方式，传输二进制文件使用 Binary 方式。

- 上传或下载文件。
  - 上传或下载单个文件
    - 执行命令 **put** *local-filename* [*remote-filename*]，将本地的文件上传到远程 FTP 服务器。
    - 执行命令 **get** *remote-filename* [*local-filename*]，从 FTP 服务器下载文件并保存在本地。
- 进行如下一种或多种操作来管理目录。
  - 执行命令 **cd** *pathname*，改变远程 FTP 服务器上的工作路径。
  - 执行命令 **pwd**，显示 FTP 服务器端工作路径。
  - 执行命令 **lcd** [*local-directory*]，显示或者改变 FTP 客户端的工作路径。
  - 执行命令 **mkdir** *remote-directory*，在 FTP 服务器上创建目录。
  - 执行命令 **rmdir** *remote-directory* ，在 FTP 服务器上删除目录。
- 进行如下一种或多种操作来管理文件。
  - 执行命令 **ls** [*remote-filename*] [*local-filename*]，显示 FTP 服务器上指定远程目录或文件的信息。

    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。

    使用参数 *local-filename*，可以将远程文件内容保存在本地另一个文件中。
  - 执行命令 **dir** [*remote-filename*] [*local-filename*]，显示 FTP 服务器上指定远程目录或文件的详细信息。

    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。

    使用参数 *local-filename*，可以将远程文件内容保存在本地另一个文件中。
  - 执行命令 **delete** *remote-filename*，删除 FTP 服务器上指定文件。

    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。

  说明

  FTP 文件操作的其他命令可在 Windows 命令行提示符下执行命令 **help** [*command*]获取帮助。

----结束

6.3.9 检查配置结果

路由器作为 FTP 服务器配置成功后，可以查看到 FTP 服务器的配置和状态信息、登录的 FTP 用户信息等内容。

前提条件

已完成路由器作为 FTP 服务器的所有配置

操作步骤

- 使用 **display 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。

----结束

任务示例

执行命令 **display ftp-server**，可以看到 FTP 服务器正在运行。

```
<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     1.1.1.1
```

执行命令 **display ftp-users**，可以看到当前配置的 FTP 用户的用户名、端口号、授权目录等信息。

```
<Huawei> display ftp-users
  username  host                                      port  idle  topdir
  zll       100.2.150.226                             1383  3     flash:
```

6.4 通过 SFTP 进行文件操作

SFTP 使得用户可以从远端安全登录路由器进行文件管理，这样使远程系统升级等需要文件的传送的地方，增加了数据传输的安全性。

6.4.1 建立配置任务

在通过 SFTP 进行文件操作的配置前了解此特性的应用环境、配置此特性的前置任务和数据准备，有助于快速、准确地完成配置任务。

应用环境

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。SSH 协议支持 SFTP。

SFTP 是一种安全的 FTP 服务，用户可以从终端安全地登录到 FTP 服务器，进行文件的安全传输。

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：

- 终端与路由器之间有可达路由

数据准备

在通过 SFTP 进行文件操作之前，需准备以下数据。

序号	数据
1	VTY 类型用户界面的最大个数、（可选）对 VTY 类型用户界面呼入呼出进行限制的 ACL 号、终端用户超时断开时间、终端屏幕的显示行数和历史命令缓冲区大小、用户验证方式、用户名、口令
2	SSH 用户的用户名和密码、认证方式、服务方式、为 SSH 用户分配的对端 RSA 公钥名、SSH 用户的 SFTP 工作目录

序号	数据
3	（可选）SSH 服务器监听端口号，（可选）SSH 服务器密钥对更新时间
4	SSH 服务器名称、SSH 服务器当前监听的端口号、SFTP 客户端到 SSH 服务器端的首选加密算法、SSH 服务器端到 SFTP 客户端的首选加密算法、SFTP 客户端到 SSH 服务器端的首选 HMAC 算法、SSH 服务器端到 SFTP 客户端的首选 HMAC 算法、首选密钥交换算法、出接口名称、源地址
5	目录名称、文件名称

6.4.2 配置 VTY 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。

背景信息

在通过 SFTP 方式访问设备前，必须要配置 VTY 用户界面的用户验证方式，否则用户将无法登录设备。

VTY 用户界面的其他属性在设备上都有缺省值，用户一般不需要另外配置。但是可以根据用户使用需求，配置相关属性。具体配置请参见**配置 VTY 用户界面**。

6.4.3 配置 VTY 用户界面支持 SSH 协议

当用户通过 SFTP 方式访问路由器时，需要配置 VTY 用户界面支持 SSH 协议。

背景信息

缺省情况下，用户界面支持的协议是 Telnet。如果不配置某个或某几个用户界面支持 SSH 协议，则用户不能通过 SFTP 方式访问路由器。

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 **user-interface vty** *first-ui-number* [*last-ui-number*]，进入 VTY 用户界面视图。

步骤 3 执行命令 **authentication-mode aaa**，设置验证方式为 AAA 验证。

步骤 4 执行命令 **protocol inbound ssh**，配置 VTY 支持 SSH 协议。

----结束

6.4.4 配置 SSH 用户并指定服务方式包含 SFTP

通过 SFTP 方式访问路由器时，必须要配置 SSH 用户、产生本地 RSA 密钥对、设置用户验证方式以及指定 SSH 用户的服务方式和服务授权目录。

背景信息

- SSH 支持 RSA、password、password-rsa 和 all 四种认证方式。需要在 AAA 视图下创建同名的本地用户。
- 产生本地 RSA 密钥对是成功完成 SSH 登录的首要操作。如果 SSH 用户使用 password 验证，则需要在 SSH 服务器端生成本地 RSA 密钥。如果 SSH 用户使用 RSA 验证，则在服务器端和客户端都需要生成本地 RSA 密钥。

说明

password-rsa 认证需要同时满足 password 认证和 RSA 认证，all 认证是指 password 认证和 RSA 认证方式满足其中一种即可。

请在作为 SSH 服务器的路由器上进行如下的配置。

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 **aaa**，进入 AAA 视图。

步骤 3 执行命令 **local-user** *user-name* **password** *password*，配置本地用户名和密码。

步骤 4 执行命令 **local-user** *user-name* **privilege level** *level*，配置本地用户级别。

说明

必须将用户级别配置在 3 级及 3 级以上。

步骤 5 执行命令 **quit**，返回系统视图。

步骤 6 执行命令 **rsa local-key-pair create**，产生本地 RSA 密钥对。

说明

- 在进行其它 SSH 配置之前，必须完成 **rsa local-key-pair create** 配置，生成本地密钥对。
- 密钥对生成后，可以执行 **display rsa local-key-pair public** 命令查看本地密钥对中的公钥部分信息。

步骤 7 配置 SSH 用户的认证方式。

根据实际配置需要，选择如下操作之一：

- 配置对 SSH 用户进行 Password 验证
  - 执行命令 **ssh user** *user-name* **authentication-type password**，对 SSH 用户配置 Password 验证。

  采用本地认证或 HWTACACS 服务器认证时，如果 SSH 用户数量较多，使用缺省密码验证方式可以简化配置。
- 配置对 SSH 用户进行 RSA 验证

1. 执行命令 **ssh user** *user-name* **authentication-type rsa**，对 SSH 用户配置 RSA 验证。
2. 执行命令 **rsa peer-public-key** *key-name*，进入公共密钥视图。
3. 执行命令 **public-key-code begin**，进入公共密钥编辑视图。
4. 输入 *hex-data*，编辑公共密钥。

说明

- 进入公共密钥编辑视图后，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 的客户端软件随机生成。具体操作参见相应的 SSH 客户端软件的帮助文档。
- 进入公共密钥编辑视图后，即可将客户端上产生的 RSA 公钥传送到服务器端。请采用拷贝粘贴方式将 RSA 公钥配置到作为 SSH 服务器的路由器上。

5. 执行命令 **public-key-code end**，退出公共密钥编辑视图。
   - 如果未输入合法的密钥编码 *hex-data*，执行 **peer-public-key end** 后，将无法生成密钥。
   - 如果步骤 b 中指定的密钥 *key-name* 已经在别的窗口下被删除，再执行 **peer-public-key end** 时，系统会提示：密钥已经不存在，此时直接退到系统视图。
6. 执行命令 **peer-public-key end**，退出公共密钥视图，回到系统视图。
7. 执行命令 **ssh user** *user-name* **assign rsa-key** *key-name*，为 SSH 用户分配公钥。

- 配置对 SSH 用户进行 Password-Rsa 验证
  - 执行命令 **ssh user** *user-name* **authentication-type password-rsa**，对 SSH 用户配置 Password-Rsa 验证。

  此认证方式 SSH 服务器要求客户端进行身份认证的过程中同时进行 Publickey 身份认证和 Password 身份认证，只有当两者同时满足的情况下，才认为客户端身份认证通过。
- 配置对 SSH 用户进行 All 验证
  - 执行命令 **ssh user** *user-name* **authentication-type all**，对 SSH 用户配置 All 验证。

  此认证方式 SSH 服务器可以要求客户端进行身份认证的过程中进行公钥认证或密码认证，只要满足其中一个认证，就认为客户端身份认证通过。

步骤 8 （可选）配置 SSH 用户基本验证信息

1. 执行命令 **ssh server rekey-interval** *interval*，设置服务器密钥的更新时间。

   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。
2. 执行命令 **ssh server auth-timeout** *timeout_interval*，设置 SSH 认证超时时间。

   缺省情况下，SSH 连接认证超时时间为 60 秒。
3. 执行命令 **ssh server authentication-retries** *auth-times*，设置 SSH 验证重试次数。

   缺省情况下，SSH 连接的验证重试次数为 3。

----结束

6.4.5 使能 SFTP 服务器功能

在通过 SFTP 方式访问路由器之前，需要首先使能路由器的 SFTP 服务器功能。

背景信息

缺省情况下，路由器的 SFTP 服务器功能没有使能，只有使能了此功能后，客户端才能以 SFTP 方式与路由器建立连接。

请在作为 SSH 服务器的路由器上进行如下的配置。

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 **sftp server enable**，使能 SFTP 服务器功能。

缺省情况下，SFTP 服务为关闭状态。

----结束

6.4.6 （可选）配置 SFTP 服务器参数

用户可以配置是否使能兼容低版本 SSH 协议，配置或变更 SSH 服务器监听端口号以及配置服务器密钥对更新时间、指定源接口。

背景信息

服务器参数如表 6-1 所示。

表 6-1 服务器参数

服务器参数	说明
兼容低版本 SSH 协议	SSH 协议有 SSH1.X（SSH2.0 之前的版本）和 SSH2.0 版本。SSH2.0 协议相比 SSH1.X 协议来说，在结构上做了扩展，可以支持更多的认证方法和密钥交换方法，同时提高了服务能力（如 SFTP）。AR3200 支持大于等于 1.3 且小于等于 2.0 之间的 SSH 协议版本。
监听端口号	缺省情况下，SSH 服务器端监听端口号是 22，此时登录路由器可以不指定端口号。但如果使用标准的监听端口号，可能会有攻击者不断访问此端口，导致带宽和服务器性能的下降，造成其他正常用户无法访问。所以可以重新配置 SSH 服务器的监听端口号，攻击者不知道 SSH 监听端口号的更改，有效防止了攻击者对 SSH 服务标准端口的访问，确保了安全性。
服务器密钥对更新时间	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。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 配置 SSH 服务器参数，根据需要，可执行如表 6-2 中的一个或多个操作。

表 6-2 配置服务器参数

服务器参数	操作
使能兼容低版本功能	执行命令 **ssh server compatible-ssh1x enable** 缺省情况下，SSH2.0 协议的服务器是兼容 SSH1.X 服务器功能的。如果不允许 SSH1.3 ～ SSH1.99（SSH 的协议版本号大于等于 1.3 且小于等于 1.99）的客户端登录，则执行 **undo ssh server compatible-ssh1x enable**，去使能兼容低版本功能。
配置 SSH 服务器监听端口号	执行命令 **ssh server port** *port-number* 如果配置了新的监听端口号，SSH 服务器端先断开当前已经建立的所有 STelnet 和 SFTP 连接，然后使用新的端口号开始监听。缺省情况下，SSH 服务器端监听端口号是 22。
配置服务器密钥对更新时间	执行命令 **ssh server rekey-interval** *rekey-interval* 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。

----结束

6.4.7 用户通过 SFTP 协议访问系统

完成以上配置后，用户可以使用 SFTP 方式从终端安全地访问路由器，从而实现对路由器上文件的管理。

背景信息

从终端通过 SFTP 访问路由器，可以选择使用第三方软件。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。

在用户终端上安装 OpenSSH 软件后，请在用户终端上进行以下配置。

说明

OpenSSH 软件的安装请参考该软件的安装说明。

使用 OpenSSH 软件从终端通过 SFTP 登录到系统时，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。

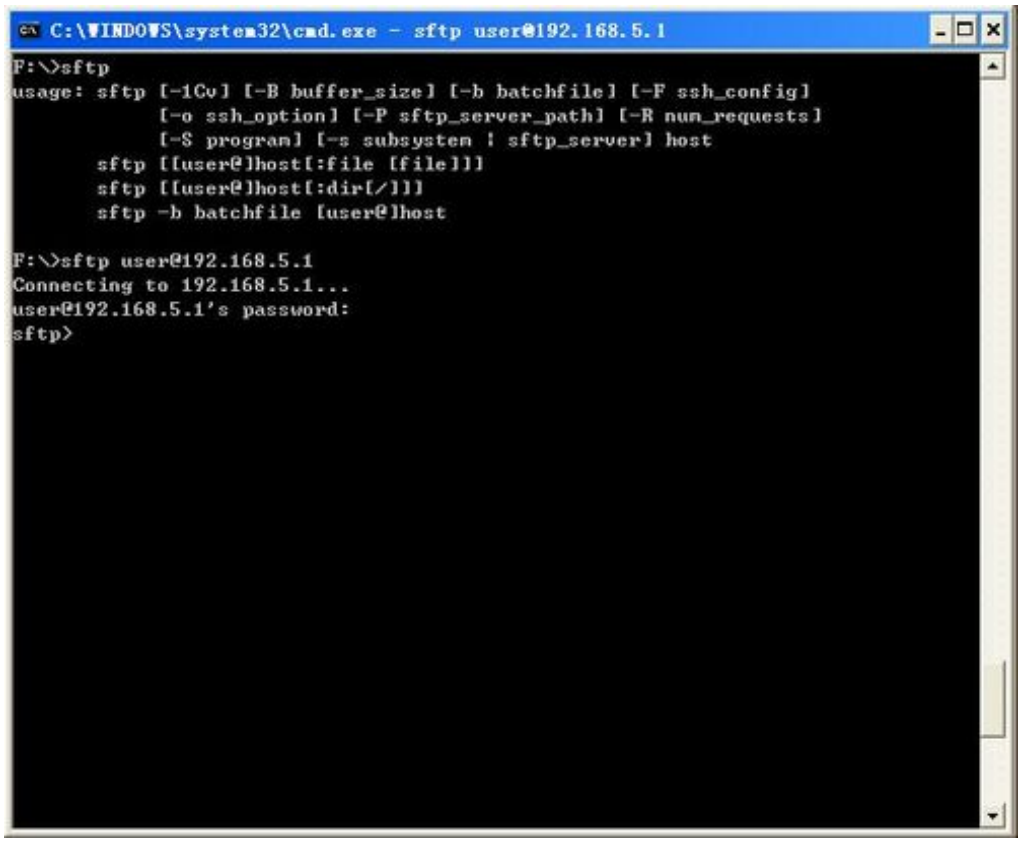
操作步骤

步骤 1 进入 Windows 的命令行提示符。

步骤 2 执行 OpenSSH 命令，通过 SFTP 方式访问路由器。

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。

图 6-2 SFTP 登录示意图



----结束

6.4.8 用户使用 SFTP 命令进行文件操作

当用户成功登录作为 SFTP 服务器的路由器后，可以在路由器上管理目录和文件。

背景信息

用户登录 SFTP 服务器后可以进行如下主要操作：

- 获取 SFTP 客户端命令帮助
- 管理 SFTP 服务器的目录
- 管理 SFTP 服务器的文件

当用户登录 SFTP 服务器进入 SFTP 客户端视图后，即可在用户终端进行以下一种或多种操作。这里以客户端使用第三方软件 OpenSSH 为例。

操作步骤

- 执行命令 **help** [**all** | *command-name*]，显示 SFTP 客户端命令帮助。
- 可根据需要，执行如下一个或多个操作管理目录：
  - 执行命令 **cd** [*remote-directory*]，改变用户的当前工作目录。
  - 执行命令 **pwd**，显示用户的当前工作目录。

- 执行命令 **dir** [**-l -a**] [*path*]，显示指定目录下的文件列表。
- 执行命令 **rmdir** *remote-directory* &<1-10>，删除服务器上目录。
- 执行命令 **mkdir** *remote-directory*，在服务器上创建新目录。

- 可根据需要，执行如下一个或多个操作管理文件：
  - 执行命令 **rename** *old-name new-name*，改变服务器上指定的文件的名字。
  - 执行命令 **get** *remote-filename* [*local-filename*]，下载远程服务器上的文件。
  - 执行命令 **put** *local-filename* [*remote-filename*]，上传本地文件到远程服务器。
  - 执行命令 **rmdir** *remote-directory* &<1-10>，删除服务器上文件。

----结束

6.4.9 检查配置结果

通过 SFTP 进行文件操作配置成功后，可以查看到 SSH 用户信息和 SSH 服务器的全局配置信息等内容。

前提条件

已完成 SSH 用户的所有配置。

操作步骤

- 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。

----结束

任务示例

运行命令 **display ssh user-information** *username*，可以看到名为 **client001** 的 SSH 用户的验证方式为 **password**，服务方式为 **sftp**。

```
<Huawei> display ssh user-information client001
      Sftp-directory          : -
      Service-type            : sftp
 ------------------------------------------------------------------------------
 Username         Auth-type          User-public-key-name
 ------------------------------------------------------------------------------
 client001        password           null
 ------------------------------------------------------------------------------
```

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。

运行命令 **display ssh server status**，可以查看 SSH 服务器全局配置信息。

```
<Huawei> display ssh server status
 SSH version                        : 1.99
 SSH connection timeout             : 60 seconds
 SSH server key generating interval : 2 hours
 SSH Authentication retries         : 5 times
 SFTP Server                        : Enable
 Stelnet server                     : Enable
```

说明

如果当前监听端口号是缺省值，不显示当前监听端口号信息。

运行命令 **display ssh server session**，可以查看 SSH 服务器与客户端连接的会话信息。

```
<Huawei> display ssh server session
  ------------------------------------------------------------------
  Conn    Ver   Encry     State  Auth-type        Username
  ------------------------------------------------------------------
  VTY 0   1.5   BLOWFISH  run    password         john

  ------------------------------------------------------------------
```

6.5 配置举例

配置用户通过登录系统、FTP、SFTP、FTPS 进行文件操作的示例。请结合配置流程图了解配置过程。配置示例中包括组网需求、配置注意事项和配置思路等。

6.5.1 通过登录系统进行文件操作举例

通过登录系统进行文件操作的示例。在本示例中，通过登录路由器，进行查看目录、拷贝等操作。

组网需求

用户通过 Console 口、Telnet 或 STelnet 方式登录路由器，对路由器上的文件进行操作。文件在存储器中的路径一定要正确，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。

配置思路

采用如下的思路配置:

1. 查看某目录下有哪些文件。
2. 拷贝文件到该目录下。
3. 查看该目录，可看到文件已经成功拷贝到指定目录。

数据准备

为完成此配置例，需准备如下的数据:

- 源文件名和目标文件名
- 源文件路径和目标文件路径

操作步骤

步骤 1 显示当前目录下的文件信息，其中 flash:/为闪存标识符。

```
<Huawei> dir
Directory of flash:/
  Idx  Attr     Size(Byte)  Date        Time(LMT)  FileName
    0  -rw-         1,241  Jun 16 2011 09:15:58   rootcert.pem
    1  -rw-         2,688  Apr 27 2011 17:06:50   pat1.pat
    2  -rw-           396  Mar 21 2011 08:25:25   rsa_host_key.efs
    3  -rw-           540  Mar 21 2011 08:25:43   rsa_server_key.efs
```

```
  4  -rw-            705  Apr 13 2011 11:23:45   iascfg.zip
  5  -rw-         88,942  Jul 01 2011 15:18:22   creat_vlanif.bat
  6  -rw-         80,783  Jul 01 2011 16:28:32   undovlanif.bat
  7  -rw-         56,523  Jun 15 2011 10:43:50   mon_file.txt

2,128 KB total (1,760 KB free)
```

步骤 2 拷贝文件从 usb0:/sample.txt 到 flash:/sample1.txt。

```
<Huawei> copy usb0:/sample.txt flash:/sample1.txt
Copy usb0:/sample.txt to flash:/sample1.txt?[Y/N]:y
100%  complete
Info:Copied file usb0:/sample.txt to flash:/sample1.txt...Done
```

步骤 3 显示当前目录下的文件信息，可以看到文件已经被拷贝至指定目录下。

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

  Idx  Attr     Size(Byte)  Date        Time(LMT)  FileName
    0  -rw-          1,241  Jun 16 2011 09:15:58   rootcert.pem
    1  -rw-          2,688  Apr 27 2011 17:06:50   pat1.pat
    2  -rw-            396  Mar 21 2011 08:25:25   rsa_host_key.efs
    3  -rw-            540  Mar 21 2011 08:25:43   rsa_server_key.efs
    4  -rw-            705  Apr 13 2011 11:23:45   iascfg.zip
    5  -rw-         88,942  Jul 01 2011 15:18:22   creat_vlanif.bat
    6  -rw-         80,783  Jul 01 2011 16:28:32   undovlanif.bat
    7  -rw-         56,523  Jun 15 2011 10:43:50   mon_file.txt
    8  -rw-          1,605  Jun 15 2011 10:43:50   sample1.txt

2,128 KB total (1,758 KB free)
```

----结束

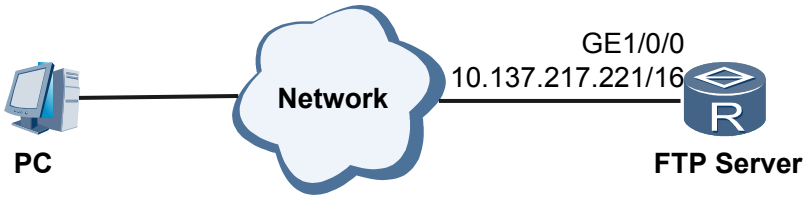
6.5.2 通过 FTP 进行文件操作举例

配置通过 FTP 进行文件操作的示例。在本示例中，通过使用正确的用户名和密码从用户终端以 FTP 方式登录到 FTP 服务器，实现文件的上传和下载。

组网需求

如图 6-3 所示，作为 FTP 服务器的路由器使能 FTP 服务器功能后，从超级终端登录到 FTP 服务器，实现文件的上传和下载。

图 6-3 配置 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 进行文件操作基本功能：

1. 配置 FTP 服务器的 IP 地址。

2. 使能 FTP 服务器功能。
3. 配置 FTP 用户的验证信息、用户授权方式及访问目录。
4. 使用正确的用户名和密码以 FTP 方式登录到 FTP 服务器。
5. 上传文件至服务器、下载文件到用户终端。

数据准备

为完成此配置例，需准备如下的数据：

- FTP 服务器的 IP 地址为 10.137.217.221。
- FTP 服务器超时断连时间为 20 分钟。
- 在服务器端设置 FTP 用户名为“huawei”，密码为“huawei”。
- 上传的文件在用户终端的指定路径下，需下载的文件在 FTP 服务器指定的路径。
- 确保 PC 与 FTP 服务器之间通信正常。

操作步骤

步骤 1 配置 FTP 服务器的 IP 地址

```
<Huawei> system-view
[Huawei] sysname server
[server] interface gigabitethernet1/0/0
[server-GigabitEthernet1/0/0] ip address 10.137.217.221 255.255.0.0
[server-GigabitEthernet1/0/0] quit
```

步骤 2 使能 FTP 服务器功能

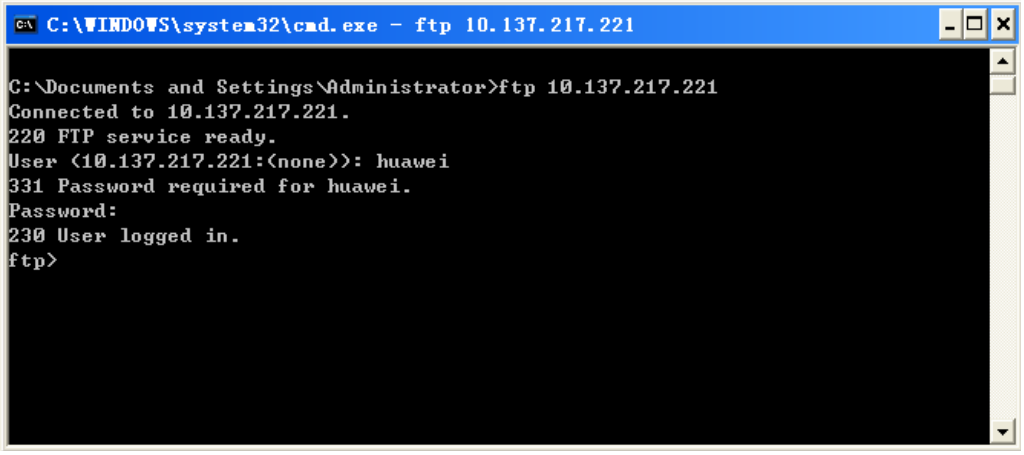
```
[server] ftp server enable
[server] ftp timeout 20
```

步骤 3 在 FTP 服务器上配置 FTP 用户的验证信息、授权方式和授权目录

```
[server] aaa
[server-aaa] local-user huawei password huawei
[server-aaa] local-user huawei service-type ftp
[server-aaa] local-user huawei privilege level 15
[server-aaa] local-user huawei ftp-directory flash:
[server-aaa] quit
```

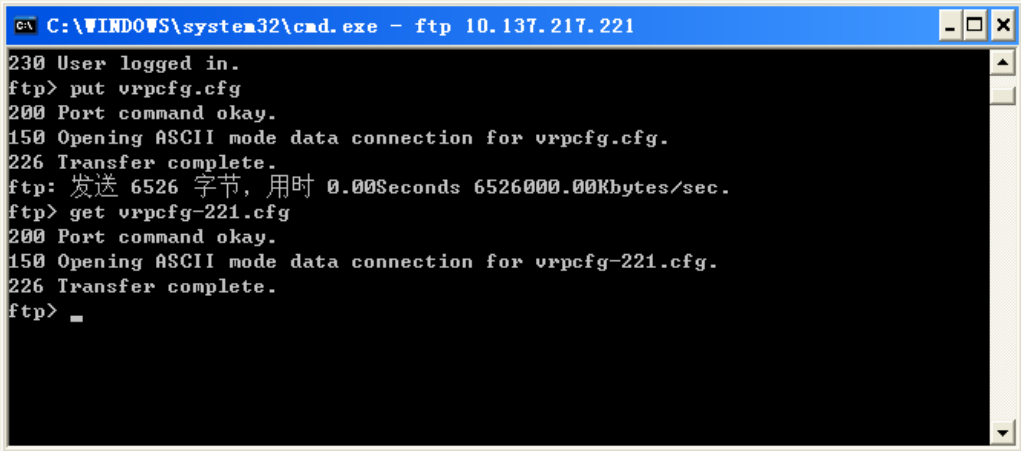
步骤 4 进入 windows 命令行提示符输入,执行 ftp 命令，然后使用正确的用户名和密码与 FTP 服务器建立 FTP 连接。

图 6-4 从用户终端登录 FTP 服务器



步骤 5 在用户终端实现文件的上传和下载，如下图所示。

图 6-5 通过 FTP 进行文件操作



说明

用户在进行文件下载前或文件上传后可以使用 **dir** 命令，查看需要下载的文件或是所上传的文件的详细信息。

----结束

配置文件

- FTP 服务器的配置文件

```
#
sysname Server
#
 ftp server enable
 ftp timeout 20
#
interface GigabitEthernet1/0/0
 ip address 10.137.217.221 255.255.0.0
#
aaa
 local-user huawei password N`C55QK<`=/Q=^Q`MAF4<1!!
 local-user huawei service-type ftp
 local-user huawei ftp-directory flash:
 authentication-scheme default
#
authorization-scheme default
#
accounting-scheme default
#
domain default
#
return
```

6.5.3 通过 SFTP 进行文件操作举例

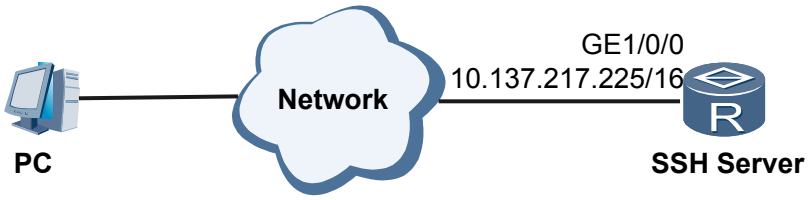
配置用户通过 SFTP 进行文件操作的示例。在本示例中，通过在 SSH 服务器端生成本地密钥对，并在 SSH 服务器端配置 SSH 用户的用户名和密码，使能 SFTP 服务，实现 SFTP 客户端连接 SSH 服务器后进行文件操作。

组网需求

如图 6-6 所示，在作为 SSH 服务器的路由器上使能 SFTP 服务器功能后，SFTP 客户端 PC 可以通过 Password、RSA、password-rsa 或 all 认证的方式连接到 SSH 服务器端。

配置用户通过 password 认证方式登录 SSH Server。

图 6-6 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，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，包括用户名和密码。
4. 在 SSH 服务器端使能 SFTP 服务器功能以及配置用户的服务类型。

数据准备

为完成此配置举例，需准备如下的数据：

- SSH 用户的认证方式为 password，用户名为“client001”，密码为“huawei”。
- client001 的用户级别为 3。
- SSH 服务器端的 IP 地址为 10.137.217.225。

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] rsa local-key-pair create
The key name will be: Host
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
       It will take a few minutes.
Input the bits in the modulus[default = 512]: 768
Generating keys...
.......++++++++++++
..........++++++++++++
.....................................++++++++
......++++++++
```

步骤 2 在服务器端配置 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
```

步骤 3 在服务器端配置 SSH 用户的用户名和密码

```
[SSH Server] aaa
[SSH Server-aaa] local-user client001 password huawei
[SSH Server-aaa] local-user client001 privilege level 3
[SSH Server-aaa] local-user client001 service-type ssh
[SSH Server-aaa] local-user client001 ftp-directory flash:
[SSH Server-aaa] quit
```

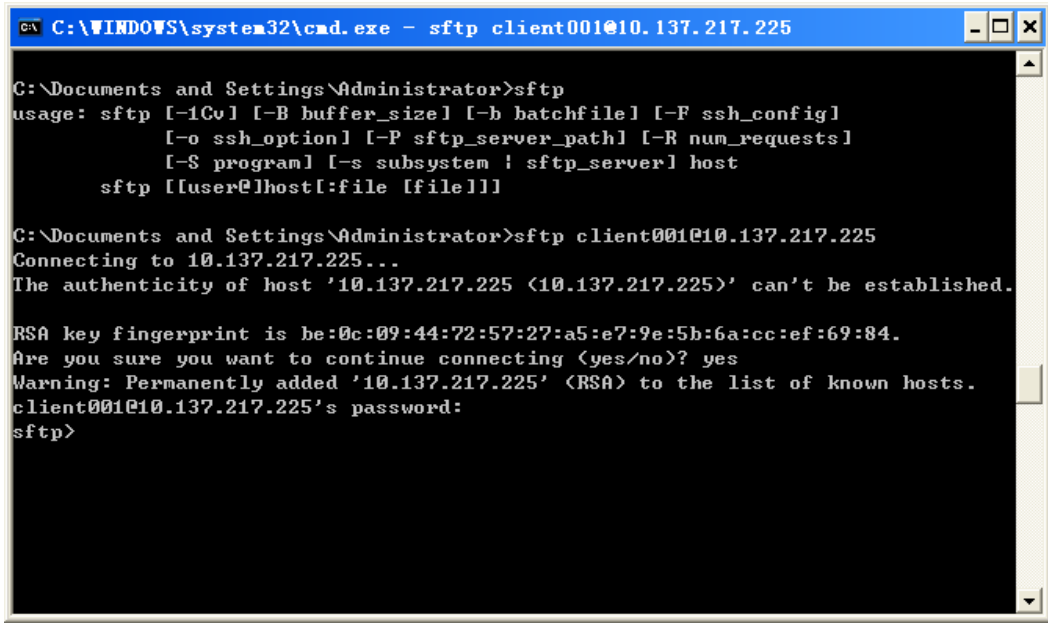
步骤 4 使能 SFTP 功能

```
[SSH Server] sftp server enable
```

步骤 5 验证配置结果

#通过 OpenSSH 软件实现访问 SFTP 服务器

图 6-7 访问界面



----结束

配置文件

- SSH 服务器的配置文件

```
#
 sysname SSH Server
#
aaa
 local-user client001 password  N`C55QK<`=/Q=^Q`MAF4<1!!
 local-user client001 privilege level 3
 local-user client001 service-type ssh
 local-user client001 ftp-directory flash:
#
interface GigabitEthernet1/0/0
 ip address 10.137.217.225 255.255.0.0
#
 sftp server enable
```

```
#
user-interface vty 0 4
 authentication-mode aaa
 protocol inbound ssh
#
return
```

7 配置系统启动

关于本章

路由器启动时将会启动系统软件和加载配置文件。有效地管理系统软件和配置文件可以保证路由器正常启动。

7.1 系统启动简介
路由器启动时需要加载系统软件和配置文件。

7.2 管理配置文件
用户可以对路由器的当前配置以及系统下次启动的配置文件进行管理。

7.3 设置系统启动文件
设置系统启动文件包括设置指定的系统软件和配置文件，可以保证路由器下一次启动时以指定的系统软件启动以及以指定的配置文件初始化配置。

7.4 配置举例
配置用户启动系统的示例。配置示例中包括组网需求、配置注意事项和配置思路等。

7.1 系统启动简介

路由器启动时需要加载系统软件和配置文件。

7.1.1 系统软件

系统软件是路由器的操作系统，是路由器能够正常运行以及提供各种业务服务的基础。

系统软件文件名必须以.cc 作为扩展名，而且必须存放在存储设备的根目录下。

7.1.2 配置文件和当前配置

路由器运行过程中，有配置文件和当前配置，这是两个不同的概念。

配置文件和当前配置的概念如下表：

概念		查看方式
配置文件	路由器上电时，从默认存储路径中读取配置文件进行路由器的初始化工作，因此该配置文件中的配置称为起始配置，如果默认存储路径中没有配置文件，则路由器用缺省参数初始化。	● 使用 **display startup** 命令可以查看到路由器本次以及下次启动的配置文件。 ● 使用 **display saved-configuration** 命令可以查看路由器下次启动时的配置文件信息。
当前配置	与起始配置相对应，路由器运行过程中正在生效的配置称为当前配置。	使用 **display current-configuration** 命令查看路由器的当前配置信息。

用户通过命令行接口可以修改路由器当前配置，为了使当前配置能够作为路由器下次上电时的起始配置，需要用 **save** 命令保存当前配置到默认存储设备中，形成配置文件。

7.2 管理配置文件

用户可以对路由器的当前配置以及系统下次启动的配置文件进行管理。

7.2.1 建立配置任务

在进行管理配置文件的配置前了解此特性的应用环境、配置此特性的前置任务和数据准备，有助于快速、准确地完成配置任务。

应用环境

管理配置文件包括保存、清除以及比较配置文件。当路由器需要升级、巡检或者配置文件遭到破坏、需要查看路由器启动后的配置项等情况时，需要进行管理配置文件的操作。

前置任务

在对配置文件进行管理之前，需要完成以下任务：

- 路由器安装完毕并上电正常启动

数据准备

管理配置文件之前，需准备以下数据。

序号	数据
1	配置文件及其文件名
2	自动保存配置文件的时间间隔及延迟时间间隔
3	配置文件比较的开始行数

7.2.2 保存配置文件

用户可以定时保存配置文件，也可以立即保存当前配置文件。

背景信息

为了降低由于路由器掉电或者意外重启导致配置信息的丢失，系统提供定时保存配置的功能，同时也提供实时保存配置的功能。

操作步骤

- 定时保存配置。

  警告

  自动保存时，如果接口板不在位，相关的配置可能会丢失。

  1. 执行命令 **autosave interval** { *time* } | { *value* } | { **configuration** *time* }，配置系统定时保存配置。

     指定 **interval** *time* 参数，无论配置是否发生了变化，当设置的定时保存配置时间间隔到达时，系统都会定时保存配置。

     - 缺省情况下，系统自动保存配置的时间间隔是 0，即不启动定时自动保存配置功能。
     - 使能自动保存功能后，如果不指定 *time*，缺省值是 30 分钟。

- 实时保存配置。
  - 执行命令 **save** [**all**] [*configuration-file*]，保存当前配置。

    配置文件必须以“.cfg” 或“.zip”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。

用户通过命令行接口可以修改路由器的当前配置，为了使当前配置能够作为路由器下次上电时的初始配置，需要用 **save** 命令保存当前配置到存储器中，形成配置文件。

执行命令 **save all**，将会保存当前所有的配置，包括不在位的板卡的配置，至系统默认的存储路径中。

----结束

7.2.3 清除配置文件的内容

用户可以清除当前设备上加载的配置文件的内容。

背景信息

在以下两种情况下，需要擦除配置文件：

- 在路由器软件升级之后，软件和配置文件不匹配。
- 发现配置文件遭到破坏，或加载了错误的配置文件。

操作步骤

- 在用户视图下，执行命令 **reset saved-configuration**，清除当前加载的配置文件的内容。
  - 如果路由器当前启动与下次启动的配置文件一致，执行该命令将同时清除这两个配置文件。路由器下次启动采用缺省配置文件。
  - 如果路由器当前启动与下次启动的配置文件不一致，执行该命令将清除当前启动的配置文件。
  - 如果路由器当前启动的配置文件为空，执行该命令后，系统将提示配置文件不存在。

  配置文件被清除后，如果不使用 **startup saved-configuration** *configuration-file* 命令重新指定含有正确配置信息的配置文件，或者不使用 **save** 命令保存配置文件，则路由器下次启动时，将采用缺省的配置参数进行初始化。

----结束

7.2.4 比较配置文件

用户可以比较当前配置和初始配置。

背景信息

在路由器上进行如下配置。

操作步骤

步骤 1 执行命令 **compare configuration** [*configuration-file* [*current-line-number save-line-number*]]，比较当前的配置与下次启动的配置文件内容是否一致。

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。

系统在比较出不同之处时，将从不同的行开始，分别对当前配置文件和保存的配置文件，显示一定数量字符的文件内容（默认显示 120 个字符），如果该不同之处到文件末尾不足 120 个字符，将显示到文件尾为止。

比较当前配置和下次配置文件时，如果下次配置文件为空，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。

----结束

7.2.5 检查配置结果

管理配置文件配置成功后，可以查看到当前配置文件、路由器下次启动时加载的配置文件的内容、设备启动时使用的文件信息和存储设备中的文件信息等内容。

前提条件

已完成管理配置文件的所有配置。

操作步骤

- 使用 **display current-configuration** [**configuration** [*configuration-type* [*configuration-instance*]] | **controller** | **interface** [*interface-type* [*interface-number*]]] [**feature** *feature-name* [**filter** *filter-expression*] | **filter** *filter-expression*]或者 **display current-configuration** [**all** | **inactive**]命令查看当前配置信息。
- 使用 **display startup** 命令查看设备启动时使用的文件信息。
- 使用 **dir** [/**all**] [*filename*] [*device-name*]命令查看存储设备中的文件信息。
- 使用 **display saved-configuration** [**last** | **time** | **configuration**]命令查看路由器下次启动时加载的配置文件的内容。
- 使用 **display autosave configuration** 命令查看自动保存功能的配置信息。包括自动保存功能的状态和自动保存的检测时长。
- 使用 **display this** 命令查看当前视图的运行配置。

----结束

任务示例

执行命令 **display startup**，可以查看设备启动时使用的文件信息。

```
<Huawei> display startup
MainBoard:
  Startup system software:                  usb0:/ar0210_30735_1220.cc
  Next startup system software:             usb0:/ar0210_30735_1220.cc
  Backup system software for next startup:  null
  Startup saved-configuration file:         flash:/arcfg.cfg
  Next startup saved-configuration file:    flash:/arcfg.cfg
  Startup license file:                     null
  Next startup license file:                null
  Startup patch package:                    null
  Next startup patch package:               null
  Startup voice-files:                      null
  Next startup voice-files:                 null
```

7.3 设置系统启动文件

设置系统启动文件包括设置指定的系统软件和配置文件，可以保证路由器下一次启动时以指定的系统软件启动以及以指定的配置文件初始化配置。

7.3.1 建立配置任务

在进行设置系统启动文件的配置前了解此特性的应用环境、配置此特性的前置任务和数据准备，有助于快速、准确地完成配置任务。

应用环境

为了让路由器在下次启动时继续提供用户配置的业务，用户需要正确选择路由器在下次启动时加载的 AR3200 系统软件和配置文件。

前置任务

在对系统启动文件进行设置之前，需要完成以下任务：

- 路由器安装完毕并上电启动正常

数据准备

设置系统启动文件之前，需准备以下数据。

序号	数据
1	AR3200 系统软件及其文件名
2	配置文件及其文件名

7.3.2 配置路由器下次启动时加载的系统软件

用户在升级路由器系统软件等情况时，需要指定路由器下次启动时加载的系统软件。

背景信息

如果不配置路由器下次启动时加载的系统软件，则路由器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。

系统软件文件名必须以“.cc”作为扩展名，而且必须存放在存储设备的根目录下。

操作步骤

步骤 1 在用户视图下执行命令 **startup system-software** *filename* [**verify**]，配置路由器下次启动时加载的 AR3200 系统软件。

----结束

7.3.3 配置路由器下次启动时加载的配置文件

用户在重启设备之前，可以指定路由器下次启动时加载的配置文件。

背景信息

可以使用 **display startup** 命令查看路由器是否配置了下次启动时加载的配置文件。如果没有配置，则下次启动采用缺省配置文件。

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设备的根目录下。

路由器上电时，默认从 Flash 存储器中读取配置文件进行初始化，因此该配置文件中的配置称为初始配置。如果 Flash 中尚没有配置文件，则路由器用缺省参数初始化。

操作步骤

- 执行 **startup saved-configuration** *configuration-file* 命令，配置路由器下次启动时加载的配置文件。

----结束

7.3.4 检查配置结果

设置系统启动文件配置成功后，可以查看路由器下次启动时加载的配置文件的内容和设备启动时使用的文件信息。

前提条件

已完成设置系统启动文件的相关配置。

操作步骤

- 使用 **display current-configuration** [**configuration** [*configuration-type* [*configuration-instance*]] | **controller** | **interface** [*interface-type* [*interface-number*]]] [**feature** *feature-name* [**filter** *filter-expression*] | **filter** *filter-expression*]命令查看当前配置信息。
- 使用 **display saved-configuration** [**last** | **time**]命令查看路由器下次启动时加载的配置文件的内容。
- 使用 **display startup** 命令查看设备启动时使用的文件信息。

----结束

任务示例

执行命令 **display startup**，可以查看设备启动时使用的文件信息。

```
<Huawei> display startup
MainBoard:
  Startup system software:                  usb0:/ar0210_30735_1220.cc
  Next startup system software:             usb0:/ar0210_30735_1220.cc
  Backup system software for next startup:  null
  Startup saved-configuration file:         flash:/arcfg.zip
  Next startup saved-configuration file:    flash:/arcfg.zip
  Startup license file:                     null
  Next startup license file:                null
  Startup patch package:                    null
  Next startup patch package:               null
  Startup voice-files:                      null
  Next startup voice-files:                 null
```

7.4 配置举例

配置用户启动系统的示例。配置示例中包括组网需求、配置注意事项和配置思路等。

7.4.1 配置系统启动示例

配置系统启动的示例。在本示例中，通过保存配置文件、指定路由器下次启动时加载的系统软件和配置文件，实现系统的正确启动。

组网需求

要求对路由器进行配置后，在系统下次启动时新配置生效。

配置思路

采用如下的思路配置系统启动：

1. 保存当前配置。
2. 配置路由器下次启动时加载的配置文件。
3. 配置路由器下次启动时加载的系统软件。

数据准备

为完成此配置例，需准备如下的数据：

- 配置文件的文件名。
- 系统软件的文件名。

操作步骤

步骤 1 查看系统本次启动的配置文件和系统软件

```
<Huawei> display startup
MainBoard:
  Startup system software:                   usb0:/ar0312.cc
  Next startup system software:              usb0:/ar0312.cc
  Backup system software for next startup:   null
  Startup saved-configuration file:          flash:/iascfg.zip
  Next startup saved-configuration file:     flash:/iascfg.zip
  Startup license file:                      null
  Next startup license file:                 null
  Startup patch package:                     null
  Next startup patch package:                null
  Startup voice-files:                       null
  Next startup voice-files:                  null
```

步骤 2 保存当前配置到指定文件

```
<Huawei> save arcfg.cfg
```

系统将提示是否在主控板中保存当前配置到 arcfg.cfg 文件。输入 **y**，则保存成功。

步骤 3 配置路由器下次启动时加载的配置文件

```
<Huawei> startup saved-configuration usb0:/arcfg.cfg
```

步骤 4 配置路由器下次启动时加载的系统软件

在主控板上配置下次启动时加载的系统软件。

```
<Huawei> startup system-software usb0:/arsoft.cc
```

说明

系统软件 arsoft.cc 已上传至 AR3200 设备，具体上传过程请参考**通过 FTP 进行文件操作**内容。

步骤 5 验证配置结果

配置完成之后，执行如下命令，查看路由器下次启动时加载的配置文件和路由器下次启动时加载的系统软件。

```
<Huawei> display startup
MainBoard:
  Startup system software:                  usb0:/ar0312.cc
  Next startup system software:             usb0:/arsoft.cc
  Backup system software for next startup:  null
  Startup saved-configuration file:         flash:/iascfg.zip
  Next startup saved-configuration file:    usb0:/arcfg.cfg
  Startup license file:                     null
  Next startup license file:                null
  Startup patch package:                    null
  Next startup patch package:               null
  Startup voice-files:                      null
  Next startup voice-files:                 null
```

----结束

配置文件

无

8 访问其他设备

关于本章

当用户需要对网络中其他设备进行管理配置或者进行文件操作时，可以在当前设备通过Telnet、STelnet、TFTP、FTP 或 SFTP 访问网络上的这些设备。

8.1 访问其他设备简介
分别介绍了采用 Telnet、FTP、TFTP 和 SSH 方式访问其他设备。

8.2 通过 Telnet 登录其他设备
网络中有大量路由器需要管理与维护，用户不可能为每个路由器连接用户终端，特别是终端与需要管理的路由器之间无可达路由时，用户可以使用 Telnet 方式从当前路由器登录到网络上另一台路由器，从而实现对远程路由器的管理与维护。

8.3 通过重定向连接其他设备
当用户需要管理远程设备，但远程设备只能通过串口传输数据时，可以通过路由器的重定向服务来实现。

8.4 通过 STelnet 登录其他设备
STelnet 是一种安全的 Telnet 服务。用户可以通过 STelnet 方式从当前路由器登录到另一台路由器，对其进行远程管理。

8.5 通过 TFTP 访问其他设备的文件
配置当前路由器作为 TFTP 客户端，通过 TFTP 协议的客户端功能登录 TFTP 服务器，进行文件的上传和下载。

8.6 通过 FTP 访问其他设备的文件
配置路由器作为 FTP 客户端，登录网络上的 FTP 服务器，实现文件的上传和下载等操作。

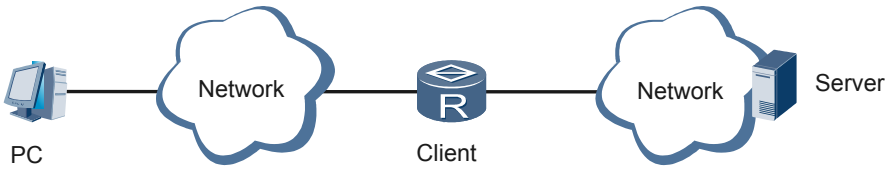
8.7 通过 SFTP 访问其他设备的文件
SFTP 是一种安全的 FTP 服务。配置路由器作为 SFTP 客户端，服务器通过对客户端的认证及双向的数据加密，为网络文件传输提供了安全的服务。

8.8 配置举例
配置设备访问其他设备的示例。请结合配置流程图了解配置过程。配置示例中包括组网需求、配置注意事项和配置思路等。

8.1 访问其他设备简介

分别介绍了采用 Telnet、FTP、TFTP 和 SSH 方式访问其他设备。

图 8-1 当前路由器访问其他设备示意图



如图 8-1 所示，用户在 PC 上通过终端仿真程序或 Telnet 程序建立与路由器的连接后，仍可以将当前路由器作为客户端，通过下面一种或几种方式访问网络上的其他设备。

8.1.1 Telnet 方式

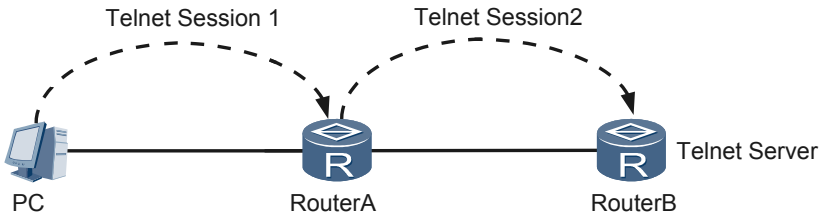
当用户需要对网络上的设备进行配置和管理时，可以在当前路由器使用 Telnet Client 和重定向终端服务。

Telnet 协议在 TCP/IP 协议族中属于应用层协议，通过网络提供远程登录和虚拟终端功能。

AR3200 提供的 Telnet 服务包括：

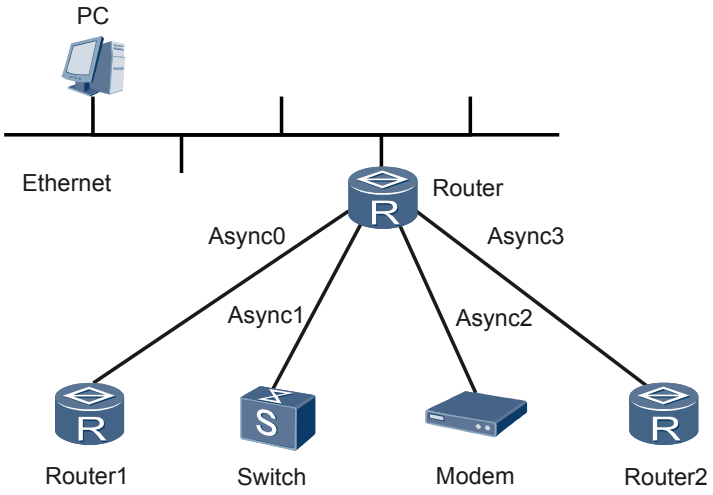
- Telnet server：用户在 PC 上运行 Telnet 客户端程序登录到路由器，对路由器进行配置管理。此时，路由器提供 Telnet server 服务。
- Telnet client：用户在 PC 上通过终端仿真程序或 Telnet 客户端程序建立与路由器的连接后，再执行 **telnet** 命令登录到其它设备，对其进行配置管理。如图 8-2 所示，RouterA 此时既作为 Telnet server，也同时提供 Telnet client 服务。

  图 8-2 提供 Telnet client 服务

- 重定向终端服务：用户在 PC 上运行 Telnet 客户端程序以特定的端口号登录到路由器，再与路由器异步口连接的串口设备建立连接，如图 8-3 所示。典型的应用是路由器的异步口以直连方式外接多个设备，实现对这些设备的远程配置和维护。

图 8-3 提供 Telnet 重定向服务



说明

只有提供异步口的设备才支持 Telnet 重定向服务。

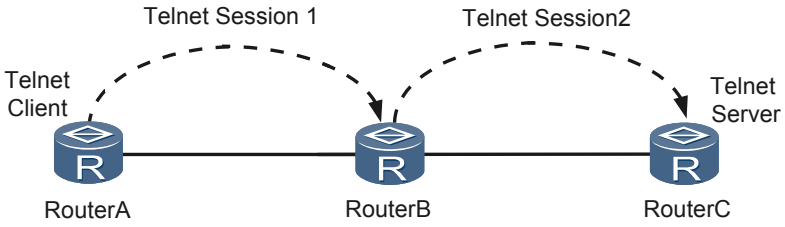
- 中断 Telnet 服务

  在 Telnet 连接过程中，可以使用两种快捷键来中断连接。

  如图 8-4 所示，RouterA 通过 Telnet 登录到 RouterB，再 Telnet 连接到 RouterC，形成级联结构。

  RouterA 是 RouterB 的 Telnet 客户端，RouterB 是 RouterC 的 Telnet 客户端，以此结构说明两种快捷键的用法。

图 8-4 Telnet 快捷键使用示意图



<Ctrl_]>快捷键——通知服务器端断开连接

在网络畅通的情况下，键入<Ctrl_]>将通知 Telnet 服务器中断本次 Telnet 登录，即，Telnet 服务器端主动断开连接。

如下例所示：

```
<RouterC>
```

此时键入<Ctrl_]>，将退回到 RouterB 的提示符。

```
Configuration console exit, please retry to log on
The connection was closed by the remote host
<RouterB>
```

此时键入<Ctrl_]>，将退回到 RouterA 的提示符。

```
Configuration console exit, please retry to log on
```

```
The connection was closed by the remote host
<RouterA>
```

说明

如果由于某些原因网络连接断开，快捷键的指令无法到达 Telnet 服务器端，输入无效。

<Ctrl_T>快捷键——客户端主动断开连接

当服务器端故障且客户端无法感知时，客户端输入任何指令服务器均无响应，这种情况下键入<Ctrl_T>快捷键，则 Telnet 客户端主动中断并退出 Telnet 连接。

如下例所示：

```
<RouterC>
```

此时键入<Ctrl_T>，将直接中断并退出 Telnet 连接。

```
<RouterA>
```

注意

当远端用户登录数达到 VTY 类型用户界面的最大个数时，系统会提示所有的用户接口都在使用，不允许 Telnet。

8.1.2 FTP 方式

当用户需要访问远程主机上的文件时，可以在当前路由器通过 FTP 方式建立与远程 FTP 服务器的连接。

FTP 实现主机间文件的传输，并提供常用的文件操作命令，供用户进行文件系统的简单管理。客户可以利用设备外部的 FTP 客户端程序与路由器进行文件的上传、下载和目录访问等操作；还可以使用设备内部的 FTP 客户端程序与其他设备的 FTP 服务器端的程序进行文件传输。

FTP 向用户提供本地和远程主机之间的文件传输，尤其在进行版本升级、日志下载、文件传输和配置保存等业务操作中广泛应用。

8.1.3 TFTP 方式

当客户端和服务器之间不需要复杂的交互环境时，用户可以在当前路由器通过 TFTP 方式访问 TFTP 服务器上的文件。

TFTP（Trivial File Transfer Protocol）是一种简单文件传输协议。

与 FTP 相比，TFTP 不具有复杂的交互存取接口和认证控制，适用于客户机和服务器之间不需要复杂交互的环境。例如，系统启动时使用 TFTP 获取系统内存映像。

TFTP 协议在 UDP 基础上实现。

TFTP 协议传输由客户端发起。当需要下载文件时，由客户端向 TFTP 服务器发送读请求包，然后从服务器接收数据包，并向服务器发送确认；当需要上传文件时，由客户端向 TFTP 服务器发送写请求包，然后向服务器发送数据包，并接收服务器的确认。

TFTP 传输文件有两种模式：

- 二进制模式：用于传输程序文件
- ASCII 码模式：用于传输文本文件

目前，AR3200 只能作为 TFTP 客户端，且只能使用二进制模式传输文件。

8.1.4 SSH 方式

当用户需要安全地访问网络上其他设备时，可以通过 SSH 方式（包括 STelnet、SFTP）从当前路由器访问其他设备。

SSH 简介

用户通过不安全的网络环境远程登录到设备时，安全外壳 SSH（Secure Shell）特性可以提供安全的信息保障和强大的认证功能，以保护设备不受诸如 IP 地址欺诈、明文密码截取等攻击。

SSH 客户端功能允许用户与支持 SSH Server 的路由器、UNIX 主机等建立 SSH 连接。

SSH 客户端功能

AR3200 提供 SFTP、STelnet 客户端功能。

- STelnet 客户端功能

  STelnet 是 Secure Telnet 的简称。

  Telnet 缺少安全的认证方式，而且传输过程采用 TCP 进行明文传输，存在很大的安全隐患。单纯提供 Telnet 服务容易招致 DoS（Denial of Service）、主机 IP 地址欺骗、路由欺骗等恶意攻击。

  相对于 Telnet，SSH 通过以下措施实现在不安全网络上提供安全的远程访问：

  - 支持 RSA（Remote Subscriber Access）验证方式，根据非对称加密体系的加密原则，通过生成公钥和私钥，实现密钥的安全交换，最终实现安全的会话全过程。
  - 支持数据加密标准 DES（Data Encryption Standard）、3DES、AES。
  - SSH 客户端与服务器端通讯时，用户名及口令均进行加密，有效防止对口令的窃听。
  - 对传输的数据加密。

  当 STelnet 服务器端或是与客户端的连接存在故障时，客户端需要及时了解故障的存在，并主动断开连接。为了实现上述目标，客户端以 STelnet 方式登录服务器时，配置无数据接收时发送 keepalive 报文的间隔时间和服务器端的无应答限制次数。如果在指定时间间隔内未收到数据，客户端将发送 keepalive 报文至服务器端。如果服务端的无应答次数超过配置的次数，客户端将主动断开连接。

- SFTP 客户端功能

  SFTP 是 Secure FTP 的简称，使得用户可以从远端安全的登录到设备上进行文件管理，这样使远程系统升级等需要文件传送的地方，增加了数据传输的安全性。同时，由于提供了客户端功能，可以在本设备上安全 FTP 到远程设备，进行文件的安全传输。

  当 SFTP 服务器端或是与客户端的连接存在故障时，客户端需要及时了解故障的存在，并主动断开连接。为了实现上述目标，客户端以 SFTP 方式登录服务器时，配置无数据接收时发送 keepalive 报文的间隔时间和服务器端的无应答限制次数。如果在指定时间间隔内未收到数据，客户端将发送 keepalive 报文至服务器端。如果服务端的无应答次数超过配置的次数，客户端将主动断开连接。

8.2 通过 Telnet 登录其他设备

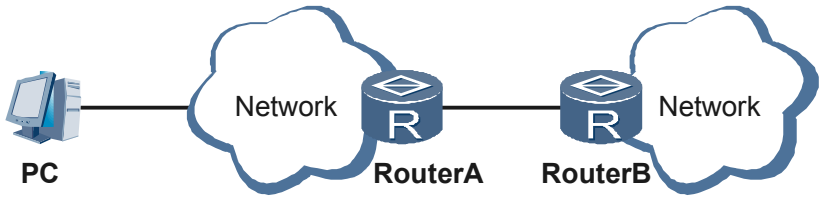
网络中有大量路由器需要管理与维护，用户不可能为每个路由器连接用户终端，特别是终端与需要管理的路由器之间无可达路由时，用户可以使用 Telnet 方式从当前路由器登录到网络上另一台路由器，从而实现对远程路由器的管理与维护。

8.2.1 建立配置任务

在进行通过 Telnet 方式从当前设备登录到其他设备配置前，了解此特性的应用环境、配置此特性的前置任务和数据准备，有助于快速、准确地完成配置任务。

应用环境

图 8-5 当前设备访问其他设备示意图



如图 8-5 所示，用户可以在 PC 上通过 Telnet 登录到 RouterA，但是由于 PC 与 RouterB 之间无可达路由，用户无法远程管理 RouterB，则此时可以在 RouterA 上通过 Telnet 方式登录到 RouterB，实现对 RouterB 的远程管理。

此时，当前路由器 RouterA 为 Telnet 客户端，待登录管理的路由器 RouterB 为服务器。

前置任务

在通过 Telnet 登录其他设备之前，需要完成以下任务：

- **配置用户通过 Telnet 登录系统**
- Telnet 客户端与 Telnet 服务器之间有可达路由。

数据准备

在通过 Telnet 登录其他设备之前，需要准备以下数据：

序号	数据
1	远程 RouterB 的 IP 地址或主机名
2	远程 RouterB 提供 Telnet 服务的 TCP 端口号

8.2.2 （可选）配置 Telnet 客户端源地址

用户可以配置 Telnet 客户端的源地址信息，从指定的客户端源地址和路由建立 Telnet 连接，保证安全性。

背景信息

用户可以在路由器上指定某一接口，为此接口配置 IP 地址，然后使用该 IP 地址作为 Telnet 连接的源 IP 地址，从而达到进行安全校验的目的。

客户端源地址可以配置为源接口或源 IP。

请在作为 Telnet 客户端的路由器上进行如下的配置。

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 **telnet client-source** { **-a** *source-ip-address* | **-i** *interface-type interface-number* }，配置 Telnet 客户端的源地址信息。

配置了 Telnet 客户端源地址信息后，在服务器端显示的 Telnet 客户端的源地址信息与该步骤中配置的一致。

----结束

8.2.3 使用 Telnet 命令登录其他设备

使用 Telnet 命令，用户可以从当前路由器登录到另一台路由器，并对其进行配置管理。

背景信息

Telnet 提供了一种通过终端远程登录到服务器的方式，呈现一个交互式操作界面。用户可以先登录到一台主机，再通过 Telnet 的方式远程登录到网络上的其他主机上，对设备进行配置和管理。而不需要为每一台主机都连接一个硬件终端。

请在作为 Telnet 客户端的路由器设备上进行如下的配置。

操作步骤

- 根据网络协议基于 IPv4 还是 IPv6，选择执行如下两个步骤之一：
  - 执行命令 **telnet** [**vpn-instance** *vpn-instance-name*] [**-a** *source-ip-address*] *host-name* [*port-number*]，登录并管理其他设备。
  - 执行命令 **telnet ipv6** *host-name* [*port-number*]，登录并管理其他设备。

----结束

8.2.4 检查配置结果

用户通过 Telnet 方式从当前路由器成功登录另一台路由器后，可以查看到当前建立的 TCP 连接情况等信息。

前提条件

已完成通过 Telnet 登录其他设备的所有配置。

操作步骤

- 使用 **display tcp status** 命令查看当前建立的所有 TCP 连接情况。

----结束

任务示例

执行命令 **display tcp status**，可以查看 TCP 连接状态。**Established** 表示一个 TCP 连接已经建立。

```
<Huawei> display tcp status
TCPCB      Tid/Soid    Local Add:port        Foreign Add:port       VPNID      State
39952df8   36 /1509     0.0.0.0:0             0.0.0.0:0              0          Closed
32af9074   59 /1        0.0.0.0:21            0.0.0.0:0              14849      Listening
34042c80   73 /17       10.164.39.99:23       10.164.6.13:1147       0          Established
```

8.3 通过重定向连接其他设备

当用户需要管理远程设备，但远程设备只能通过串口传输数据时，可以通过路由器的重定向服务来实现。

8.3.1 建立配置任务

在进行重定向连接其他设备配置前，了解此特性的应用环境、配置此特性的前置任务和数据准备，有助于快速、准确地完成配置任务。

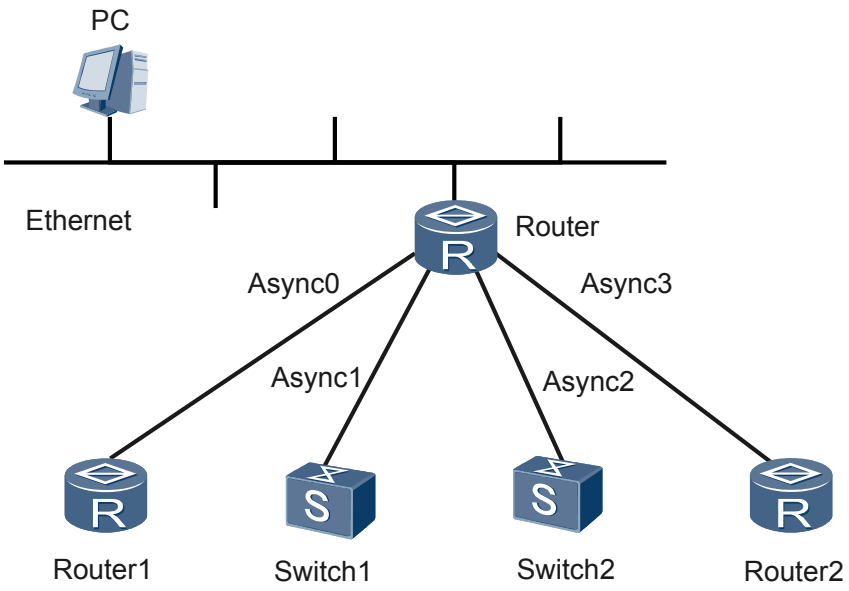
应用环境

当用户需要管理远程设备，且远程设备只能通过串口传输数据时，可以通过路由器的重定向服务来实现。

远程设备可以是路由器、交换机、电力或者金融系统终端等其他支持串口配置的设备。

- 远程设备是路由器，交换机等设备。

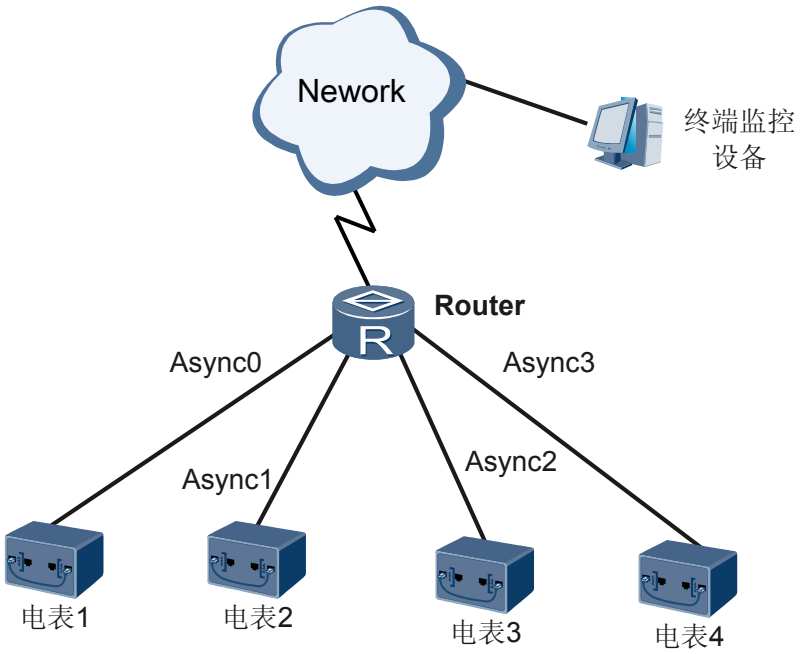
图 8-6 重定向连接到其他设备示意图（1）



如图 8-6 所示，Router 与路由器，交换机等设备直连。当用户需要远程管理终端设备时，且这些设备只能通过串口管理时，用户可以使用 Router 的重定向服务，将 Router 的异步口与终端设备的串口进行连接。实现对远程设备的管理和维护。

- 远程设备是智能电表，智能水表或者银行自助系统等终端设备。

图 8-7 重定向连接其他设备示意图（2）



如图 8-7 所示，启用重定向服务后，Router 监听相应的 TCP 端口，从串口接收由终端设备发送的数据流。接收到数据流后，Router 对数据进行封装，使之成为可以在以太网中传播的数据帧，从而实现终端设备的远程数据传输与管理。

前置任务

在通过重定向登录其他设备之前，需要完成以下任务：

- 远程设备上电且正常启动
- 路由器上“8AS”单板注册成功，且与远程设备之间通过异步线缆直连，路由器上异步串口状态“Up”。

数据准备

在通过重定向连接其他设备之前，需要准备以下数据。

序号	数据
1	路由器的 IP 地址
2	（可选）需要监听的端口号。

8.3.2 使能重定向功能

在路由器上使能重定向功能后，用户可以实现与远程串口设备的数据通讯。

前提条件

路由器上“8AS”单板已经成功注册且串口状态为“Up”。

背景信息

请在路由器上进行如下的配置。

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 **interface async** *interface-number*，进入异步串口视图。

步骤 3 执行命令 **async mode flow**，配置异步串口工作在流模式。

缺省情况下，异步串口工作在协议模式。

步骤 4 执行命令 **quit**，退出异步串口视图。

步骤 5 执行命令 **user-interface tty** *tty-number*，进入 TTY 用户界面视图。

“8AS”单板注册成功后，设备将随机生成 TTY 用户界面编号，执行 **display user-interface** 可以检查异步串口对应的 TTY 界面编号 *tty-number*。

步骤 6 执行命令 **redirect enable**，使能重定向功能。

步骤 7 执行命令 **undo shell**，禁止在用户界面上的终端服务。

步骤 8 （可选）执行命令 **redirect binding vpn-instance** *vpn-instance-name*，配置重定向功能与 VPN 实例绑定。

缺省情况下，重定向功能未与任何 VPN 实例绑定，无论公网还是私网用户均可以通过重定向功能连接远程设备。

步骤 9 （可选）执行命令 **redirect listen-port** *port-num*，配置重定向功能使能后设备监听的端口号。

缺省情况下，设备监听的端口号为 2000 加上 *tty-number*。当该端口号被其他应用程序占用时，可以执行本步骤重新配置监听端口号。

说明

- TTY 用户界面的终端属性需要与所连接的终端设备的物理属性一致，TTY 用户界面物理属性的配置请参见 **4.4.3 配置 TTY 用户界面的终端属性**。
- TTY 用户界面视图下如果配置了 Modem 的功能，串口重定向功能将不可用。

----结束

后续处理

重定向功能使能后，可以执行命令 **telnet** *host-name port-number* 登陆远程设备。*host-name* 是使能重定向功能的路由器的 IP 地址或主机名，*port-number* 为缺省的监听端口号或者用户通过 **redirect listen-port** 命令指定的端口号。

8.3.3 检查配置结果

重定向连接其他设备配置成功后，可以查看当前的 TCP 状态信息。

前提条件

已完成重定向连接其他设备的所有配置。

操作步骤

- 使用 **display tcp status** 命令查看当前建立的 TCP 连接情况。

----结束

任务示例

运行命令 **display tcp status**，可以查看 TCP 连接状态信息。

```
<Huawei> display tcp status
TCPCB    Tid/Soid Local Add:port       Foreign Add:port      VPNID  State
1973f250 9   /2    0.0.0.0:22           0.0.0.0:0             23553  Listening
1973f0ec 9   /1    0.0.0.0:23           0.0.0.0:0             23553  Listening
1973ef88 109/1    0.0.0.0:80           0.0.0.0:0             23553  Listening
1a16a204 9   /14   0.0.0.0:2046       0.0.0.0:0           23553  Listening
1973e9f8 7   /1    0.0.0.0:7547         0.0.0.0:0             0      Listening
1a169c74 9   /15   10.137.217.211:23    10.138.77.61:2120     0      Established
```

8.4 通过 STelnet 登录其他设备

STelnet 是一种安全的 Telnet 服务。用户可以通过 STelnet 方式从当前路由器登录到另一台路由器，对其进行远程管理。

8.4.1 建立配置任务

在进行 Stelnet 登录其他设备功能的配置前了解此特性的应用环境、配置此特性的前置任务和数据准备，有助于快速、准确地完成配置任务。

应用环境

Telnet 缺少安全的认证方式，而且传输过程采用 TCP 进行明文传输，存在很大的安全隐患。

STelnet 是 SSH Telnet 的简称，是一种安全的 Telnet 服务。STelnet 建立在 SSH 连接的基础之上，SSH 用户可以像使用 Telnet 服务一样操作 STelnet 服务。

此时，当前设备为 SSH 客户端，待登录的设备为 SSH 服务器。

前置任务

在配置通过 STelnet 客户端登录其他设备之前，需完成以下任务：

- **配置用户通过 STelnet 登录系统**
- STelnet 客户端与 STelnet 服务器之间有可达路由。

数据准备

在配置通过 STelnet 客户端登录其他设备之前，需准备以下数据。

序号	数据
1	SSH 服务器名称、客户端为 SSH 服务器分配的公钥
2	SSH 服务器的 IPv4 地址或主机名、SSH 服务器当前监听的端口号、STelnet 客户端到 SSH 服务器端的首选加密算法、SSH 服务器端到 STelnet 客户端的首选加密算法、STelnet 客户端到 SSH 服务器端的首选 HMAC 算法、SSH 服务器端到 STelnet 客户端的首选 HMAC 算法、首选密钥交换算法 服务器端配置的用户登录信息

8.4.2 配置用户首次成功登录其他设备（使能 SSH 客户端首次认证功能方式）

使能 SSH 客户端首次认证功能后，当 STelnet 客户端第一次登录 SSH 服务器时，不对 SSH 服务器的 RSA 公钥进行有效性检查。

背景信息

如果配置了使能 SSH 客户端首次认证功能，那么在 STelnet 客户端第一次登录 SSH 服务器时，不对 SSH 服务器的 RSA 公钥进行有效性检查。登录后，系统将自动分配并保存 RSA 公钥，为下次登录时认证。

请在作为 SSH 客户端的路由器上进行如下的配置。

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 **ssh client first-time enable**，使能 SSH 客户端首次认证功能。

缺省情况下，SSH 客户端首次认证功能为关闭状态。

说明

- 使能 SSH 客户端首次认证功能的目的，是当 STelnet 客户端第一次登录 SSH 服务器时，不对 SSH 服务器的 RSA 公钥进行有效性检查，因为此时 STelnet 客户端还没有保存 SSH 服务器的 RSA 公钥。
- 如果没有使能 SSH 客户端首次认证功能，当 STelnet 客户端第一次登录 SSH 服务器时，由于对 SSH 服务器的 RSA 公钥有效性检查失败，会导致登录服务器失败。

窍门

如果 STelnet 客户端需要第一次就成功登录 SSH 服务器，除了使能 SSH 客户端首次认证功能之外，还可以通过事先在客户端为 SSH 服务器分配 RSA 公钥来实现。

----结束

8.4.3 配置用户首次成功登录其他设备（SSH 客户端为 SSH 服务器分配公钥方式）

如果没有使能 SSH 客户端首次认证功能，那么需要在 STelnet 客户端登录 SSH 服务器之前为服务器分配 RSA 公钥。

背景信息

如果没有使能 SSH 客户端首次认证功能，当 STelnet 客户端第一次登录 SSH 服务器时，由于对 SSH 服务器的 RSA 公钥有效性检查失败，从而会导致登录服务器失败。所以需要在 STelnet 客户端登录 SSH 服务器之前为服务器分配 RSA 公钥。

请在作为 SSH 客户端的路由器上进行如下的配置。

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 **rsa peer-public-key** *key-name* ，进入 RSA 公共密钥视图。

步骤 3 执行命令 **public-key-code begin**，进入公共密钥编辑视图。

步骤 4 输入 *hex-data*，编辑公共密钥。

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。

说明

- 在为 SSH 服务器分配 RSA 公钥之前，所分配的 RSA 公钥必须来自 SSH 服务器端，这样 STelnet 客户端对 SSH 服务器的 RSA 公钥有效性检查才会通过。
- 进入公共密钥编辑视图后，即可将服务器上产生的 RSA 公钥传送到客户端。请采用拷贝粘贴方式将 RSA 公钥配置到作为 SSH 客户端的路由器上。

步骤 5 执行命令 **public-key-code end**，退出公共密钥编辑视图。

- 如果未输入合法的密钥编码 *hex-data*，执行 **peer-public-key end** 后，将无法生成密钥。
- 如果步骤 2 中指定的 *key-name* 已经在别的窗口下被删除，再执行 **peer-public-key end** 时，系统会提示：密钥已经不存在，此时直接退到系统视图。

步骤 6 执行命令 **peer-public-key end**，退出公共密钥视图，回到系统视图。

步骤 7 执行命令 **ssh client** *servername* **assign rsa-key** *keyname*，为 SSH 服务器分配 RSA 公钥。

说明

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**，解除 SSH 客户端与 SSH 服务器的绑定关系，再执行命令 **ssh client** *servername* **assign rsa-key** *keyname*，为 SSH 服务器分配新的 RSA 公钥。

----结束

8.4.4 使用 STelnet 命令登录其他设备

用户从 SSH 客户端以 STelnet 方式登录到 SSH 服务器上，即从当前路由器登录到另一台路由器，并对其进行配置管理。

背景信息

STelnet 客户端访问 SSH 服务器时可以携带源地址、VPN 实例名，选择密钥交换算法、加密算法和 HMAC 算法以及设置 keepalive 功能。

请在作为 SSH 客户端的路由器上进行如下的配置。

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 **stelnet** [**-a** *source-address*] *host-ipv4* [*port*] [[**-vpn-instance** *vpn-instance-name*] |[**prefer_kex** { **dh_group1** | **dh_exchange_group** }] | [**prefer_ctos_cipher** { **des** | **3des** | **aes128** }] | [**prefer_stoc_cipher** { **des** | **3des** | **aes128** }] | [**prefer_ctos_hmac** { **sha1** | **sha1_96** | **md5** | **md5_96** }] | [**prefer_stoc_hmac** { **sha1** | **sha1_96** | **md5** | **md5_96** }]] * [**-ki** *aliveinterval* [**-kc** *alivecountmax*]]，以 STelnet 方式登录到 SSH 服务器上。

----结束

8.4.5 检查配置结果

通过 STelnet 登录其他设备功能配置成功后，可以查看到 SSH 服务器的全局配置信息以及 SSH 服务器与客户端连接的会话信息。

前提条件

已完成通过 STelnet 登录其他设备功能的所有配置。

操作步骤

- 使用 **display ssh server status** 命令查看 SSH 服务器的状态信息。

----结束

任务示例

在 SSH 客户端执行命令 **display ssh server status**，查看 SSH 服务器的状态置信息。

```
<Huawei> 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
```

8.5 通过 TFTP 访问其他设备的文件

配置当前路由器作为 TFTP 客户端，通过 TFTP 协议的客户端功能登录 TFTP 服务器，进行文件的上传和下载。

8.5.1 建立配置任务

在进行 TFTP 访问其他设备的文件配置前了解此特性的应用环境、配置此特性的前置任务和数据准备，有助于快速、准确地完成配置任务。

应用环境

当用户需要在服务器端与客户端之间传送文件且不需要复杂的交互环境时，可以使用不具有复杂的交互接口和认证控制的 TFTP 协议。

此时，当前路由器为客户端，待访问的设备为 TFTP 服务器。

前置任务

在配置通过 TFTP 访问其他设备的文件之前，需要完成以下任务：

- 当前路由器和 TFTP 服务器路由可达

数据准备

在配置通过 TFTP 访问其他设备的文件之前，需要准备以下数据：

序号	数据
1	（可选）路由器作为 TFTP 客户端时的源地址（或者源接口）
2	TFTP 服务器 IP 地址或主机名
3	TFTP 服务器中特定文件的文件名、文件所在的目录

8.5.2 （可选）配置 TFTP 客户端源地址

用户可以配置 TFTP 客户端的源地址信息，从指定的客户端源地址建立 TFTP 连接，保证安全性。

背景信息

用户可以在路由器上指定某一接口，为此接口配置 IP 地址，然后使用该 IP 地址作为 TFTP 连接的源 IP 地址，从而达到进行安全校验的目的。

客户端源地址可以配置为源接口或源 IP。

请在作为 TFTP 客户端的路由器上进行如下的配置。

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 **tftp client-source** { **-a** *source-ip-address* | **-i** *interface-type interface-number* }，配置 TFTP 客户端的源地址信息。

配置了 TFTP 客户端源地址信息后，在服务器端显示的 TFTP 客户端的源地址信息与该步骤中配置的一致。

----结束

8.5.3 （可选）配置 TFTP 访问限制

通过 ACL 规则配置客户端登录 TFTP 服务器的访问限制，实现允许当前路由器以 TFTP 方式可以访问哪些 TFTP 服务器。

背景信息

ACL（Access Control List）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接口 ACL 规则、基本 ACL 规则和高级 ACL 规则。

说明

TFTP 只支持基本访问控制列表（编号范围为 2000 ~ 2999）。

请在作为 TFTP 客户端的路由器进行如下的配置。

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 **acl** *acl-number*，进入 ACL 视图。

步骤 3 执行命令 **rule** [*rule-id*] { **deny** | **permit** } [{ **fragment** | **none-first-fragment** } | **source** { *source-address source-wildcard* | **any** } | **time-range** *time-name* | **vpn-instance** *vpn-instance-name*] *，配置 ACL 规则。

说明

创建的 ACL 规则默认对所有报文进行 deny 操作。如果需要让报文正常通过，还需要在 ACL 规则中配置 permit 操作。例如，配置丢弃源 IP 为 10.1.1.10 的报文，那么 ACL 中应当定义两条规则：

- **rule deny source 10.1.1.10 0**
- **rule permit source any**

如果没有定义 **rule permit source any**，其他源 IP 地址不是 10.1.1.10 的报文也会被丢弃。

步骤 4 执行命令 **quit**，退回到系统视图。

步骤 5 执行命令 **tftp-server acl** *acl-number*，使用访问控制列表限制本设备端对 TFTP 服务器的访问。

----结束

8.5.4 使用 TFTP 命令下载其他设备的文件

用户可以使用 TFTP 命令在当前路由器下载服务器上的文件。

请在作为 TFTP 客户端的路由器进行如下的配置。

操作步骤

- 根据服务器端 IP 地址类型不同，进行如下操作。
  - 服务器端是 IPv4 地址，执行命令 **tftp** [**-a** *source-ip-address* | **-i** *interface-type interface-number*] *tftp-server* [**public-net** | **vpn-instance** *vpn-instance-name*] **get** *source-filename* [*destination-filename*]，使用 TFTP 方式下载文件。

- 服务器端是 IPv6 地址，执行命令 **tftp ipv6** [**-a** *source-ip-address*] *tftp-server-ipv6* [**-i** *interface-type interface-number*] **get** *source-filename* [*destination-filename*]，使用 TFTP 方式下载文件。

----结束

8.5.5 使用 TFTP 命令向其他设备上传文件

用户可以使用 TFTP 命令从当前路由器上传文件至服务器。

请在作为 TFTP 客户端的路由器进行如下的配置。

操作步骤

- 根据服务器端 IP 地址类型不同，进行如下操作。
  - 服务器端是 IPv4 地址，执行命令 **tftp** [**-a** *source-ip-address* | **-i** *interface-type interface-number*] *tftp-server* [**public-net** | **vpn-instance** *vpn-instance-name*] **put** *source-filename* [*destination-filename*]，使用 TFTP 方式上传文件。
  - 服务器端是 IPv6 地址，执行命令 **tftp ipv6** [**-a** *source-ip-address*] *tftp-server-ipv6* [**-i** *interface-type interface-number*] **put** *source-filename* [*destination-filename*]，使用 TFTP 方式上传文件。

----结束

8.5.6 检查配置结果

设备作为 TFTP 客户端配置成功后，可以查看客户端的源地址和配置的访问控制列表的规则。

前提条件

已完成设备作为 TFTP 客户端的所有配置。

操作步骤

- 使用 **display tftp-client** 命令查看设备作为 TFTP 客户端时的源地址。
- 使用 **display acl** { **name** *acl-name* | *acl-number* | **all** }查看 TFTP 客户端配置的访问控制列表的规则。

----结束

任务示例

执行命令 **display tftp-client**，可以查看客户端的源地址。

```
<Huawei> display tftp-client
Info: The source address of TFTP client is 1.1.1.1.
```

执行命令 **display acl**{ **name** *acl-name* | *acl-number* | **all** }，可以查看 TFTP 客户端配置的访问控制列表的规则。

```
<Huawei> display acl 2001
Basic acl  2001, 2 rules,
Acl's step is 5
 rule 5 deny source 10.1.1.10 0
 rule 10 permit
```

8.6 通过 FTP 访问其他设备的文件

配置路由器作为 FTP 客户端，登录网络上的 FTP 服务器，实现文件的上传和下载等操作。

8.6.1 建立配置任务

在进行 FTP 访问其他设备文件的配置前了解此特性的应用环境、配置此特性的前置任务和数据准备，有助于快速、准确地完成配置任务。

应用环境

当用户需要与远程 FTP 服务器进行文件传输、目录管理等操作时，可以配置当前路由器为 FTP 客户端，通过 FTP 方式访问远程 FTP 服务器。

前置任务

在配置通过 FTP 访问其他设备文件之前，需要完成以下任务：

- 路由器与服务器路由可达

数据准备

如果配置通过 FTP 访问其他设备文件，需要准备以下数据：

序号	数据
1	（可选）路由器作为 FTP 客户端时的源地址
2	FTP 服务器的主机名或 IP 地址、建立 FTP 连接使用的端口号、登录时需要的用户名及密码
3	FTP 协议命令、本地的文件名和远程 FTP 服务器上的文件名、远程 FTP 服务器上的工作路径名、FTP 客户端的本地工作路径或远程 FTP 服务器目录名

8.6.2 （可选）配置 FTP 客户端源地址

用户可以配置 FTP 客户端的源地址信息，从指定的客户端源地址建立 FTP 连接，保证安全性。

背景信息

用户可以在路由器上指定某一接口，为此接口配置 IP 地址，然后使用该 IP 地址作为 FTP 连接的源 IP 地址，从而达到进行安全校验的目的。

客户端源地址可以配置为源接口或源 IP。

请在作为 FTP 客户端的路由器上进行如下的配置。

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 **ftp client-source** { **-a** *source-ip-address* | **-i** *interface-type interface-number* }，配置 FTP 客户端的源地址信息。

配置了 FTP 客户端源地址信息后，在服务器端执行 **display ftp-users** 命令时，显示的 FTP 客户端的源地址信息与该步骤中配置的一致。

----结束

8.6.3 使用 FTP 命令连接其他设备

用户可以使用 FTP 命令从作为 FTP 客户端的路由器登录到其他设备。

背景信息

在用户视图和 FTP 客户端视图下，用户均可以使用相应命令登录 FTP 服务器。

请在作为客户端的路由器上进行如下的配置。

操作步骤

- 用户视图下，建立与 FTP 服务器的连接。
  - 服务器端是 IPv4 地址。

    执行命令 **ftp** [**-a** *source-ip-address* | **-i** *interface-type interface-number*] *host* [*port-number*] [**public-net** | **vpn-instance** *vpn-instace-name*]，与 FTP 服务器建立连接。
  - 服务器端是 IPv6 地址。

    执行命令 **ftp ipv6** *host* [*port-number*]，与 FTP 服务器建立连接。
- FTP 视图下，建立与 FTP 服务器的连接。
  - 服务器端是 IPv4 地址。
    1. 用户视图下执行命令 **ftp**，进入 FTP 视图。
    2. 执行命令 **open** [**-a** *source-ip-address* | **-i** *interface-type interface-number*] *host* [*port-number*] [**vpn-instance** *vpn-instance-name*]，与 FTP 服务器建立连接。
  - 服务器端是 IPv6 地址。
    1. 用户视图下执行命令 **ftp**，进入 FTP 视图。
    2. 执行命令 **open ipv6** *host-ipv6-address* [*port-number*]，与 FTP 服务器建立连接。

  说明

  在登录 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。

----结束

8.6.4 通过 FTP 文件操作命令进行文件操作

用户登录 FTP 服务器后，可以通过 FTP 文件操作命令进行文件操作。包括配置文件传输方式、查看 FTP 命令在线帮助、上传下载文件、管理目录、管理文件等。

背景信息

当 FTP 客户端登录到 FTP 服务器之后，用户可以在 FTP 客户端进行如下操作：

- 配置传输文件的数据类型和文件传输方式。
- 在 FTP 客户端视图下查看 FTP 命令的在线帮助。
- 将本地的文件上传到远程 FTP 服务器，也可以从 FTP 服务器下载文件并保存在本地。
- 在 FTP 服务器上进行创建、删除目录等管理操作。
- 可以显示 FTP 服务器上指定远程目录或文件的信息，或者删除 FTP 服务器上的指定文件。

登录作为客户端的路由器进入 FTP 客户端视图后进行如下的配置。

操作步骤

- 配置传输文件的数据类型和文件传输方式。
  - 执行命令 **ascii** 或 **binary**，配置传输的文件的数据类型为 ASCII 码或者二进制。

    说明

    FTP 支持 ASCII 码、二进制文件类型。二者的区别是:
    - ASCII 传输使用 ASCII 字符，把回车键和换行符分开。
    - 二进制不用转换或格式化就可传字符。

    FTP 传输模式由客户端进行选择，系统默认 ASCII 方式。客户端可使用模式切换命令进行切换（ASCII 和 Binary）。传输文本文件使用 ASCII 方式，传输二进制文件使用 Binary 方式。
  - 执行命令 **passive**，配置文件传输方式为被动方式。

    系统默认为被动方式。
  - 执行命令 **verbose**，打开 verbose 开关。

    打开 verbose 开关，将显示所有 FTP 响应，在文件传送完成后，将同时显示与传送效率有关的统计信息。
- 查看 FTP 命令的在线帮助。

  执行命令 **remotehelp** [*command*]，查看 FTP 命令的在线帮助。
- 上传或下载文件。
  - 上传或下载单个文件
    - 执行命令 **put** *local-filename* [*remote-filename*]，将本地的文件上传到远程 FTP 服务器。
    - 执行命令 **get** *remote-filename* [*local-filename*]，从 FTP 服务器下载文件并保存在本地。
- 进行如下一种或多种操作来管理目录。
  - 执行命令 **cd** *pathname*，改变远程 FTP 服务器上的工作路径。
  - 执行命令 **cdup**，改变 FTP 服务器端的工作路径到上一级目录。
  - 执行命令 **pwd**，显示 FTP 服务器端工作路径。
  - 执行命令 **lcd** [*local-directory*]，显示或者改变 FTP 客户端的工作路径。
  - 执行命令 **mkdir** *remote-directory*，在 FTP 服务器上创建目录。
  - 执行命令 **rmdir** *remote-directory*，在 FTP 服务器上删除目录。

说明

- 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。
- 如果执行命令 **mkdir /abc**，则是在根目录下创建一个名为“abc”的子目录。

- 进行如下一种或多种操作来管理文件。
  - 执行命令 **ls** [*remote-filename*] [*local-filename*]，显示 FTP 服务器上指定远程目录或文件的信息。

    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。

    使用参数 *local-filename*，可以将远程文件内容保存在本地另一个文件中。
  - 执行命令 **dir** [*remote-filename*] [*local-filename*]，显示 FTP 服务器上指定远程目录或文件的详细信息。

    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。

    使用参数 *local-filename*，可以将远程文件内容保存在本地另一个文件中。
  - 执行命令 **delete** *remote-filename*，删除 FTP 服务器上指定文件。

    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。

----结束

8.6.5 更改登录用户

用户登录 FTP 服务器后，可以更改当前的登录用户，用其他的用户名登录 FTP 服务器。

背景信息

AR3200 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。

请在作为客户端的路由器上进行如下的配置。

操作步骤

- 在 FTP 客户端视图下执行命令 **user** *user-name* [*password*]，更改当前的登录用户，重新进行登录。

  更改当前的登录用户后，原用户与 FTP 服务器的连接将断开。

----结束

8.6.6 断开与 FTP 服务器的连接

用户可以终止与 FTP 服务器的连接，并退回到用户视图或 FTP 视图。

背景信息

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。

请在作为客户端的路由器上进行如下的配置。

操作步骤

- 根据不同配置需要，选择执行如下操作。
  - 退回到用户视图。
    执行命令 **bye** 或 **quit**，终止与服务器的连接，并退回到用户视图。
  - 退回到 FTP 视图。
    执行命令 **close** 或 **disconnect**，终止与服务器的连接，并退回到 FTP 视图。

----结束

8.6.7 检查配置结果

通过 FTP 访问其他设备的文件配置成功后，可以查看到 FTP 客户端配置的源参数。

前提条件

已完成通过 FTP 访问其他设备的文件的所有配置。

操作步骤

- 使用 **display ftp-client** 命令查看设备作为 FTP 客户端时的源参数。

----结束

任务示例

执行命令 **display ftp-client**，可以查看 FTP 客户端的源参数。

```
<Huawei> display ftp-client
Info: The source address of FTP client is 1.1.1.1.
```

8.7 通过 SFTP 访问其他设备的文件

SFTP 是一种安全的 FTP 服务。配置路由器作为 SFTP 客户端，服务器通过对客户端的认证及双向的数据加密，为网络文件传输提供了安全的服务。

8.7.1 建立配置任务

在进行 SFTP 访问其他设备文件的配置前了解此特性的应用环境、配置此特性的前置任务和数据准备，有助于快速、准确地完成配置任务。

应用环境

SFTP 是 SSH FTP 的简称，一种安全的 FTP。SFTP 建立在 SSH 连接的基础之上，远程用户可以安全地登录设备，进行文件管理和文件传送等操作，为数据传输提供了更高的安全保障。同时，由于路由器提供了 SFTP 客户端功能，可以从本设备安全登录到远程 SSH 服务器上，进行文件的安全传输。

前置任务

在配置通过 SFTP 访问其他设备文件之前，需完成以下任务：

- 客户端与服务器之间路由可达

数据准备

在配置 SFTP 访问其他设备文件之前，需准备以下数据。

序号	数据
1	（可选）设备作为 SFTP 客户端时的源地址
2	（可选）SSH 服务器名称
3	（可选）客户端为 SSH 服务器分配的公钥
4	SSH 服务器的 IPv4/IPv6 地址或主机名
5	SSH 服务器当前监听的端口号、SFTP 客户端到 SSH 服务器端的首选加密算法、SSH 服务器端到 SFTP 客户端的首选加密算法、SFTP 客户端到 SSH 服务器端的首选 HMAC 算法、SSH 服务器端到 SFTP 客户端的首选 HMAC 算法、首选密钥交换算法 服务器端配置的用户登录信息
6	SSH 服务器中指定文件的文件名、文件所在的目录

8.7.2 （可选）配置 SFTP 客户端源地址

用户可以配置 SFTP 客户端的源地址信息，从指定的客户端源地址建立 SFTP 连接，保证安全性。

背景信息

用户可以在设备上指定某一接口，为此接口配置 IP 地址，然后使用该 IP 地址作为 SFTP 连接的源 IP 地址，从而达到进行安全校验的目的。

客户端源地址可以配置为源接口或源 IP。

请在作为 SFTP 客户端的路由器上进行如下的配置。

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 **sftp client-source** { **-a** *source-ip-address* | **-i** *interface-type interface-number* }，配置 SFTP 客户端的源地址信息。

----结束

8.7.3 配置用户首次成功登录其他设备（使能 SSH 客户端首次认证功能方式）

使能 SSH 客户端首次认证功能后，当 SFTP 客户端第一次登录 SSH 服务器时，不对 SSH 服务器的 RSA 公钥进行有效性检查。

背景信息

如果配置了使能 SSH 客户端首次认证功能，那么在 SFTP 客户端第一次登录 SSH 服务器后，不对 SSH 服务器的 RSA 公钥进行有效性检查。登录后，系统将自动分配并保存 RSA 公钥，为下次登录时认证。

请在作为 SSH 客户端的路由器上进行如下的配置。

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 **ssh client first-time enable**，使能 SSH 客户端首次认证功能。

缺省情况下，SSH 客户端首次认证功能为关闭状态。

说明

- 使能 SSH 客户端首次认证功能的目的，是当 STelnet 客户端第一次登录 SSH 服务器时，不对 SSH 服务器的 RSA 公钥进行有效性检查，因为此时 STelnet 客户端还没有保存 SSH 服务器的 RSA 公钥。
- 如果没有使能 SSH 客户端首次认证功能，当 STelnet 客户端第一次登录 SSH 服务器时，由于对 SSH 服务器的 RSA 公钥有效性检查失败，会导致登录服务器失败。

窍门

如果 STelnet 客户端需要第一次就成功登录 SSH 服务器，除了使能 SSH 客户端首次认证功能之外，还可以通过事先在客户端为 SSH 服务器分配 RSA 公钥来实现。

----结束

8.7.4 配置用户首次成功登录其他设备（SSH 客户端为 SSH 服务器分配公钥方式）

如果没有使能 SSH 客户端首次认证功能，那么需要在 SFTP 客户端登录 SSH 服务器之前为服务器分配 RSA 公钥。

背景信息

如果没有使能 SSH 客户端首次认证功能，当 SFTP 客户端第一次登录 SSH 服务器时，由于对 SSH 服务器的 RSA 公钥有效性检查失败，从而会导致登录服务器失败。所以需要在 SFTP 客户端登录 SSH 服务器之前为服务器分配 RSA 公钥。

请在作为 SSH 客户端的路由器上进行如下的配置。

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 **rsa peer-public-key** *key-name* ，进入 RSA 公共密钥视图。

步骤 3 执行命令 **public-key-code begin**，进入公共密钥编辑视图。

步骤 4 输入 *hex-data*，编辑公共密钥。

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。

说明

- 在为 SSH 服务器分配 RSA 公钥之前，所分配的 RSA 公钥必须来自 SSH 服务器端，这样 STelnet 客户端对 SSH 服务器的 RSA 公钥有效性检查才会通过。
- 进入公共密钥编辑视图后，即可将服务器上产生的 RSA 公钥传送到客户端。请采用拷贝粘贴方式将 RSA 公钥配置到作为 SSH 客户端的路由器上。

步骤 5 执行命令 **public-key-code end**，退出公共密钥编辑视图。

- 如果未输入合法的密钥编码 *hex-data*，执行 **peer-public-key end** 后，将无法生成密钥。
- 如果步骤 2 中指定的 *key-name* 已经在别的窗口下被删除，再执行 **peer-public-key end** 时，系统会提示：密钥已经不存在，此时直接退到系统视图。

步骤 6 执行命令 **peer-public-key end**，退出公共密钥视图，回到系统视图。

步骤 7 执行命令 **ssh client** *servername* **assign rsa-key** *keyname*，为 SSH 服务器分配 RSA 公钥。

说明

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**，解除 SSH 客户端与 SSH 服务器的绑定关系，再执行命令 **ssh client** *servername* **assign rsa-key** *keyname*，为 SSH 服务器分配新的 RSA 公钥。

----结束

8.7.5 使用 SFTP 命令连接其他设备

用户可以从 SSH 客户端以 SFTP 方式登录到 SSH 服务器上。

背景信息

SFTP 客户端启动命令跟 STelnet 客户端启动命令很相似，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。

在作为 SSH 客户端的路由器上进行如下的配置。

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 **sftp** [**-a** *source-address* | **-i** *interface-type interface-number*] *host-ipv4* [*port*] [[**public-net** | **-vpn-instance** *vpn-instance-name*] | [**prefer_kex** { **dh_group1** | **dh_exchange_group** }] | [**prefer_ctos_cipher** { **des** | **3des** | **aes128** }] | [**prefer_stoc_cipher** { **des** | **3des** | **aes128** }] | [**prefer_ctos_hmac** { **sha1** | **sha1_96** | **md5** | **md5_96** }] | [**prefer_stoc_hmac** { **sha1** | **sha1_96** | **md5** | **md5_96** }]] * [**-ki** *aliveinterval* [**-kc** *alivecountmax*]]，以 SFTP 方式登录到 SSH 服务器上。

说明

成功完成 SSH 登录的首要操作是：配置并产生本地 RSA 密钥对。在进行其它 SSH 配置之前，必须先配置 rsa local-key-pair create，生成本地密钥对。

----结束

8.7.6 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。

背景信息

当 SFTP 客户端登录到 SSH 服务器之后，用户可以在 SFTP 客户端进行如下操作：

- 创建并删除 SSH 服务器上的目录，以及显示当前的工作目录和指定目录下的文件或目录信息
- 改变文件名、删除文件、显示文件列表、上传下载文件
- 查看 SFTP 客户端命令帮助

登录作为 SSH 客户端的路由器进入 SFTP 客户端视图后进行如下的配置。

操作步骤

- 管理目录操作

  可根据需要，执行如下一个或多个操作：

  - 执行命令 **cd** [*remote-directory*]，改变用户的当前工作目录。
  - 执行命令 **cdup**，改变用户的工作目录为当前工作目录的上一级目录。
  - 执行命令 **pwd**，显示用户的当前工作目录。
  - 执行命令 **dir** [**-l -a**] [*path*]，显示指定目录下的文件列表。
  - 执行命令 **rmdir** *remote-directory* & <1-10>，删除服务器上目录。
  - 执行命令 **mkdir** *remote-directory*，在服务器上创建新目录。
- 管理文件操作

  可根据需要，执行如下一个或多个操作：

  - 执行命令 **rename** *old-name new-name*，改变服务器上指定的文件的名字。
  - 执行命令 **get** *remote-filename* [*local-filename*]，下载远程服务器上的文件。
  - 执行命令 **put** *local-filename* [*remote-filename*]，上传本地文件到远程服务器。
  - 执行命令 **remove** *remote-filename*，删除服务器上文件。
- SFTP 客户端命令帮助
  - 执行命令 **help** [**all** | *command-name*]，显示 SFTP 客户端命令帮助。

----结束

8.7.7 检查配置结果

通过 SFTP 访问其他设备的文件配置成功后，可以查看到 SSH 客户端源地址、客户端所有的 SSH 服务器与 RSA 公钥之间的对应关系、SSH 服务器的全局配置信息以及与客户端连接的会话信息。

前提条件

已完成通过 SFTP 访问其他设备的文件的所有配置。

操作步骤

- 使用 **display sftp-client** 命令在 SSH 客户端查看客户端源地址。

----结束

任务示例

在客户端执行命令 **display sftp-client**，可以查看设备作为 SFTP 客户端时的源参数。

```
<Huawei> display sftp-client
Info: The source address of SFTP client is 1.1.1.1
```

8.8 配置举例

配置设备访问其他设备的示例。请结合配置流程图了解配置过程。配置示例中包括组网需求、配置注意事项和配置思路等。

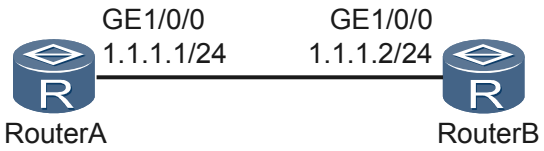
8.8.1 配置 Telnet 终端服务示例

配置 Telnet 终端服务的示例。在本示例中，通过配置用户验证方式和密码，实现 Telnet 登录。

组网需求

如图 8-8 所示，RouterA 与 RouterB 能够相互 Ping 通。用户通过 Telnet 方式从 RouterA 上 Telnet 到 RouterB。

图 8-8 配置 Telnet 终端服务组网图



配置思路

采用如下的思路配置 Telnet 终端服务的基本功能：

1. 在 RouterB 上配置 VTY0 到 VTY4 的验证方式和密码。
2. 从 RouterA 登录到 RouterB 时用户需要输入密码才能登录。
3. 在 RouterB 上配置 Telnet 服务器端口号，用户只能从指定端口登录。

数据准备

为完成此配置例，需准备如下的数据：

- RouterB 的主机地址。
- 验证方式和密码。
- Telnet 服务器端口号。
- 当前进入的用户级别是 15。

操作步骤

步骤 1 配置 IP 地址

配置 RouterA。

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] interface gigabitethernet1/0/0
[RouterA-GigabitEthernet1/0/0] ip address 1.1.1.1 24
[RouterA-GigabitEthernet1/0/0] quit
[RouterA] quit
```

配置 RouterB。

```
<Huawei> system-view
[Huawei] sysname RouterB
[RouterB] interface gigabitethernet1/0/0
[RouterB-GigabitEthernet1/0/0] ip address 1.1.1.2 24
[RouterB-GigabitEthernet1/0/0] quit
[RouterB] quit
```

步骤 2 配置 RouterB 的 Telnet 验证方式和密码

```
<RouterB> system-view
[RouterB] user-interface vty 0 4
[RouterB-ui-vty0-4] authentication-mode password
[RouterB-ui-vty0-4] set authentication password cipher hello
[RouterB-ui-vty0-4] quit
```

如果采用 ACL 方式配置 Telnet 终端服务，需要在 RouterB 上进行如下配置。

```
[RouterB] acl 2000
[RouterB-acl-basic-2000] rule permit source 1.1.1.1 0
[RouterB-acl-basic-2000] quit
[RouterB] user-interface vty 0 4
[RouterB-ui-vty0-4] acl 2000 inbound
```

说明

采用 ACL 方式配置 Telnet 终端服务的配置为可选配置。

步骤 3 验证配置结果

完成以上配置后，可以从 RouterA 上 Telnet 到 RouterB。

```
<RouterA> telnet 1.1.1.2
  Press CTRL_] to quit telnet mode
  Trying 1.1.1.2 ...
  Connected to 1.1.1.2 ...

Login authentication


Password:
<RouterB>
```

步骤 4 配置登录 RouterB 的 Telnet 端口号

```
<RouterB> system-view
[RouterB] telnet server port 1028
 After the command is executed, logging in to the port through telnet fails, al
l the telnet users exit, and a new port is created. If you need to set the port
through telnet again, wait for at least two minutes and then set the port again.
 Are you sure to continue?(y/n)[n]: y
```

步骤 5 使用端口 1028，从 RouterA 上 Telnet 到 RouterB

```
<RouterA> telnet 1.1.1.2 1028
  Press CTRL_] to quit telnet mode
  Trying 1.1.1.2 ...
```

```
  Connected to 1.1.1.2 ...

Login authentication


Password:
<RouterB>
```

----结束

配置文件

- RouterA 的配置文件

```
#
 sysname RouterA
#
interface GigabitEthernet1/0/0
 ip address 1.1.1.1 255.255.255.0
#
return
```

- RouterB 的配置文件

```
#
 sysname RouterB
#
acl number 2000
 rule 5 permit source 1.1.1.1 0
#
interface GigabitEthernet1/0/0
 ip address 1.1.1.2 255.255.255.0
#
user-interface con 0
user-interface vty 0 4
 acl 2000 inbound
 set authentication password cipher %$%$<O9QW-j{{4oqpM#yo.n4″_VM:z\#&q;k5JJQfhV@vq6A’e\
W%$%$
#
return
```

8.8.2 通过重定向登录其他设备配置示例

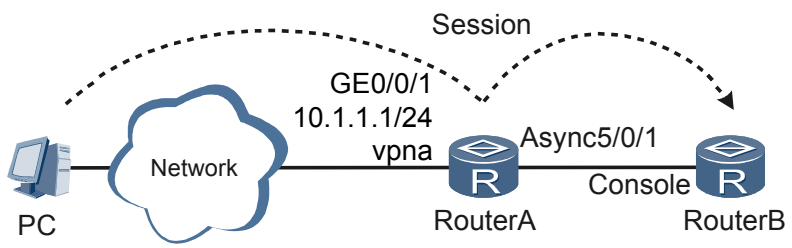
配置重定向登录其他设备的示例。在本示例中，通过使能重定向功能，实现对远程设备的管理。

组网需求

如图 8-9 所示，RouterB 出现故障只能通过 Console 口登录，用户希望只有属于私网 vpna 的用户可以管理登录 RouterB，vpna 私网用户的 PC 与 RouterA 之间有可达路由。

此时，可以使用 RouterA 的异步口与 RouterB 的 Console 口直连，在 RouterA 上使能重定向，并且绑定 VPN 实例。这样私网用户的 PC 上就可以使用指定端口远程登录到 RouterB，实现对 RouterB 的管理。

图 8-9 配置通过重定向登录其他设备组网图



配置思路

采用如下的思路配置通过 Telnet 重定向登录其他设备的基本功能：

1. 将 RouterA 上的异步串口与 RouterB 的连接。
2. 在 RouterA 上使能重定向功能。

数据准备

为完成此配置举例，需准备如下的数据：

- RouterA 的网络侧接口地址为 10.1.1.1/24。

操作步骤

步骤 1 配置异步串口工作在流模式

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] interface async 5/0/1
[RouterA-Async5/0/1] async mode flow
```

步骤 2 获取 TTY 用户界面编号

```
[RouterA] display user-interface
  Idx  Type     Tx/Rx      Modem Privi ActualPrivi Auth  Int
  0    CON 0    9600       -     15    -           N     -
  41   TTY 41   9600       inout 0     -           N     5/0/0
F 42   TTY 42   9600       -     0     -           N     5/0/1
  43   TTY 43   9600       -     0     -           N     5/0/2
  44   TTY 44   9600       -     0     -           N     5/0/3
  45   TTY 45   9600       -     0     -           N     5/0/4
  46   TTY 46   9600       -     0     -           N     5/0/5
  47   TTY 47   9600       -     0     -           N     5/0/6
  48   TTY 48   9600       -     0     -           N     5/0/7
+ 129  VTY 0               -     15    4           N     -
  130  VTY 1               -     15    -           N     -
  131  VTY 2               -     15    -           N     -
  132  VTY 3               -     15    -           N     -
  133  VTY 4               -     15    -           N     -
  145  VTY 16              -     0     -           P     -
  146  VTY 17              -     0     -           P     -
  147  VTY 18              -     0     -           P     -
  148  VTY 19              -     0     -           P     -
  149  VTY 20              -     0     -           P     -
```

步骤 3 使能 RouterA 的重定向功能并与 VPN 绑定

```
[RouterA] user-interface tty 42
[RouterA-ui-tty42] undo shell
[RouterA-ui-tty42] redirect enable
[RouterA-ui-tty42] redirect binding vpn-instance vpna
[RouterA-ui-tty42] quit
[RouterA] quit
```

说明

绑定的 VPN 实例必须与私网用户属于同一 VPN。如果不与 VPN 实例绑定，公网用户和任意私网用户均可以通过重定向功能登录 RouterB。

步骤 4 查看分配的端口

```
<RouterA> display tcp status
TCPCB    Tid/Soid Local Add:port        Foreign Add:port      VPNID  State
19fde824 9  /2    0.0.0.0:22           0.0.0.0:0             23553  Listening
```

```
19fde6c0 9   /1     0.0.0.0:23            0.0.0.0:0             23553  Listening
19fde130 109/1      0.0.0.0:80            0.0.0.0:0             23553  Listening
19fdef18 9   /4     0.0.0.0:2042          0.0.0.0:0             23553  Listening
19fde55c 7   /1     0.0.0.0:7547          0.0.0.0:0             0      Listening
19fdf07c 9   /9     10.137.217.211:23     10.138.77.61:2567     0      Established
19fdf344 9   /10    10.137.217.211:23     10.138.77.69:2824     0      Time_Wait
```

步骤 5 验证配置结果

在 PC 客户端执行 **telnet 10.1.1.1 2042**（2042 为缺省生成的端口号），以指定端口登录到 RouterB 上。

```
C:\Documents and Settings\Administrator> telnet 10.1.1.1 2042
Press CTRL_] to quit telnet mode
  Trying 10.1.1.1...
  Connected to 10.1.1.1...
 [RouterB]
```

----结束

配置文件

- RouterA 的配置文件

```
#
 sysname RouterA
#
ip vpn-instance vpna
 ipv4-family
  route-distinguisher 1:1
  vpn-target 111:1 export-extcommunity
  vpn-target 111:1 import-extcommunity
#
interface Async5/0/1
 async mode flow
#
interface GigabitEthernet 0/0/1
 ip binding vpn-instance vpna
 ip address 10.1.1.1 255.255.255.0
#
user-interface tty 42
 undo shell
 redirect enable
 redirect binding vpn-instance vpna
#
return
```

8.8.3 配置设备作为 STelnet 客户端连接 SSH 服务器的示例

配置设备作为 STelnet 客户端连接 SSH 服务器的示例。在本示例中，通过在 STelnet 客户端和 SSH 服务器端生成本地密钥对，在 SSH 服务器端生成 RSA 公钥、并为用户绑定该 RSA 公钥，实现 Stelnet 客户端连接 SSH 服务器。

组网需求

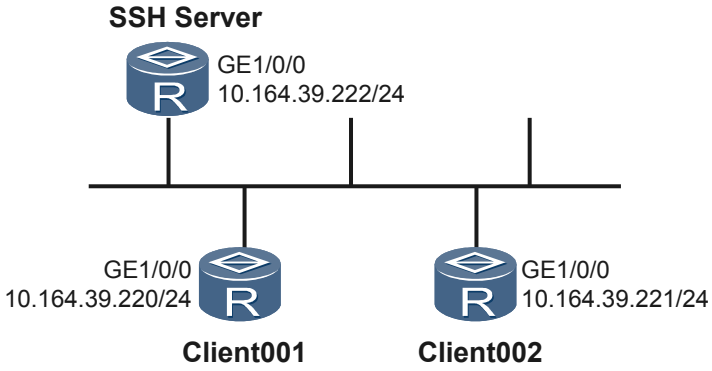
如图 8-10 所示，SSH 服务器端 STelnet 服务使能后，STelnet 客户端可以通过 Password、RSA、password-rsa 或 all 认证的方式登录到 SSH 服务器端。

配置两个登录用户：

- 用户 Client001，密码为“huawei”，登录验证方式为 password。
- 用户 Client002，验证方式为 RSA，并为其分配公钥 RsaKey001。

用户界面仅支持 SSH 协议。

图 8-10 配置设备作为 STelnet 客户端连接 SSH 服务器组网图



配置思路

采用如下的思路配置设备作为 STelnet 客户端连接 SSH 服务器：

1. 用户 Client001 和 Client002 的配置均在 SSH 服务器上完成。
2. 分别在 STelnet 客户端和 SSH 服务器端生成本地密钥对。
3. 在 SSH 服务器端生成 RSA 公钥，并为用户 Client002 绑定 SSH 客户端的 RSA 公钥。
4. SSH 服务器端 STelnet 服务使能。
5. 用户 Client001 和 Client002 分别以 STelnet 方式登录 SSH 服务器。

数据准备

为完成此配置例，需准备如下的数据：

- SSH 用户名及认证方式。
- SSH 用户密码或 RSA 公钥。
- SSH 服务器名。

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] rsa local-key-pair create
The key name will be: Host
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
       It will take a few minutes.
Input the bits in the modulus[default = 512]: 768
Generating 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 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，配置密码为 huawei，且认证方式为 password。

  ```
  [SSH Server] aaa
  [SSH Server-aaa] local-user client001 password huawei
  [SSH Server-aaa] local-user client001 service-type ssh
  [SSH Server-aaa] quit
  [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，配置密码为 huawei，且认证方式为 RSA。

  ```
  [SSH Server] aaa
  [SSH Server-aaa] local-user client002 password huawei
  [SSH Server-aaa] local-user client002 service-type ssh
  [SSH Server-aaa] quit
  [SSH Server] ssh user client002 authentication-type rsa
  ```

步骤 3 配置服务器端 RSA 公钥

客户端 Client002 生成客户端的本地密钥对

```
<Huawei> system-view
[Huawei] sysname client002
[client002] rsa local-key-pair create
```

查看客户端上生成 RSA 公钥。

```
[client002] display rsa local-key-pair public
=====================================================
Time of Key pair created: 2007-12-29 16:19:59+08:00
Key name: Host
Key type: RSA encryption Key
=====================================================
Key code:
3047
  0240
    BFF35E4B C61BD786 F907B5DE 7D6770C3 E5FD17AB
    203C8FCB BBC8FDF2 F7CB674E 519E8419 0F6B97A8
    EA91FC4B B9E18836 5E74BFD5 4C687767 A89C6B43
    1D7E3E1B
  0203
    010001
=====================================================
Time of Key pair created: 2007-12-29 16:20:05+08:00
Key name: Server
Key type: RSA encryption Key
=====================================================
Key code:
3067
  0260
    BCFAC085 49A2E70E 1284F901 937D7B63 D7A077AB
    D2797280 4BCA86C0 4CD18B70 5DFAC9D3 9A3F3E74
    9B2AF4CB 69FA6483 E87DA590 7B47721A 16391E27
    1C76ABAB 743C568B 1B35EC7A 8572A096 BCA9DF0E
    BC89D3DB 5A83698C 9063DB39 A279DD89
  0203
    010001
[client002]
```

将客户端上产生的 RSA 公钥传送到服务器端。

```
[SSH Server] rsa peer-public-key RsaKey001
Enter "RSA public key" view, return system view with "peer-public-key end".
```

```
NOTE: The number of the bits of public key must be between 769 and 2048.
[SSH Server-rsa-public-key] public-key-code begin
Enter "RSA key code" view, return last view with "public-key-code end".
[SSH Server-rsa-key-code] 3047
[SSH Server-rsa-key-code] 0240
[SSH Server-rsa-key-code] BFF35E4B C61BD786 F907B5DE 7D6770C3 E5FD17AB
[SSH Server-rsa-key-code] 203C8FCB BBC8FDF2 F7CB674E 519E8419 0F6B97A8
[SSH Server-rsa-key-code] EA91FC4B B9E18836 5E74BFD5 4C687767 A89C6B43
[SSH Server-rsa-key-code] 1D7E3E1B
[SSH Server-rsa-key-code] 0203
[SSH Server-rsa-key-code] 010001
[SSH Server-rsa-key-code] public-key-code end
[SSH Server-rsa-public-key] peer-public-key end
```

步骤 4 为 SSH 用户 Client002 绑定 SSH 客户端的 RSA 公钥。

```
[SSH Server] ssh user client002 assign rsa-key RsaKey001
```

步骤 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。

```
<Huawei> system-view
[Huawei] sysname client001
[client001] ssh client first-time enable
<Huawei> system-view
[Huawei] sysname client002
[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> system-view
[client001] stelnet 10.164.39.222
Please input the username:client001
Trying 10.164.39.222 ...
Press CTRL+K to abort
Connected to 10.164.39.222 ...
Enter password:
```

输入密码 huawei，显示登录成功信息如下：

```
Info: The max number of VTY users is 20, and the number
      of current VTY users on line is 6.
      The current login time is 2010-09-06 11:42:42.
<SSH Server>
```

STelnet 客户端 Clent002 用 RSA 认证方式连接 SSH 服务器。

```
<client002> system-view
[client002] stelnet 10.164.39.222
Please input the username: client002
Trying 10.164.39.222 ...
Press CTRL+K to abort
Connected to 10.164.39.222 ...
The server is not authenticated. Do you 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: 10.164.39.222. Please wait...
Info: The max number of VTY users is 20, and the number
      of current VTY users on line is 6.
      The current login time is 2010-09-06 11:42:42.
<SSH Server>
```

步骤 6 验证配置结果

配置完成后，在 SSH 服务器端执行 **display ssh server status** 命令和 **display ssh server session** 命令，可以查看到 STelnet 客户端已经成功连接到 SSH 服务器。

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
```

查看 SSH 服务器的连接信息。

```
[SSH Server] display ssh server session
-------------------------------------------------------------------
 Conn    Ver   Encry     State  Auth-type        Username
 -----------------------------------------------------------------
 VTY 3  2.0   AES       run    password         client001
 VTY 4  2.0   AES       run    rsa              client002
 -----------------------------------------------------------------
```

查看 SSH 用户信息。

```
[SSH Server] display ssh user-information
 ------------------------------------------------------------------------------
 Username         Auth-type          User-public-key-name
 ------------------------------------------------------------------------------
 client001        password           null
 client002        rsa                RsaKey001
 ------------------------------------------------------------------------------
```

----结束

配置文件

- SSH 服务器的配置文件

```
#
 sysname SSH Server
#
 rsa peer-public-key rsakey001
  public-key-code begin
   3047
     0240
BFF35E4B C61BD786 F907B5DE 7D6770C3 E5FD17AB 203C8FCB BBC8FDF2 F7CB674E
       519E8419 0F6B97A8 EA91FC4B B9E18836 5E74BFD5 4C687767 A89C6B43 1D7E3E1B      0203
       010001
  public-key-code end
 peer-public-key end
#
aaa
 local-user client001 password N`C55QK<`=/Q=^Q`MAF4<1!!
 local-user client001 service-type ssh
 local-user client002 password N`C55QK<`=/Q=^Q`MAF4<1!!
 local-user client002 service-type ssh
#
 ssh user client002 authentication-type rsa
 ssh user client002 assign rsa-key RsaKey001
#
user-interface vty 0 4
 authentication-mode aaa
 protocol inbound ssh
#
return
```

- SSH 客户端 Client001 的配置文件

```
#
 sysname client001
#
interface GigabitEthernet1/0/0
 ip address 10.164.39.220 255.255.255.0
#
ssh client first-time enable
```

```
#
return
```

- SSH 客户端 Client002 的配置文件

```
#
 sysname client002
#
interface GigabitEthernet1/0/0
 ip address 10.164.39.221 255.255.255.0
#
ssh client first-time enable
#
return
```

8.8.4 配置 TFTP 示例

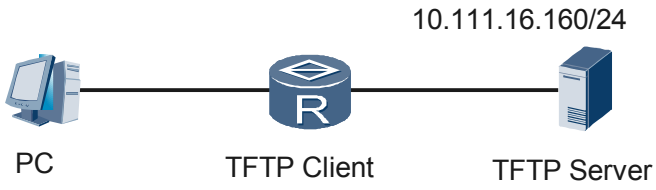
配置 TFTP 的示例。在本示例中，通过在 TFTP 服务器端运行 TFTP 软件，并设置源文件在服务器中的位置，实现上传和下载文件。

组网需求

如图 8-11 所示，TFTP 服务器 IP 地址为 10.111.16.160/24。

从超级终端登录到路由器，再从 TFTP 服务器下载文件 ar.cc。

图 8-11 配置 TFTP 组网图



配置思路

采用如下的思路配置 TFTP 服务器基本功能：

1. 在 TFTP 服务器端运行 TFTP 软件，并设置源文件在服务器中的位置。
2. 在路由器上使用 TFTP 命令下载文件。
3. 在路由器上使用 TFTP 命令上传文件。

数据准备

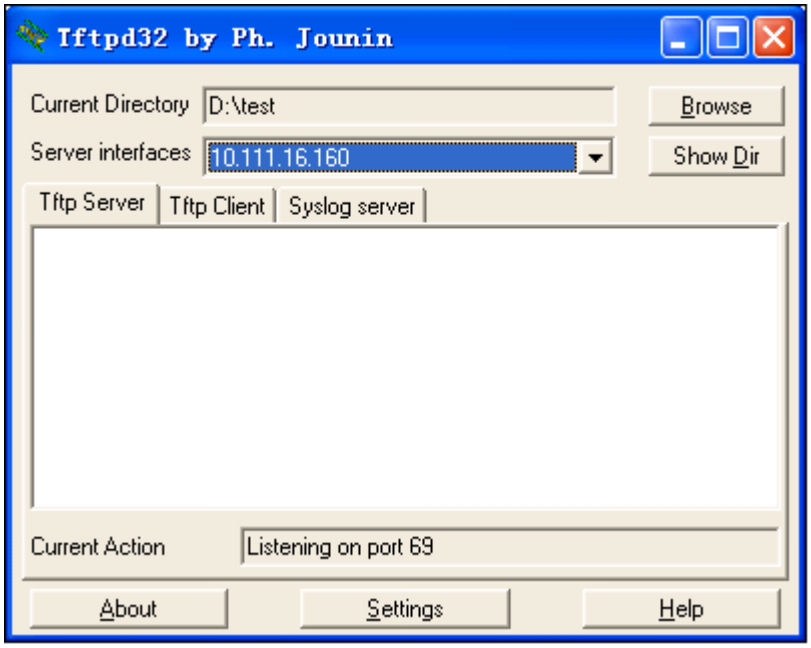
为完成此配置例，需准备如下的数据：

- TFTP 服务器端安装 TFTP 软件。
- 源文件在 TFTP 服务器中的路径。
- 目标文件名及在路由器存放的路径。

操作步骤

步骤 1 启动 TFTP 服务器，设置 TFTP 服务器的 Current Directory 目录为文件 ar.cc 所在的目录。界面如图 8-12。

图 8-12 设置 TFTP 服务器基础目录



说明

由于计算机使用的 TFTP 服务器软件不同，屏幕显示可能不同。

步骤 2 通过计算机超级终端登录到路由器，输入以下命令下载文件。

```
<Huawei> tftp 10.111.16.160 get ar.cc sd1:/
Info: Transfer file in binary mode.
Downloading the file from the remote TFTP server. Please wait...
       69143936 bytes received in 42734 second.
TFTP: Downloading the file successfully.
```

步骤 3 检查配置结果，通过 **dir** 命令查看：下载的目标文件是否存在于指定的路由器目录下。

```
<Huawei> dir sd1:/
Directory of sd1:/

  Idx  Attr     Size(Byte)  Date        Time(LMT)  FileName
    0  -rw-      1,738,816  Mar 28 2011 17:00:24   web.zip
    1  -rw-            396  Feb 11 2008 14:34:17   rsa_host_key.efs
    2  -rw-            540  Feb 11 2008 14:35:10   rsa_server_key.efs
    3  -rw-          1,498  Apr 01 2011 09:49:37   iascfg.zip
    4  -rw-        525,337  Apr 01 2011 09:50:00   private-data.txt
    5  -rw-          1,215  Mar 26 2011 11:32:27   iascfg_autobackup.zip
    6  -rw-      1,703,936  Feb 27 2008 10:00:10   ar_1220_b230_smk2.cc
    7  drw-              -  Mar 07 2008 15:44:46   dd
    8  -rw-     69,143,936  Mar 28 2008 07:34:54   ar.cc
    9  -rw-          8,996  Apr 07 2008 14:56:24   1.cap
   10  -rw-          5,602  May 27 2011 13:59:31   ab.cap
   11  -rw-            220  Mar 28 2011 16:51:16   elab.txt
   12  -rw-          1,686  Mar 28 2011 17:04:53   lic_ar.dat

1,933,056 KB total(1,861,426 KB free)
```

步骤 4 通过计算机超级终端登录到路由器，输入以下命令上传文件。

```
<Huawei> tftp 10.111.16.160 put sd1:/iascfg.zip
Info: Transfer file in binary mode.
Uploading the file to the remote TFTP server. Please wait...
```

```
TFTP: Uploading the file successfully.
    3856 bytes send in 1 second.
```

----结束

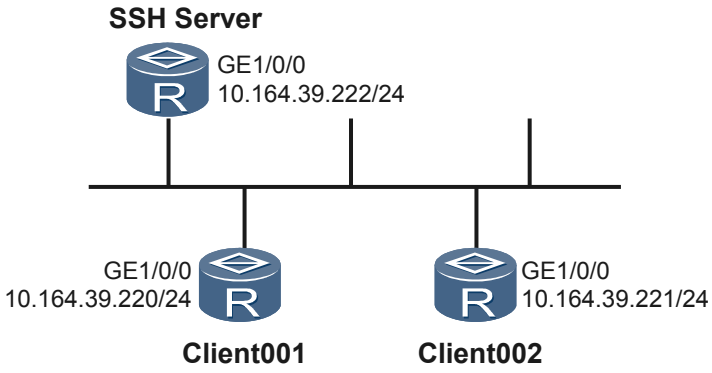
8.8.5 配置 SFTP 客户端连接 SSH 服务器的示例

配置 SFTP 客户端连接 SSH 服务器的示例。在本示例中，通过在 SFTP 客户端和 SSH 服务器端生成本地密钥对，在 SSH 服务器端生成 RSA 公钥，并为用户绑定该 RSA 公钥，实现 SFTP 客户端连接 SSH 服务器。

组网需求

如图 8-13 所示，SSH 服务器端 SFTP 服务使能后，SFTP Client 端可以通过 Password、RSA、password-rsa、all 认证的方式登录到 SSH 服务器端。

图 8-13 配置 SFTP 客户端连接 SSH 服务器组网图



配置思路

采用如下思路配置 SFTP 客户端连接 SSH 服务器的示例：

1. 用户 Client001 和 Client002 的配置均在 SSH 服务器上完成。
2. 分别在 SFTP 客户端和 SSH 服务器端生成本地密钥对。
3. 在 SSH 服务器端生成 RSA 公钥，并为用户 Client002 绑定 SSH 客户端的 RSA 公钥。
4. SSH 服务器端 SFTP 服务使能。
5. 配置 SSH 用户的服务方式和授权目录。
6. 用户 Client001 和 Client002 分别以 SFTP 方式登录 SSH 服务器。

数据准备

为完成此配置例，需准备如下的数据：

- SSH 用户名及认证方式。
- SSH 用户密码或 RSA 公钥。
- SSH 服务器名。

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] rsa local-key-pair create
The key name will be: Host
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
       It will take a few minutes.
Input the bits in the modulus[default = 512]: 768
Generating 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 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，配置密码为 huawei，且认证方式为 password。

  ```
  [SSH Server] aaa
  [SSH Server-aaa] local-user client001 password huawei
  [SSH Server-aaa] local-user client001 service-type ssh
  [SSH Server-aaa] local-user client001 privilege level 3
  [SSH Server-aaa] local-user client001 ftp-directory flash:
  [SSH Server-aaa] quit
  ```

- 创建 SSH 用户 Client002。

  # 新建用户名为 Client002 的 SSH 用户，配置密码为 huawei，且认证方式为 RSA。

  ```
  [SSH Server] aaa
  [SSH Server-aaa] local-user client002 password huawei
  [SSH Server-aaa] local-user client002 service-type ssh
  [SSH Server-aaa] local-user client002 privilege level 3
  [SSH Server-aaa] local-user client002 ftp-directory flash:
  [SSH Server-aaa] quit
  [SSH Server] ssh user client002 authentication-type rsa
  ```

步骤 3 配置服务器端 RSA 公钥

客户端 Client002 生成客户端的本地密钥对

```
<Huawei> system-view
[Huawei] sysname client002
[client002] rsa local-key-pair create
```

查看客户端上生成 RSA 公钥。

```
[client002] display rsa local-key-pair public
=============================================
Time of Key pair created: 2007-12-29 16:19:59+08:00
Key name: Host
Key type: RSA encryption Key
=============================================
Key code:
3047
  0240
    BFF35E4B C61BD786 F907B5DE 7D6770C3 E5FD17AB
```

```
    203C8FCB BBC8FDF2 F7CB674E 519E8419 0F6B97A8
    EA91FC4B B9E18836 5E74BFD5 4C687767 A89C6B43
    1D7E3E1B
  0203
    010001
=====================================================
Time of Key pair created: 2007-12-29 16:20:05+08:00
Key name: Server
Key type: RSA encryption Key
=====================================================
Key code:
3067
  0260
    BCFAC085 49A2E70E 1284F901 937D7B63 D7A077AB
    D2797280 4BCA86C0 4CD18B70 5DFAC9D3 9A3F3E74
    9B2AF4CB 69FA6483 E87DA590 7B47721A 16391E27
    1C76ABAB 743C568B 1B35EC7A 8572A096 BCA9DF0E
    BC89D3DB 5A83698C 9063DB39 A279DD89
  0203
    010001
[client002]
```

将客户端上产生的 RSA 公钥传送到服务器端。

```
[SSH Server] rsa peer-public-key RsaKey001
Enter "RSA public key" view, return system view with "peer-public-key end".
NOTE: The number of the bits of public key must be between 769 and 2048.
[SSH Server-rsa-public-key] public-key-code begin
Enter "RSA key code" view, return last view with "public-key-code end".
[SSH Server-rsa-key-code] 3047
[SSH Server-rsa-key-code] 0240
[SSH Server-rsa-key-code] BFF35E4B C61BD786 F907B5DE 7D6770C3 E5FD17AB
[SSH Server-rsa-key-code] 203C8FCB BBC8FDF2 F7CB674E 519E8419 0F6B97A8
[SSH Server-rsa-key-code] EA91FC4B B9E18836 5E74BFD5 4C687767 A89C6B43
[SSH Server-rsa-key-code] 1D7E3E1B
[SSH Server-rsa-key-code] 0203
[SSH Server-rsa-key-code] 010001
[SSH Server-rsa-key-code] public-key-code end
[SSH Server-rsa-public-key] peer-public-key end
```

步骤 4 为 SSH 用户 Client002 绑定 SSH 客户端的 RSA 公钥。

```
[SSH Server] ssh user client002 assign rsa-key RsaKey001
```

步骤 5 SSH 服务器端 SFTP 服务使能

使能 SFTP 服务功能

```
[SSH Server] sftp server enable
```

步骤 6 SFTP 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。

```
<Huawei> system-view
[Huawei] sysname client001
[client001] ssh client first-time enable
<Huawei> system-view
[Huawei] sysname client002
[client002] ssh client first-time enable
```

SFTP 客户端 Client001 用 password 认证方式连接 SSH 服务器。

```
<client001> system-view
[client001] sftp 10.164.39.222
Please input the username:client001
Trying 10.164.39.222 ...
Press CTRL+K to abort
Connected to 10.164.39.222 ...
Enter password:
```

```
sftp-client>
```

SFTP 客户端 Client002 用 RSA 认证方式连接 SSH 服务器。

```
<client002> system-view
[client002] sftp 10.164.39.222
Please input the username: client002
Trying 10.164.39.222 ...
Press CTRL+K to abort
Connected to 10.164.39.222 ...
sftp-client>
```

步骤 7 检查配置结果

配置完成后，在 SSH 服务器端执行 **display ssh server status** 命令和 **display ssh server session** 命令，可以查看到 SFTP 服务已经使能，并且 SFTP 客户端已经成功连接到 SSH 服务器。

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
```

查看 SSH 服务器的连接信息。

```
[SSH Server] display ssh server session
-------------------------------------------------------------------
 Conn    Ver   Encry     State  Auth-type        Username
 -----------------------------------------------------------------
 VTY 3   2.0   AES       run    password         client001
 VTY 4   2.0   AES       run    rsa              client002
 -----------------------------------------------------------------
```

查看 SSH 用户信息。

```
[SSH Server] display ssh user-information
 ------------------------------------------------------------------------------
 Username         Auth-type          User-public-key-name
 ------------------------------------------------------------------------------
 client001        password           null
 client002        rsa                RsaKey001
 ------------------------------------------------------------------------------
```

----结束

配置文件

- SSH 服务器上的配置文件

```
#
 sysname SSH Server
#
 rsa peer-public-key rsakey001
  public-key-code begin
   3047
     0240
       C4989BF0 416DA8F2 2675910D 7F2997E8 5573A35D 0163FD4A FAC39A6E 0F45F325
       A4E3AA1D 54692B04 C6A28D3D C58DE2E8 E0D58D65 7A25CF92 A74D21F9 E917182B
     0203
       010001
  public-key-code end
 peer-public-key end
#
aaa
```

```
 local-user client001 password N`C55QK<`=/Q=^Q`MAF4<1!!
 local-user client001 privilege level 3
 local-user client001 ftp-directory flash:
 local-user client001 service-type ssh
 local-user client002 password N`C55QK<`=/Q=^Q`MAF4<1!!
 local-user client002 privilege level 3
 local-user client002 ftp-directory flash:
 local-user client002 service-type ssh
#
 sftp server enable
 ssh user client002 authentication-type rsa
 ssh user client002 assign rsa-key RsaKey001
 #
user-interface vty 0 4
 authentication-mode aaa
 protocol inbound ssh
#
Return
```

- SSH 客户端 Clien001 的配置文件

```
#
 sysname client001
#
interface GigabitEthernet1/0/0
 ip address 10.164.39.220 255.255.255.0
#
 ssh client first-time enable
#
return
```

- SSH 客户端 Clien002 的配置文件

```
#
 sysname client002
#
interface GigabitEthernet1/0/0
 ip address 10.164.39.221 255.255.255.0
#
 ssh client first-time enable
#
return
```

8.8.6 配置 SSH 支持 RADIUS 认证的示例

配置 SSH 支持 RADIUS 认证的示例。在本示例中，通过 RADIUS 服务器认证用户信息，实现 SSH 服务器根据认证结果决定是否允许 SSH 客户端建立连接。

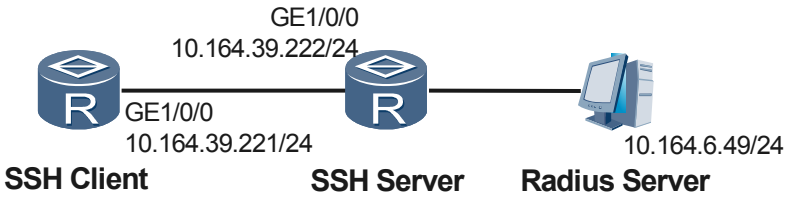
组网需求

如果 RADIUS 用户连接 SSH 服务器，那么在 SSH 认证过程中，SSH 服务器将 SSH 客户端的认证信息（用户名、密码）发送给 RADIUS 服务器（兼容 TACACS 服务器）进行认证。

RADIUS 服务器认证该用户，将认证结果（成功、失败，如果成功还包含用户等级）返回给 SSH 服务器。SSH 服务器根据认证结果决定是否允许 SSH 客户端建立连接。

组网图如图 8-14 所示。

图 8-14 配置 SSH 支持 RADIUS 认证组网图



配置思路

采用如下的思路配置 SSH 支持 RADIUS 认证的示例：

1. SSH 服务器端配置 RADIUS 模板。
2. SSH 服务器端配置域。
3. RADIUS 服务器创建用户。
4. 分别在 SSH 客户端和 SSH 服务器端生成本地密钥对。
5. 在 SSH 服务器端生成 RSA 公钥，并为用户 ssh2@ssh.com 绑定 SSH 客户端的 RSA 公钥。
6. SSH 服务器端 STelnet 和 SFTP 服务使能。
7. 配置 SSH 用户的服务方式和授权目录。
8. 用户 ssh1@ssh.com 和 ssh2@ssh.com 分别以 STelnet 和 SFTP 方式登录 SSH 服务器。

数据准备

为完成此配置例，需准备如下的数据：

- 配置 STelnet 用户采用的认证方式为 Password。
- 配置 SFTP 用户采用的认证方式为 RSA。
- 认证模式为 RADIUS。
- RADIUS 模板名称。
- RADIUS 域名称。
- RADIUS 用户名称和密码。

操作步骤

步骤 1 在 SSH 服务器端生成本地密钥对

```
<Huawei> system-view
[Huawei] rsa local-key-pair create
The key name will be: Host
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
       It will take a few minutes.
Input the bits in the modulus[default = 512]: 768
Generating keys...
.......++++++++++++
..........++++++++++++
.....................................++++++++
......++++++++
```

步骤 2 配置服务器端 RSA 公钥

客户端生成客户端的本地密钥对

```
<Huawei> system-view
[Huawei] sysname client
[client] rsa local-key-pair create
```

查看客户端上生成 RSA 公钥。

```
[client] display rsa local-key-pair public
=====================================================
Time of Key pair created: 16:38:51  2007/5/25
Key name: Host
Key type: RSA encryption Key
=====================================================
Key code:
3047
  0240
    BFF35E4B C61BD786 F907B5DE 7D6770C3 E5FD17AB
    203C8FCB BBC8FDF2 F7CB674E 519E8419 0F6B97A8
    EA91FC4B B9E18836 5E74BFD5 4C687767 A89C6B43
    1D7E3E1B
  0203
    010001
=====================================================
Time of Key pair created: 16:38:51  2007/5/25
Key name: Server
Key type: RSA encryption Key
=====================================================
Key code:
3067
  0260
    BCFAC085 49A2E70E 1284F901 937D7B63 D7A077AB
    D2797280 4BCA86C0 4CD18B70 5DFAC9D3 9A3F3E74
    9B2AF4CB 69FA6483 E87DA590 7B47721A 16391E27
    1C76ABAB 743C568B 1B35EC7A 8572A096 BCA9DF0E
    BC89D3DB 5A83698C 9063DB39 A279DD89
  0203
    010001
[client]
```

将客户端上产生的 RSA 公钥传送到服务器端。

```
[Huawei] rsa peer-public-key RsaKey001
Enter "RSA public key" view, return system view with "peer-public-key end".
[Huawei-rsa-public-key] public-key-code begin
Enter "RSA key code" view, return last view with "public-key-code end".
[Huawei-rsa-key-code] 3047
[Huawei-rsa-key-code] 0240
[Huawei-rsa-key-code] BFF35E4B C61BD786 F907B5DE 7D6770C3 E5FD17AB
[Huawei-rsa-key-code] 203C8FCB BBC8FDF2 F7CB674E 519E8419 0F6B97A8
[Huawei-rsa-key-code] EA91FC4B B9E18836 5E74BFD5 4C687767 A89C6B43
[Huawei-rsa-key-code] 1D7E3E1B
[Huawei-rsa-key-code] 0203
[Huawei-rsa-key-code] 010001
[Huawei-rsa-key-code] public-key-code end
[Huawei-rsa-public-key] peer-public-key end
```

步骤 3 创建 SSH 用户

在 RADIUS 服务器端，添加两个用户，用户名分别为 ssh1@ssh.com 和 ssh2@ssh.com；另外还须指定 NAS 的地址 10.164.39.222 和密钥 huawei。NAS 的地址是指和 RADIUS 服务器连接的 SSH 服务器的地址。

在 SSH 服务器端配置 VTY 用户界面。

```
[Huawei] user-interface vty 0 4
[Huawei-ui-vty0-4] authentication-mode aaa
```

```
[Huawei-ui-vty0-4] protocol inbound ssh
[Huawei-ui-vty0-4] quit
```

在 SSH 服务器端创建 SSH 用户 ssh1@ssh.com 和 ssh2@ssh.com，并指定认证方式。

```
[Huawei] aaa
[Huawei-aaa] local-user ssh1@ssh.com password huawei
[Huawei-aaa] local-user ssh1@ssh.com service-type ssh
[Huawei-aaa] local-user ssh2@ssh.com password huawei
[Huawei-aaa] local-user ssh2@ssh.com service-type ssh
[Huawei-aaa] local-user ssh2@ssh.com ftp-directory flash:
[Huawei-aaa] local-user ssh2@ssh.com privilege level 15
[Huawei-aaa]
[Huawei-aaa] quit
[Huawei] ssh user ssh1@ssh.com authentication-type password
[Huawei] ssh user ssh2@ssh.com authentication-type rsa
[Huawei] ssh user ssh2@ssh.com assign rsa-key RsaKey001
```

步骤 4 配置 RADIUS 模板

配置认证方案 newscheme，认证方法为 RADIUS。

```
[Huawei] aaa
[Huawei-aaa] authentication-scheme newscheme
[Huawei-aaa-authen-newscheme] authentication-mode radius
[Huawei-aaa-authen-newscheme] quit
```

配置 SSH 服务端的 RADIUS 模板为 ssh。

```
[Huawei] radius-server template ssh
```

配置 RADIUS 认证服务器的 IP 地址为 10.164.6.49 和端口 1812。

```
[Huawei-radius-ssh] radius-server authentication 10.164.6.49 1812
```

配置 RADIUS 服务器密钥为 huawei。

```
[Huawei-radius-ssh] radius-server shared-key cipher huawei
[Huawei-radius-ssh] quit
```

步骤 5 配置 RADIUS 域名

配置 SSH 服务端的 RADIUS 域名为 ssh.com，在域下应用认证方案 newscheme、RADIUS 模板 ssh。

```
[Huawei] aaa
[Huawei-aaa] domain ssh.com
[Huawei-aaa-domain-ssh.com] authentication-scheme newscheme
[Huawei-aaa-domain-ssh.com] radius-server ssh
[Huawei-aaa-domain-ssh.com] quit
[Huawei-aaa] quit
```

步骤 6 SSH 客户端连接 SSH 服务器。

使能 SSH 服务器端的 SFTP 服务功能。

```
[Huawei] sftp server enable
```

第一次登录，则需要使能 SSH 客户端首次认证功能。

```
[client] ssh client first-time enable
[client] quit
```

STelnet 客户端采用 RADIUS 认证连接 SSH 服务器。

```
<client> system-view
[client] stelnet 10.164.39.222
Please input the username: ssh1@ssh.com
Trying 10.164.39.222 ...
```

```
Press CTRL+K to abort
Connected to 10.164.39.222 ...
The server is not authenticated. Do you 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: 10.164.39.222. Please wait...
Enter password:
```

输入密码 huawei，显示登录成功信息如下：

```
Info: The max number of VTY users is 10, and the current number
      of VTY users on line is 2.
<Huawei>
```

SFTP 客户端采用 RADIUS 认证连接 SSH 服务器。

```
<client> system-view
[client] sftp 10.164.39.222
Please input the username: ssh2@ssh.com
Trying 10.164.39.222 ...
Press CTRL+K to abort
Connected to 10.164.39.222 ...
Enter password:
sftp-client>
```

步骤 7 检查配置结果

配置完成后，在 SSH 服务器端执行 **display radius-server configuration** 命令和 **display ssh server session** 命令，可以查看到 SSH 服务器端关于 RADIUS 服务器的配置，并且看到 STelnet 客户端或 SFTP 客户端采用 RADIUS 认证已经成功连接到 SSH 服务器。

查看 RADIUS 服务器的配置信息。

```
[Huawei-aaa] display radius-server configuration
-------------------------------------------------------------------
  Server-template-name             :  ssh
  Protocol-version                 :  standard
  Traffic-unit                     :  B
  Shared-secret-key                :  N`C55QK<`=/Q=^Q`MAF4<1!!
  Timeout-interval(in second)      :  5
  Primary-authentication-server    :  10.164.6.49    :1812    LoopBack:NULL
  Primary-accounting-server        :  0.0.0.0        :0       LoopBack:NULL
  Secondary-authentication-server  :  0.0.0.0        :0       LoopBack:NULL
  Secondary-accounting-server      :  0.0.0.0        :0       LoopBack:NULL
  Retransmission                   :  3
  Domain-included                  :  YES
  -------------------------------------------------------------------
```

查看 SSH 服务器的连接信息。

```
[Huawei] display ssh server session
-------------------------------------------------------------------
 Conn    Ver   Encry     State  Auth-type        Username
 -------------------------------------------------------------------
 VTY 0  2.0   AES       run    password         ssh1@ssh.com
 VTY 1  2.0   AES       run    rsa              ssh2@ssh.com
 -------------------------------------------------------------------
```

----结束

配置文件

SSH 服务器的配置文件

```
#
radius-server template ssh
 radius-server authentication 10.164.6.49 1812
#
 rsa peer-public-key rsakey001
```

```
  public-key-code begin
   3047
     0240
       C4989BF0 416DA8F2 2675910D 7F2997E8 5573A35D 0163FD4A FAC39A6E 0F45F325
       A4E3AA1D 54692B04 C6A28D3D C58DE2E8 E0D58D65 7A25CF92 A74D21F9 E917182B
     0203
       010001
  public-key-code end
 peer-public-key end
#
aaa
 authentication-scheme newscheme
 authentication-mode radius
 local-user ssh1@ssh.com password N`C55QK<`=/Q=^Q`MAF4<1!!
 local-user ssh1@ssh.com service-type ssh
 local-user ssh2@ssh.com password N`C55QK<`=/Q=^Q`MAF4<1!!
 local-user ssh2@ssh.com privilege level 15
 local-user ssh2@ssh.com ftp-directory flash:
 local-user ssh2@ssh.com service-type ssh
#
 domain ssh.com
  authentication-scheme newscheme
  radius-server ssh
#
 sftp server enable
 ssh user ssh1@ssh.com
 ssh user ssh2@ssh.com
 ssh user ssh2@ssh.com assign rsa-key RsaKey001
#
user-interface vty 0 4
 authentication-mode aaa
 protocol inbound ssh
#
return
```

9 升级与维护

关于本章

通过升级与维护，实现优化路由器系统配置、监控设备运行状态以及简化运行维护，降低运营商的运营成本。

9.1 升级与维护简介
用户可以通过激活 GTL License 文件、升级系统软件、管理补丁、监控 CPU 和内存占用率、重启等操作实现设备的升级与维护。

9.2 激活 GTL License 文件
GTL（Global Trotter License） License 文件是华为公司提供给用户对设备的容量、功能和期限等进行授权的授权文件。

9.3 升级系统软件
升级设备软件可以实现设备原有性能的优化、新性能的增加以及解决当前运行版本更新不及时的问题。

9.4 管理补丁
介绍补丁的几种使用方法。通过安装补丁可以在不中断业务的情况下，实现系统升级。通过指定下次启动的补丁文件可以为系统指定下次启动后执行的补丁文件。通过卸载补丁可以去激活不符合系统要求的补丁，或者删除系统不需要的补丁文件，从而释放设备主控板补丁区的内存空间。

9.5 监控 CPU 和内存的占用率
通过对 CPU 和内存占用率进行告警阈值配置，可以监控 CPU 和内存的使用情况，及时了解系统运行的性能。

9.6 重新启动设备
当路由器升级系统软件后，需要重新启动路由器使配置生效。或者因为大量临时文件而导致系统瘫痪是，需要重新启动设备。

9.7 配置举例
配置示例中包括组网需求、配置注意事项和配置思路等。

9.1 升级与维护简介

用户可以通过激活 GTL License 文件、升级系统软件、管理补丁、监控 CPU 和内存占用率、重启等操作实现设备的升级与维护。

9.1.1 License 授权

AR3200 提供了 License 授权的管理平台。用户可以对 License 文件进行申请、升级和激活等操作，获得相应权限。

通过 License 授权模式，新用户可以根据需要购买相应的业务功能模块和资源权限，降低购买成本；升级扩容用户可以在扩容时通过申请新的 License 达到容量的扩充以及功能的支持和维护。

SSL VPN 功能需要 License 授权。

在 AR3200 设备上，语音的 PBX 功能需要 License 授权。

9.1.2 软件升级

可以通过对补丁包文件、系统软件、配置文件、PAF 文件和 License 文件等进行升级操作，从而升级设备系统软件，以满足用户新的功能需求。

软件升级涉及软件下载和启动加载。

9.1.3 补丁管理

通过给主机软件加载补丁，可以在不中断设备运行的情况下实现对主机软件的动态在线升级，从而避免影响系统业务，有利于提高通信服务质量。

在设备的运行过程中，有时需要对主机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、增加新功能以适应业务需求等。传统的做法是对主机软件进行静态的停机升级，这将使系统的业务受到影响，不利于提高通信服务质量。

通过对补丁进行管理，可以实现对主机软件的动态在线升级从而解决上述问题。

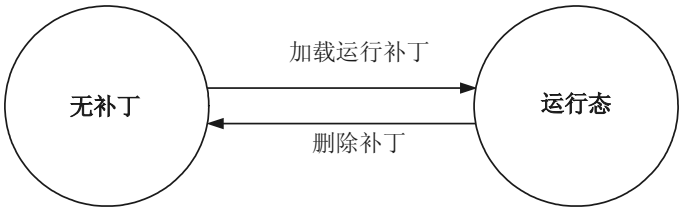
设备支持的补丁状态详细信息如表 9-1 所示。

表 9-1 补丁的状态说明

状态	说明	各状态之间的转换关系
无	此时，补丁文件存储在设备的存储介质中，但文件中的补丁还没有被加载到内存补丁区中。	当用户将补丁从存储介质中加载到内存补丁区后，补丁的状态将被设置为运行（running）。
运行（running）	当补丁被存储在内存补丁区中，且被永久运行时，补丁就处于运行（running）状态。当单板被复位后，此单板上在复位前处于运行（running）状态的补丁将保持运行（running）状态。	用户可以卸载处于运行（running）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



9.1.4 CPU 和内存占用率告警阈值

用户可以通过配置 CPU 和内存占用率告警阈值，监控 CPU 和内存的使用情况，及时了解系统运行的性能。

- CPU 占用率超出告警阈值时，记录日志信息

  适当设置 CPU 占用率的告警阈值，在超过阈值时，系统发出告警，记录日志信息，便于用户了解 CPU 的使用情况。
- 内存占用率超出告警阈值时，记录日志信息

  适当设置内存的占用率的告警阈值，在超过阈值时，系统发出告警，记录日志信息，便于用户了解内存的使用情况。

9.1.5 重新启动设备

用户可以根据需要定时重启或者立即重启设备，实现对设备的维护。

在某些特殊情况下，例如系统升级，需要重新启动路由器使配置生效。

除了断电重启外，AR3200 还提供两种通过命令行重启路由器的方式：

- 立即重启
- 定时重启

9.2 激活 GTL License 文件

GTL（Global Trotter License） License 文件是华为公司提供给用户对设备的容量、功能和期限等进行授权的授权文件。

9.2.1 建立配置任务

激活 GTL License 文件分为以下两种情况：一种是新购买设备的用户需要同时申请购买 GTL License 文件，获取相应的业务模块授权。另一种是如果设备上存在已经激活的 GTL License 文件，但 GTL License 文件使用期限已到，用户需要重新申请、升级、激活 GTL License 文件,否则造成业务中断。

应用环境

- 首次激活 GTL

新购买设备的用户需要同时申请购买 GTL License 文件，获取相应的业务模块授权。在设备上激活 GTL License 文件，实现对相应业务模块的应用。

- 升级激活 GTL

  设备上存在已经激活的 GTL License 文件，但 GTL License 文件使用期限已到，用户需要重新申请、升级、激活 GTL License 文件。否则，GTL License 文件在超过使用期限后会失效，造成各功能模块关闭，业务中断。

  确认 GTL License 升级操作前，需要确认是否要申请新的 GTL License 文件。如果用户要更新的 GTL License 文件授权值小于当前 GTL License 文件的授权值，在激活后会返回交互信息，提示用户在需要更新的授权值小于当前 GTL License 文件的授权值的情况下是否选择激活。

  - 如果选择是，会提示用户升级成功。
  - 如果选择否，会提示更新 GTL License 文件失败，同时返回当前 GTL License 状态。

执行激活 GTL License 文件操作之前，用户需要确认 GTL License 文件后缀为“.dat”。获得 GTL License 后，请先查看设备主控板 ESN 序列号是否和获得的 GTL License 一致。直接用“记事本”程序即可打开 GTL License 文件进行查看。

说明

GTL License 文件后缀为“.dat”。

GTL License 文件分为 COMM 和 DEMO 两个版本，具体区别如下：

版本	运行截止日期	保留天数
COMM	按照合同规定	按照产品定义，一般不超过 90 天，最长不超过 180 天
DEMO	按照产品定义，一般不超过 60 天	按照产品定义，一般不超过 60 天 可以通过 **display license state** 命令查看 DEMO 版本 License 文件剩余的有效时间。

在保留天数期间系统每天会有告警提示。如果想继续使用，需要从公司正规渠道重新获取 GTL License 文件。

说明

保留天数是指 GTL License 运行截止日期后，用户可以继续使用的天数。

前置任务

在激活 GTL License 文件之前，需要完成以下任务：

- 申请获取 GTL License 文件

数据准备

在激活 GTL License 文件之前，需要准备好以下数据。

序号	数据
1	GTL License 文件名称

9.2.2 上传 GTL License 文件

申请 GTL License 文件后，上传该文件到设备的存储介质中才能进行激活。

背景信息

上传 GTL License 文件之前，可以执行命令 **dir** 查看设备中存储介质的占用情况。请确保存储介质有足够的存储空间存放 GTL License 文件。

操作步骤

步骤 1 执行命令 **dir** *device-name*，查看 license 文件是否存在。

AR 上 License 文件为*.dat 文件，请存放于 Flash，SD 卡和 U 盘的根目录下。

说明

对于升级激活 GTL License 文件的用户，需要先执行命令 **license revoke** 获得 GTL License 失效码。通过 GTL License 失效码向华为公司申请新的 GTL License 文件，再将 GTL License 文件上传到存储设备中，获取相应的业务模块授权。

----结束

9.2.3 配置激活 GTL License 文件

通过激活 GTL License 文件，获取相应的授权，实现设备上对应业务模块应用权限。

操作步骤

- 首次激活 GTL License 文件
  1. 执行命令 **license active** *file-name*，激活 GTL License 文件，获取相应授权。

     说明

     对于首次激活 GTL License 文件的用户，需要向华为公司申请购买 GTL License 文件。
- 升级激活 GTL License 文件
  1. 执行命令 **license revoke**，获得 GTL License 失效码。

     说明

     使用 GTL License 失效码向华为公司申请新的 GTL License 文件。
  2. 执行命令 **license active** *file-name*，激活 GTL License 文件，获取相应授权。

----结束

9.2.4 （可选）使能 license 模块的 Emergency 状态

使能 Emergency 状态会启用当前 license 文件内有资源项特性模块的最大规格。

背景信息

在路由器上进行如下配置，且需要保证当前设备处于以下场景之一：

- 已激活过 Comm 版本的 license 文件，状态为 Normal。
- 已激活过 Demo 版本的 license 文件，状态为 Demo。
- 在 Emergency 状态的最后一天启用下一次 Emergency 状态操作。

操作步骤

步骤 1 执行命令 **license emergency**，使能 license 模块的 Emergency 状态。

说明

使能 Emergency 状态后要注意以下事项：

- Emergency 状态不允许手动取消。
- Emergency 状态只能启用 3 次，每次可以保持 7 天 Emergency 状态。
- Emergency 状态只能在前一次的最后一天才可以进行启动下一次操作。

----结束

9.2.5 检查配置结果

激活 GTL License 文件后，可以查看到主备板的 GTL License 文件信息。

前提条件

已完成激活 GTL License 文件的所有配置。

操作步骤

- 使用 **display license** 命令显示主备板的 GTL License 文件信息。
- 使用 **display license state** 命令显示 License 的类型。

----结束

任务示例

```
<Huawei> display license
 Active License on master board: flash:/LIC_ON77076_A6D2CE1AEC3_AR.dat

 Active license    : flash:/LIC_ON77076_A6D2CE1AEC3_AR.dat
 License state     : Demo
 Revoke ticket     : No ticket

 Product name      : AR
 Product version   : V200R002
 License file ESN  : AR00050123456789,AR00060123456789,AR00070123456789,AR000801
23456789
 License Serial No : LIC20110309010210
 Creator           : Huawei Technologies Co., Ltd.
 Created Time      : 2011-03-09 19:36:14
 Country           : China
 Custom            : R&D of Huawei Technologies Co., Ltd.
 Office            : Shenzhen

 Feature name      : ACCESS
 Authorize type    : DEMO
 Expired date      : 2011-06-07
 Trial days        : 60
```

```
Item name          : LLE0IPPBX01
Item type          : Function
Control value      : 1
Used value         : 1
Item state         : Normal
Item expired date  : 2011-06-07
Item trial days    : 60
Description        : LLE0IPPBX01
```

9.3 升级系统软件

升级设备软件可以实现设备原有性能的优化、新性能的增加以及解决当前运行版本更新不及时的问题。

9.3.1 建立配置任务

当设备在运行过程中，基于用户需求可能会出现需要增加新特性、优化原有特性的情况，此时，需要对设备软件的当前运行版本进行升级，从而满足用户需求。

应用环境

在执行本任务时，用户可以根据需要选择需要升级的资源文件。

说明

在对设备进行升级之前，需要注意以下事项：

- 从华为公司正规渠道取得所要升级的新版本系统软件和 GTL License 文件以及相应的版本配套文档。
- 因为设备软件不同版本间存在差异，所以设备升级请以华为公司发布的正式升级指导书为准。
- 打开日志功能，记录整个升级过程中所有的操作，以便出现升级失败后，进行故障的分析和定位。
- 如果由于资源文件配置错误而造成设备重启，设备在重启后会自动将资源文件回退到以前的版本。

前置任务

在升级资源文件之前，需完成以下任务：

- 确保待升级的路由器正常工作，并成功登录。

数据准备

在配置升级系统软件之前，需准备以下数据。

序号	数据
1	串行接口的波特率
2	FTP 服务器的 IP 地址或路由器的 IP 地址
3	FTP 登录的用户名和密码
4	（可选）新版本的系统软件、配置文件、License 文件和补丁包文件

9.3.2 升级前检查

为保证设备的顺利升级，需要严格按照要求进行升级前的准备工作。

操作步骤

步骤 1 用户根据需要进行相关硬件准备，如清理设备内存空间，用于存放新的版本配套文档等。

步骤 2 确认是否需要申请新的 GTL License 文件，如果需要，请从华为公司正规渠道获取。

说明

- 升级到新的 R 版本或 V 版本时需要申请新的 GTL License 文件。
- 保证获取到的新 GTL License 文件与系统中的软件大包配套。

如果需要查找 GTL License 文件所对应的特性，首先用文本编辑器打开相应的 GTL License 文件，文件中 Resource 字段和 Function 字段所对应的内容分别是该文件控制的资源项和功能项。

步骤 3 获取所需的升级软件。从华为公司正规渠道获取所要升级的新版本系统软件（*.cc）以及相应的版本配套文档。

步骤 4 在用户视图下，执行命令 **display version**，查看设备当前运行的软件版本。如果版本一致或优于待升级版本则不用升级。

步骤 5 通过一系列的命令检查设备的运行状态：

在用户视图下，执行命令 **display memory-usage**，查看设备主控板内存使用率，从而保证主控板工作正常。

在用户视图下，执行命令 **display health**，记录下显示信息，若在升级过程中出现无法定位的问题，请将这些信息发送给华为公司技术支持工程师进行故障定位。

步骤 6 搭建可通过 TFTP 或 FTP 协议升级的环境，便于备份升级前的原资源文件和上传升级所需的新资源文件。

通过 FTP 协议升级时：

- 如果待升级设备作为客户端，PC 作服务器端，用户需在自己的 PC 上先安装 FTP Server 应用程序。FTP Server 应用程序由用户自己购买、安装，待升级设备不附带此软件。
- 如果待升级设备作为服务器端（待升级设备提供 FTP Server 功能），PC 作客户端，用户不需要安装 FTP Server 应用程序。缺省情况下待升级设备的 FTP 功能是关闭的，需要在系统视图下执行 **ftp server enable** 命令使能 FTP Server 功能。

通过 TFTP 协议升级时，由于待升级设备只能做为客户端不能提供 TFTP Server 功能，因此用户必须在 PC 上先安装 TFTP Server 应用程序。

步骤 7 备份待升级设备存储介质中的重要数据。

步骤 8 检查待升级设备存储介质中的剩余空间,保证有足够的空间存放待上传升级的软件文件及配套的文档。

----结束

9.3.3 下载系统文件

背景信息

本节将介绍 AR3200 作为 FTP 服务器、FTP 客户端、TFTP 客户端和通过 BootROM 菜单下载系统文件至 AR3200。

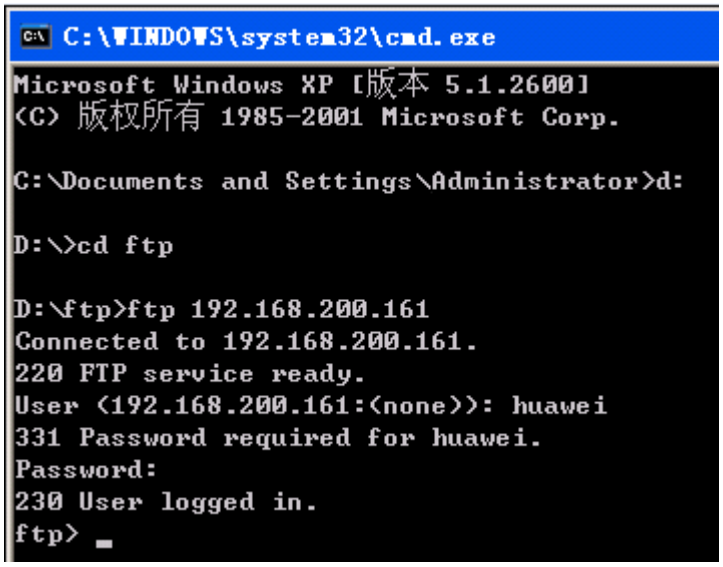
操作步骤

- **配置 AR3200 作为 FTP 服务器，PC 作为客户端将系统文件上传到 AR3200**

  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **ftp server enable**，启动 FTP 服务器。
  3. 执行命令 **aaa**，进入 AAA 视图。
  4. 执行命令 **local-user** *user-name* **password** *password*，配置本地用户名和密码。
  5. 执行命令 **local-user** *user-name* **service-type ftp**，配置本地用户的服务类型为 FTP。
  6. 执行命令 **local-user** *user-name* **ftp-directory** *directory*，配置 FTP 用户的授权目录。
  7. 在 PC 上进入 Windows 的命令行提示符（此处以 Windows 操作系统为例）。
  8. 进入指定的路径，并将系统文件放入其中，如 D:\ftp。
  9. 执行 Windows 命令 **ftp** *ip-address*，通过 FTP 方式登录路由器。

     根据提示输入之前设置的用户名和口令，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。如图 9-2 所示。

     图 9-2 从 PC 端登录 FTP 服务器

  10. 执行命令 **binary** 设置文件传输方式为二进制模式。

说明

FTP 支持 ASCII 码、二进制文件类型。二者的区别是：

- ASCII 传输使用 ASCII 字符，并由回车键和换行符分开。
- 二进制不用转换或格式化就可传字符。

FTP 传输模式由客户端进行选择，系统默认 ASCII 方式。客户端可使用模式切换命令进行切换（ASCII 和 Binary）。传输文本文件使用 ASCII 方式，传输二进制文件使用 Binary 方式，此处建议使用 Binary 方式。

11. 执行命令 **put** *remote-filename* [*local-filename*]从 PC 端将系统文件上传到路由器。
12. 在路由器上执行命令 **dir**，可查看当前存储目录下是否存在该系统文件。

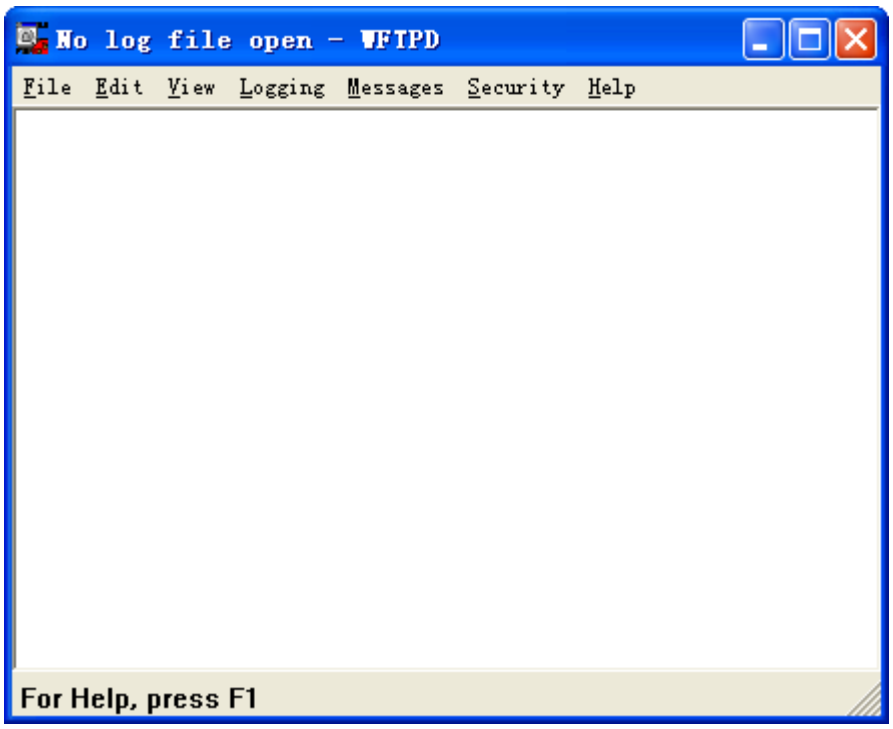
说明

如果路由器存储目录下的系统文件与 PC 端的大小不一致，可能是在传输过程中出现异常，请重新传输。

- **配置 AR3200 作为 FTP 客户端，PC 作为服务器将系统文件上传到 AR3200**

1. 在 PC 上运行 FTP Server 程序（以 wftpd32 为例介绍），如图 9-3 所示。

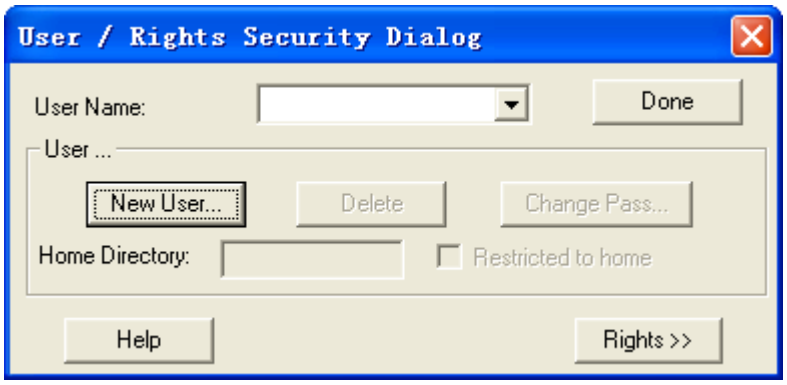
图 9-3 PC 端运行 FTP Server 程序



2. 在菜单栏中选择“Security” ->“Uers/rights”配置用户名、密码和 PC 上 FTP 的工作目录，如图 9-4 所示。

   在弹出的对话框中单击“New User…”设置好用户名和密码，如用户名为 AR，密码为 123456。在“Home Directory:”处设置 PC 上 FTP 的工作目录，如 D:\ftp，并将系统文件放入此路径下，然后单击“Done”按钮关闭对话框。

图 9-4 配置 FTP 用户



3. 在路由器上执行命令 **ftp** *host* [*port-number*]，登录 PC 端。

   说明

   登录 FTP Server 端前，确保路由器当前存储目录有足够的空间用于存放系统文件。登录时需输入之前设置的用户名和密码。

4. 执行命令 **binary** 设置文件传输方式为二进制模式。
5. 执行命令 **get** *remote-filename* [*local-filename*]从 FTP Server 端下载系统文件。
6. 系统文件下载成功后，执行命令 **bye** 或 **quit**，终止与服务器的连接，并退回到用户视图。
7. 执行命令 **dir**，可查看路由器当前存储目录下是否存在该系统文件。

   说明

   如果路由器存储目录下的系统文件与 PC 端的大小不一致，可能是在传输过程中出现异常，请重新传输。

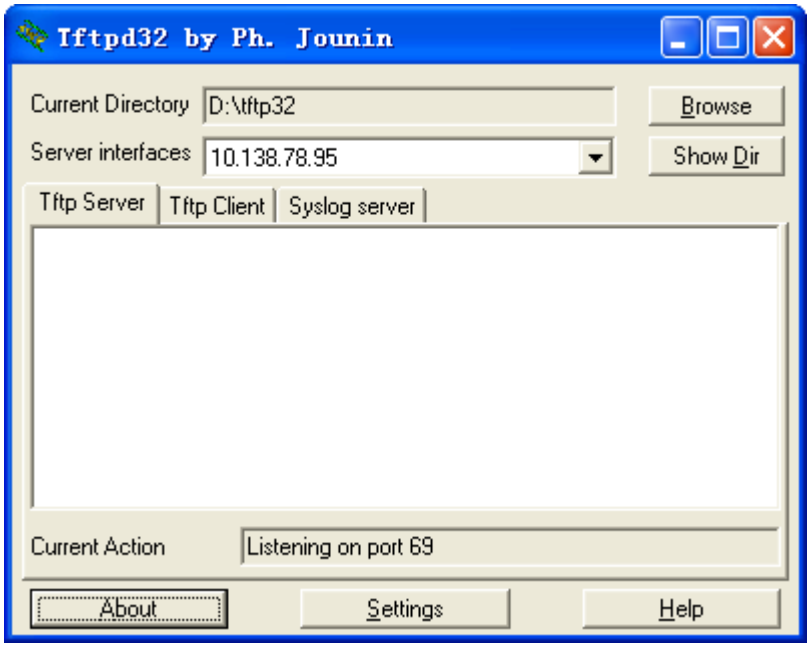
- **配置 AR3200 作为 TFTP 客户端，PC 作为服务器将系统文件上传到路由器**

  说明

  目前 AR3200 只支持作为 TFTP 客户端。

  1. 在 PC 上运行 TFTP Server 程序（以 TFTP32 为例介绍），如图 9-5 所示。

图 9-5 PC 端运行 TFTP Server 程序



2. 工作目录（“Current Directory”）设置为系统软件备份到的路径，可单击“Browse”来更改，并将系统文件放入相应路径；服务器接口（“Server interface”）处填写 TFTP 服务器的 IP 地址，一般系统会自动填上当前 PC 的 IP 地址。
3. 在路由器上执行命令 **tftp** *tftp-server* **get** *source-filename* [*destination-filename*]从 PC 端下载系统文件。

   说明

   下载前请确保路由器当前存储目录有足够的空间存放系统文件。
4. 执行命令 **dir**，可查看路由器当前存储目录下是否存在该系统文件。

   说明

   如果路由器存储目录下的系统文件与 PC 端的大小不一致，可能是在传输过程中出现异常，请重新传输。

- **通过 BootROM 菜单下载系统文件至 AR3200**

  说明

  - 通过启动菜单升级软件的过程比较复杂，一般不建议使用此方法，只有路由器程序无法启动的时候才需要使用启动菜单升级系统软件。
  - 需将路由器的管理网口与 PC 端相连。
  - AR150 系列的管理网口为 Ethernet0/0/3，AR200 系列的管理网口为 Ethernet0/0/6，AR1200 系列的管理网口为 GigabitEthernet0/0/0，AR2200 的管理网口为 GigabitEthernet0/0/0，AR2240 的管理网口为 GigabitEthernet0/0/2，AR3200 系列的管理网口为 GigabitEthernet0/0/2。

  1. 在配置终端或 PC 运行 FTP Server 程序（以 wftpd32 为例），指定系统文件所在的路径并创建 FTP 用户和密码，可参见**配置 AR3200 作为 FTP 客户端，PC 作为服务器将系统文件上传到 AR3200 中的步骤 2**。
  2. 通过 Console 口登录路由器，具体请参见**通过 Console 口登录路由器**。
  3. 重启路由器，在路由器出现以下提示信息时按 Ctrl_B，进入 BootROM 菜单。

```
Sep 16 2011,17:14:28
Copying Data : Done
Uncompressing : Done
Initializing SMI Bus:OK
Init flash, please wait......
Base Address: 0xfffffffffc000000
Size is: 0x200000000K
flash drv init.
Initializing FlashPiece Module:
FlashPiece start offset at: 0x300000
FlashPiece size is: 0x100000
Initializing FlashDynamic Module:
FlashDynamic start offset at: 0x400000
FlashDynamic size is: 0x200000
Initializing I2C Bus:OK
USB2 Host Stack Initialized.
USB Hub Driver Initialized
USBD  Wind River Systems, Inc
EHCI Controller found.
Waiting to attach to USBD...0xbfffdf0 (tRootTask): usb1_base = 0xbff22000Done.
0xbfffdf0 (tRootTask): usbBulkDevInit() returned OK


Press Ctrl+B to break auto startup ... Attached TCP/IP interface to teth1.
```

说明

- 按下 Ctrl_B 后，用户需要输入初始密码 huawei 才可以进入 BootROM 菜单。

4. 进入 BootROM 菜单后，选择第 3 项，进入网络子菜单。

```
Enter Password:

        Main Menu

    1. Default Startup
    2. Serial Menu
    3. Network Menu
    4. Startup Select
    5. File Manager
    6. Reboot

Enter your choice(1-6):3
```

5. 进入网络子菜单后，选择第 2 项，修改属性。

```
NetWork Menu

    1. Display parameter
    2. Modify parameter
    3. Save parameter
    4. Download file
    0. Return
Enter your choice(1-10): 2
```

根据实际情况配置 ftp 类型、系统文件名称、管理网口的 IP 地址、ftp 服务器的 IP 地址、ftp 的用户名和密码等参数。

```
NOTE:
Ftp type define:  0(ftp), 1(tftp),
ENTER = no change; '.' = clear;

Ftp type            : 0
File name           : ar.cc
Ethernet ip address : 192.168.200.174
Ethernet ip mask    : ffffff00
Gateway ip address  :
Ftp host ip address : 192.168.200.1
Ftp user            : ar
Ftp password        : ar
```

6. 完成属性配置后，自动返回至网络子菜单，选择第 4 项，从 PC 端下载系统文件。

```
NetWork Menu

    1. Display parameter
    2. Modify parameter
    3. Save parameter
    4. Download file
    0. Return
Enter your choice(1-10): 4
```

7. 选择系统文件下载存放的位置。

```
Download file to: [ 1:flash 2:usb0 3:sd0 4:sd1 ]:
```

输入数字选择对应的存储介质，例如；输入 **4** 表示存入 sd1 存储介质中。

说明

sd1 为设备内置的 SD 存储卡，sd1 和 flash 为设备固有的存储介质，其他的存储介质例如 U 盘，只有当用户安装以后才会显示。

8. 系统文件下载成功后，重新启动路由器即可。

----结束

9.3.4 指定下次启动文件

指定路由器下次启动时使用的系统软件之后，必须清除下次启动后的补丁状态文件。

背景信息

在指定下次启动文件之前，需要完成以下操作：

上传系统软件到设备主控板，具体步骤请参见**用户使用 FTP 命令进行文件操作**中上传或下载文件部分。

上传系统软件之前，请确保主控板的存储介质有足够的存储空间存放系统软件。

说明

务必通过文件大小、日期的对比等来检查上传文件的正确性。

请在待升级的路由器上进行如下配置。

操作步骤

步骤 1 在用户视图下执行命令 **startup system-software** *system-file* [**verify**]，为主控板指定下次启动后的系统软件。

步骤 2 （可选）当升级的系统文件需要同时启动补丁包文件时，可以执行以下操作：

- 执行 **startup patch** *file-name* 命令，为主控板指定下次启动后的补丁包文件。

步骤 3 （可选）执行 **startup saved-configuration** *configuration-file* 命令，为主控板指定下次启动后的配置文件。

----结束

9.3.5 配置备份启动文件

设置一个系统备份启动软件包，确保系统在出现故障的情况下能重新正常启动。

背景信息

当前启动软件包所在的存储介质出现损坏时，将导致系统无法正常启动，可调用备份系统软件包进行启动。

说明

- 系统软件包必须以“.cc”作为扩展名，且必须存储在根目录中。
- 备份的启动软件包可以和当前的启动软件包完全相同，也可以是不同的版本文件，但前提是该软件包一定能保证系统正常启动。

请在路由器上进行如下配置。

操作步骤

步骤 1 在用户视图下执行命令 **startup system-software** *filename* **backup**，指定备份的系统软件包。

----结束

9.3.6 （可选）升级接口板 BootROM

系统软件升级后，2FE 和 1GEC 单板需要手工执行升级 BootROM 操作。

背景信息

说明

执行 **diaplay device** 命令可以查看设备是否存在注册成功的 2FE 和 1GEC 单板。

操作步骤

步骤 1 执行命令 **upgrade slot** *slot-id* **startup bootrom**，升级接口板的 BootROM。

步骤 2 执行命令 **reset slot** *slot-id* 命令复位接口板。

复位单板后，可以执行 **display version slot** *slot-id* 检查 BootROM 升级是否成功，出现单板对应槽位的显示信息说明 BootROM 加载成功。

----结束

9.3.7 重启设备

在设备升级过程中，对系统中软件和文件进行更改后需要重启设备，使得新的软件和文件及时生效，同时也能快速验证更改操作是否正确。

背景信息

在设备升级过程中，出现以下情况时，需要用户重启设备：

- 在线指定下次启动时加载的系统软件、配置文件之后，需要用户重启设备。

注意

在重启路由器之前，请先执行 **save** 命令保存当前配置文件。

设备重启后，先以设置的下次启动软件包进行重启，如果用于下次启动的软件包被破坏，则以系统备份软件包启动。如果仍然失败，设备将在存储设备上搜索合法的软件包启动（搜索顺序：flash→SD 卡→U 盘）,如果某一存储设备存在多个合法的软件包则选用找到的第一个进行启动。如果设备存储介质内存在合法的系统软件包和配置文件，设备将在 24 分钟内找到一个回退版本并正常启动；否则系统将停止在 BOOT 菜单。

操作步骤

- 在用户视图下，执行命令 **reboot [fast]**，实现对设备的重新启动。

----结束

9.3.8 检查配置结果

升级系统软件配置成功后，可以查看到接口的参数信息和资源文件版本一致情况等内容。

前提条件

已完成升级系统软件的所有配置。

操作步骤

- 使用 **display patch-information** 命令查看当前所有的补丁信息。
- 执行命令 **display startup**，在显示内容中查看“Startup system software”和“Startup saved-configuration file”字段所对应的文件名称，与用户所需启动的文件名称进行比对。

----结束

任务示例

安装补丁后，执行 **display patch-information** 命令，可以看到补丁包中的补丁单元在各个单板上的状态。

```
<Huawei> display patch-information
Patch version    :    ARV200R002C00SPH100
Patch packet name:    sd1:/patch_lic2.pat
```

执行命令 **display startup**，可以查看启动的系统软件和配置文件名称。例如：

```
<Huawei> display startup
MainBoard:
  Startup system software:                  sd1:/ar0215_31345_3220.cc
  Next startup system software:             sd1:/ar0215_31345_3220.cc
  Backup system software for next startup:  null
  Startup saved-configuration file:         sd1:/iascfg.zip
  Next startup saved-configuration file:    sd1:/iascfg.zip
  Startup license file:                     null
  Next startup license file:                null
  Startup patch package:                    null
  Next startup patch package:               null
  Startup voice-files:                      null
  Next startup voice-files:                 null
```

9.4 管理补丁

介绍补丁的几种使用方法。通过安装补丁可以在不中断业务的情况下，实现系统升级。通过指定下次启动的补丁文件可以为系统指定下次启动后执行的补丁文件。通过卸载补丁可以去激活不符合系统要求的补丁，或者删除系统不需要的补丁文件，从而释放设备主控板补丁区的内存空间。

9.4.1 建立配置任务

当需要弥补系统漏洞或缺陷时，可以对系统进行安装补丁操作。通过安装补丁可以在不中断业务的情况下，实现系统升级。

应用环境

在安装补丁时，系统会同时为主控板和接口板安装补丁。

为系统安装补丁文件可以实现对设备系统软件的动态在线升级，用户可以选择以下两种方式：

- 立即安装补丁文件，补丁文件生效的时间是在执行命令后，此时补丁文件立即进入运行态而不用重启设备，详见安装补丁。
- 指定下次启动的补丁文件，补丁文件生效时间是在设备重启之后。

前置任务

在管理补丁之前，需完成以下任务：

- 确保路由器正常工作。
- 补丁存储在路由器的存储设备中。

数据准备

在为系统管理补丁之前，需准备以下数据。

序号	数据
1	补丁包文件

9.4.2 安装补丁

用户可以在用户视图下执行加载补丁和运行补丁的操作，从而实现对设备的适应性和排错性修改，优化系统性能。

背景信息

由于同一时刻系统中只能有一个补丁文件在运行，所以在安装补丁前需要执行命令 **display patch-information** 检查当前所有的补丁信息，包括运行的补丁文件。如果信息中显示有正在运行的补丁文件，请执行删除补丁操作进行补丁文件的卸载删除。

用户在进行加载补丁的操作之前，还需要先完成以下操作：

- 上传补丁包到主用主控板，具体步骤参考用户使用 FTP 命令进行文件操作中上传或下载文件部分。

操作步骤

步骤 1 进入用户视图。

步骤 2 执行命令 **patch load** *patchname* **all run**，为系统激活补丁。

说明

- **patch load** *patchname* **all run** 命令只能激活单个补丁包。
- 补丁包要求增量发布，如果系统中已经运行了补丁 patchA.pat，用户激活了增量的补丁 patchB.pat 后，基于某些原因需要再运行补丁 pachA.pat 时，需要先执行 **patch delete all** 命令删除补丁后，再重新加载激活补丁 patchA.pat 或者通过 **startup patch** 命令设置 patchA.pat 为下次启动的补丁，通过复位系统使得 patchA.pat 生效。

----结束

9.4.3 指定下次启动的补丁

用户在上传补丁文件到存储介质后，如果不需要立即生效，可通过指定下次启动的补丁文件使补丁文件在设备重启后生效，实现对系统软件的优化。

背景信息

在指定下次启动后的补丁文件之前，需完成以下任务：

- 上传所要指定的补丁文件到主用主控板的存储介质中，具体操作步骤详见用户使用 FTP 命令进行文件操作中上传或下载文件部分。

操作步骤

步骤 1 在用户视图下，执行命令 **startup patch** *file-name*，为所有主控板指定下次启动后的补丁文件，文件格式为*.pat。

----结束

后续处理

指定下次启动的补丁文件后，可以执行命令 **display startup**，查看主控板“Next startup patch package”字段所对应的文件名称。

9.4.4 卸载补丁

如果补丁未能满足系统要求，或者需要内存补丁去的存储空间时，用户可以在用户视图下执行卸载补丁的操作。

背景信息

在为系统安装补丁的过程中，因为系统中只允许一个补丁文件在运行，所以如果需要加载一个新的补丁文件，然后在系统中运行新加载的补丁文件，那么此时需要删除存在于补丁内存区中处于运行态的补丁文件。

操作步骤

步骤 1 执行命令 **patch delete all**，删除系统中所有的补丁。

----结束

后续处理

对补丁文件执行删除操作后，可以按以下指导检查配置结果。

- 执行命令 **display patch-information**，查看补丁状态。

对补丁进行删除操作后，执行命令 **display patch-information**，查看系统的补丁信息。

```
<Huawei> display patch-information
 Info: No patch in the system
```

9.4.5 检查配置结果

安装补丁配置成功后，可以查看到补丁信息和补丁状态等内容。

前提条件

已完成安装补丁的所有配置。

操作步骤

- 使用 **display patch-information** 命令查看当前所有的补丁信息。

----结束

任务示例

安装补丁后，执行 **display patch-information** 命令，可以看到补丁包中的补丁单元在各个单板上的状态。

```
<Huawei> display patch-information
Patch version    :    ARV200R002C00SPH100
Patch packet name:    sd1:/patch_lic2.pat
```

9.5 监控 CPU 和内存的占用率

通过对 CPU 和内存占用率进行告警阈值配置，可以监控 CPU 和内存的使用情况，及时了解系统运行的性能。

9.5.1 建立配置任务

在进行 CPU 和内存占用率告警阈值的配置前了解此特性的应用环境、配置此特性的前置任务和数据准备，有助于快速、准确地完成配置任务。

应用环境

CPU 和内存是设备的核心部分，当系统中存在如大量路由信息、快速路由算法等配置时，均会占用大量 CPU 资源，这将会极大影响系统的性能，造成数据处理不及时、高丢包率、或死机等状况。这些将会给运营商客户带来无法预计的损失。

在路由器处理数据的过程中，如果能够对 CPU 和内存出现高占用率的情况及时告警，可以更有效地监控 CPU 和内存的使用情况，优化系统性能，以保证系统一直处于良性运作。

前置任务

在监控 CPU 和内存占用率之前，需完成以下任务：

- 确保路由器正常工作。

数据准备

在监控 CPU 和内存占用率之前，需要准备以下数据。

序号	数据
1	CPU 占用率监控告警开始阈值和恢复阈值
2	内存占用率的告警阈值

9.5.2 配置 CPU 占用率告警阈值

配置 CPU 占用率告警阈值，实现对 CPU 使用情况的监控。

背景信息

本配置步骤中涉及告警开始阈值和告警恢复阈值两个概念。

- 告警开始阈值：当 CPU 占用率达到该阈值时，系统发出告警。
- 告警恢复阈值：当 CPU 占用率低于该阈值时，系统告警消除。

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 **set cpu-usage threshold** *threshold-value* [**restore** *restore-threshold-value*] [**slot** *slot-id*]，配置主控板或者指定槽号的接口板的 CPU 占用率监控告警开始阈值和监控告警恢复阈值。

说明

缺省情况下:

CPU 占用率的监控告警开始阈值是 80%，监控告警恢复阈值是 75%。

当 CPU 占用率告警门限值小于 60%时，监控告警恢复阈值的默认值为告警门限值减 1%。

当 CPU 占用率告警门限值大于等于 60%时，监控告警恢复阈值的默认值为告警门限值减 5%。

----结束

9.5.3 配置内存占用率告警阈值

配置内存占用率告警阈值，实现对内存使用情况的监控。

背景信息

本配置步骤中涉及告警开始阈值和告警恢复阈值两个概念。

- 告警开始阈值：当内存占用率达到该阈值时，系统发出告警。
- 告警恢复阈值：当内存占用率低于该阈值时，系统告警消除。

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 **set memory-usage threshold** *threshold-value*，配置内存占用率告警阈值。

缺省情况下：

- 接口板的内存容量在小于等于 128MB 时，内存占用率的告警阈值是 90%；
- 接口板的内存容量在 128MB ～ 256MB 时，内存占用率的告警阈值是 95%；
- 接口板的内存容量在 256MB ～ 512MB 时，内存占用率的告警阈值是 95%；
- 接口板的内存容量大于 512MB 时，内存的占用率的告警阈值是 95%。

----结束

9.5.4 检查配置结果

CPU 和内存占用率阈值配置成功后，可以查看到 CPU 和内存占用率告警阈值的配置信息。

前提条件

已完成 CPU 和内存占用率阈值的所有配置。

操作步骤

- 使用 **display cpu-usage configuration** [**slot** *slot-id*]命令，查看 CPU 的占用率。
- 使用 **display memory-usage threshold** 命令，查看内存的占用率。

----结束

任务示例

```
# 查看当前主控板的CPU占用率信息。CPU的占用率主要体现在显示信息的CPU列。
<Huawei> display cpu-usage
CPU Usage Stat. Cycle: 60 (Second)
CPU Usage            : 0% Max: 100%
CPU Usage Stat. Time : 2011-01-30  15:41:37
CPU utilization for five seconds: 0%: one minute: 0%: five minutes: 0%.

TaskName        CPU  Runtime(CPU Tick High/Tick Low)  Task Explanation
BOX              0%         0/  7097de       BOX Output
_TIL             0%         0/       0       Infinite loop event task
VCLK             0%         0/  d90e00
TICK             0%         0/ 38b72ad
co0              0%         0/  1e677b       co0 Line user's task
TAD              0%         0/       0       TAD Transmission Alarm Damping
RTMR             0%         0/ 18a307e       RTMR
IPCQ             0%         0/ 1c181c4       IPCQIPC task for single queue
IPCK             0%         0/       0       IPCKIPC task for ack message
VP               0%         0/   38700       VP  Virtual path task
IPCW             0%         0/   1a167       IPCWIPC task of WVRP
```

VPWV	0%	0/ 19540d	VPWVP task of WVRP
RPCQ	0%	0/ 1540dc	RPCQRemote procedure call
VFS	0%	0/ 0	VFS Virtual file system
VMON	0%	0/ 59002	VMONSystem monitor
HACK	0%	0/ 0	HACKtask for HA ACK
MTP	0%	0/ 0	MTP
STND	0%	0/ 5de440	STNDStandby task
CFA	0%	0/ 28c9fa	CFA Configuration agent
INFO	0%	0/ e7e7	INFOInformation center
SAPP	0%	0/ 39569	SAPP
NQAC	0%	0/ 0	NQAC
NQAS	0%	0/ 0	NQAS
VOAM	0%	0/ 0	VOAM
MINM	0%	0/ 532c94	MINMMac in Mac
APS	0%	0/ 570eda	APS Automatic Protection Switch
ISC6	0%	0/ 0	ISC6
FIB6	0%	0/ 0	FIB6IPv6 FIB
BFD	0%	0/ 8557f7	BFD Bidirection Forwarding Detect
TNLM	0%	0/ 16dc594	TNLM
OAM	0%	0/ 7e0fb2	OAM OAM
LSPA	0%	0/ 0	LSPA
L2V	0%	0/ 12eb43	L2V
SNPG	0%	0/ 552703	SNPG
CCTL	0%	0/ 0	CCTLBulk stat connect control
TCTL	0%	0/ 0	TCTLBulk stat transmit control
NAP	0%	0/ 0	NAP
PM	0%	0/ e509c	PM
PMF	0%	0/ 0	PMF
EOAM	0%	0/ 6c0c8	EOAMEthernet OAM 802.1ag
1731	0%	0/ bbbaf	1731Ethernet OAM Y1731
TRAF	0%	0/ 0	TRAFTraffic Statistics
SLAG	0%	0/ 0	SLAG
ITSK	0%	0/ 176169	ITSKIPOS common task
CDM	0%	0/ 9d3ca	CDM
CSBR	0%	0/ 0	CSBRCompare slave buildrun-info
NFPT	0%	0/ aab1f	NFPTNFP timer task
SOCK	0%	0/ 61e702	SOCKPacket schedule and process
VTRU	0%	0/ 0	VTRUNK
FIB	0%	0/ 0	FIB Forward Information Base
MFIB	0%	0/ 22b68	MFIBMulticast forward info
IFNT	0%	0/ 0	IFNTIfnet task
U 0	0%	0/ 0	U 0 user command process task
PDTT	0%	0/ 0	PDTTPDT timer task
VTYD	0%	0/ 180a11	VTYDVirtual terminal
RSA	0%	0/ 0	RSA RSA public-key algorithms
GRSA	0%	0/ 0	GRSA
AGNT	0%	0/ 0	AGNTSNMP agent task
TRAP	0%	0/ ec52e5	TRAPSNMP trap task
AGT6	0%	0/ 0	AGT6SNMP AGT6 task
FMAT	0%	0/ 262b90	FMATFault Manage task
MDMT	0%	0/ e825a5	MDMTModem task
NTPT	0%	0/ 1b3d998	NTPTNetwork time protocol task
CFM	0%	0/ 0	CFM Configuration file management
HS2M	0%	0/ 0	HS2MHigh available task
ISSU	0%	0/ 0	ISSU
WEBS	0%	0/ add886	WEBSERVER
CMDA	0%	0/ 0	CMDA
MACR	0%	0/ 10c76	MACRO
SNP	0%	0/ 0	SNP DHCP snooping function
AAA	0%	0/ 0	AAA AAA
RDS	0%	0/ 0	RDS RADIUS
TACH	0%	0/ 5d0a21	TACHWTACACS
WEB	0%	0/ 0	WEB WEB Authentication
UCM	0%	0/ bd69	UCM User Connection Management
LAM	0%	0/ 0	LAM Local Accounting Management
GTL	0%	0/ 0	GTL
CPPS	0%	0/ 0	CPPS
ROUT	0%	0/ 1dbd703	ROUTRoute task
LSPM	0%	0/ 1c0a41	LSPMLsp management

```
RSVP            0%          0/       0       RSVP task
LDP             0%          0/  cffb6c       LDP task
CSPF            0%          0/   cd083       CSPF task
GRES            0%          0/       0       GRESM task
GEM             0%          0/       0       GEM
GEM             0%          0/       0       GEM RUN
UTSK            0%          0/       0       UTSK
APP             0%          0/   16649       APP
IP              0%          0/   9ff0c       IP
LINK            0%          0/ 1f0b816       LINK
VRPT            0%          0/   8da6a       VRPT
HOTT            0%          0/       0       HOTT
TNQA            0%          0/   d9e0e       TNQAC
TTNQ            0%          0/       0       TTNQAS
TARP            0%          0/       0       TARPING
TTVP            0%          0/       0       TTVPLS
L2              0%          0/  67387b       L2
VRRP            0%          0/ 25d5a0c       VRRP
L2_P            0%          0/  b18764       L2_PR
ARP             0%          0/       0       ARP
PBBL            0%          0/       0       PBBL
RMON            0%          0/   ab97a       RMONRemote monitoring
OS            100%       20/98434960        Operation System
```

显示当前主控板的 CPU 占用率的配置信息。

```
<Huawei> display cpu-usage configuration
The CPU usage monitor is turned on.
The current monitor cycle is 60 seconds.
The current monitor warning threshold is 80%.
The current monitor restore threshold is 75%.
```

查看当前主控板的内存占用率配置信息。

```
<Huawei> display memory-usage threshold
 Current memory threshold of the main board is 90%.
```

9.6 重新启动设备

当路由器升级系统软件后，需要重新启动路由器使配置生效。或者因为大量临时文件而导致系统瘫痪是，需要重新启动设备。

9.6.1 建立配置任务

在进行重新启动路由器的配置前了解此特性的应用环境、配置此特性的前置任务和数据准备，有助于快速、准确地完成配置任务。

应用环境

当路由器系统软件升级后，需要重新启动路由器使配置生效。或者因为大量临时文件而导致系统瘫痪时，需要重新启动设备。

AR3200 提供两种通过命令行重启路由器的方式：

- 立即重启
- 定时重启

前置任务

在重新启动路由器之前，需要完成以下任务：

- 路由器工作正常

数据准备

在重新启动设备之前，需要准备以下数据。

序号	数据
1	路由器定时重启的时间
2	路由器定时重启的等待时间

9.6.2 配置立即重启设备

用户可以配置立即重启路由器，重启之前需要确认是否需要保存路由器的当前配置文件。

背景信息

注意

一般情况下，建议不要使用 **reboot** 命令，它将导致短时间内业务中断。

操作步骤

- 执行命令 **reboot** [**fast**]，立即重新启动路由器。

----结束

9.6.3 配置定时重启设备

用户可以配置启动路由器定时重启功能，并设定重启的具体时间或者设定重启前的等待时间。

背景信息

请在定时重新启动的路由器上进行下面的配置。

操作步骤

步骤 1 在用户视图下，执行命令 **schedule reboot at** *exact-time*，启动路由器定时重启功能，并设定重启的具体时间。

步骤 2 执行命令 **schedule reboot delay** *interval*，启动路由器定时重启功能，并设定重启前的等待时间。

步骤 1、步骤 2 是并列关系，都可以实现定时重新启动的功能，用户可以根据实际需要选择其中一种步骤。

缺省情况下，禁止路由器定时重启功能。

说明

可通过 **undo schedule reboot** 命令取消定时重新启动功能。

----结束

9.6.4 检查配置结果

重新启动路由器配置成功后，可以查看到路由器定时重启的参数设置等内容。

前提条件

已完成重新启动路由器的所有配置。

操作步骤

- 使用 **display schedule reboot** 命令查看路由器定时重启的参数设置。

----结束

任务示例

查看 00:00 定时重启路由器的配置信息。

```
<Huawei> display schedule reboot
Info:System will reboot at 00:00:00 2009/07/01 (in 12 hours and 33 minutes).
```

查看等待 12 小时后定时重启路由器的配置信息。

```
<Huawei> display schedule reboot
Info:System will reboot at 23:27:14 2009/06/30 (in 11 hours and 59 minutes).
```

9.7 配置举例

配置示例中包括组网需求、配置注意事项和配置思路等。

9.7.1 升级设备软件示例

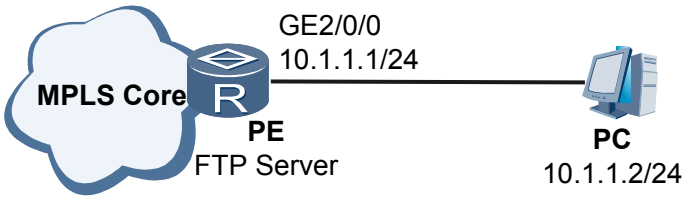
通过介绍设备升级的具体步骤，帮助用户顺利完成系统设备升级。

组网需求

设备当前系统软件版本已经不能满足用户需要，用户需要更大的规格和部署更多的特性，此时用户需要对系统软件进行升级。

如图 9-6 所示，网络中的某设备的软件版本无法满足用户需求需要更新，华为公司提供了系统软件升级的配套软件文件，此时，用户可以为设备进行软件升级。

图 9-6 升级设备软件组网图



配置注意事项

- 备份设备存储介质中的重要数据到 PC 机中。
- 检查设备存储介质中的剩余空间，保证有足够的存储空间来存储新的系统软件。

配置思路

采用以下思路升级设备：

1. 上传新版本的系统软件，本举例中上传文件的方式为 FTP 方式，将设备作为 FTP 服务器，用户名是 user1，密码是 huawei。
2. 指定下次重新启动时使用的系统软件和配置文件。
3. 保存配置文件，重启设备。
4. 检查配置结果。

数据准备

为完成此配置项，需准备如下的数据：

- 确认升级前设备的系统软件版本，本举例中升级前的版本为 V200R001C00.cc。
- 确认要指定的系统软件版本，本举例指定的系统软件版本为 V200R002C00.cc。
- 确认系统备份启动软件包，本举例指定的系统软件版本为 V200R001C00_backup.cc
- 确认设备存储介质中剩余足够的存储空间。

操作步骤

步骤 1 上传新版本系统软件文件。

将设备作为 FTP 服务器。

```
<Huawei> system-view
[Huawei] ftp server enable
Info: Succeeded in starting the FTP server.
[Huawei] aaa
[Huawei-aaa] local-user user1 password huawei
info: A new user added
[Huawei-aaa] local-user user1 service-type ftp
[HuaWei-aaa] local-user user1 ftp-directory sd1:/
[Huawei-aaa] quit
[Huawei] quit
```

上述配置完成后，执行命令 **display local-user** 可以查看配置的用户信息。

```
<Huawei> display local-user
------------------------------------------------------------------------------
  User-name                      State  AuthMask  AdminLevel
  ------------------------------------------------------------------------------
  user1                          A      H         -
  user2                          A      A         -
  ------------------------------------------------------------------------------
  Total 2 user(s)
```

在 PC 上，配置二进制传输格式和 c:\temp 为工作目录。

说明

以下操作以 WindowsXP 系统为例进行说明。

将上传文件存放到指定目录（假定为 C:\temp 目录）中，在“开始”菜单“运行”中键入 cmd，然后按“回车”键。之后键入 FTP 10.1.1.1，在“user”提示下输入用户名，在“password”提示下输入密码，配置信息如下：

```
C:\Documents and Settings\Administrator> ftp 10.1.1.1
Connect to 10.1.1.1.
220 FTP server ready.
User <10.1.1.1:<none>>:user1
331 Please specify the password.
Password:
230 User logged in.
```

设置 FTP 客户端存放上传文件的目录路径和文件的传输模式。

```
ftp> binary
200 Type set to I.
ftp> lcd c:\temp
Local directory now c:\temp.
```

在 PC 上，将 PC 上的新版本系统软件文件（*.cc）上传到设备中去。

```
ftp> put V200R002C00.cc
200 Port command okay.
226 Transfer complete.
```

步骤 2 指定下次重新启动时运行的系统软件和配置文件。

指定下次启动时运行的系统软件。

```
<Huawei> startup system-software sd1:/V200R002C00.cc
This operation will take several minutes, please wait.........
Info: Succeeded in setting the file for booting system
```

指定下次启动时运行的配置文件。

```
<Huawei> startup saved-configuration aa.cfg
This operation will take several minutes, please wait...
Info: Succeeded in setting the file for booting system
```

查看下次重新启动时的系统软件和配置文件，确认下次启动软件为指定的软件版本。

```
<Huawei> display startup
MainBoard:
  Startup system software :                  sd1/V200R001C00.cc
  Next startup system software :             sd1/V200R002C00.cc
  Backup system software for next startup:   null
  Startup saved-configuration file:          sd1:/iascfg.zip
  Next startup saved-configuration file :    sd1:/aa.cfg
  Startup license file:                      null
  Next startup license file:                 null
  Startup patch package:                     null
  Next startup patch package:                null
  Startup voice-files:                       null
  Next startup voice-files:                  null
```

步骤 3 指定系统备份启动软件包。

配置系统的备份启动软件包，确保系统在出现故障的情况下能重新正常启动。

```
<Huawei> startup system-software sd1:/V200R001C00_backup.cc backup
This operation will take several minutes, please wait...
Info: Succeeded in setting the backup file for booting system
```

步骤 4 保存配置文件，重启设备。

保存配置文件。

```
<Huawei> save
The current configuration will be written to the device.
Are you sure to continue? [Y/N]:y
It will take several minutes to save configuration file, please wait...
```

```
Configuration file had been saved successfully
Note: The configuration file will take effect after being activated
```

重启设备。

```
<Huawei> reboot
Info: The system is comparing the configuration, please wait.
Warning: All the configuration will be saved to the next startup configuration.
Continue ? [y/n]:y
  It will take several minutes to save configuration file, please wait........
  Configuration file had been saved successfully
  Note: The configuration file will take effect after being activated
System will reboot! Continue ? [y/n]:y
Info: system is rebooting ,please wait...
```

步骤 5 验证配置结果。

设备重启后，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。

```
<Huawei> system-view
[Huawei] display version
Huawei Versatile Routing Platform Software
VRP (R) software, Version 5.10 (AR3200 V200R002C00)
Copyright (C) 2000-2010 Huawei Technologies Co., LTD
Huawei AR3260 Router uptime is 0 week, 0 day, 3 hours, 59 minutes
BKP 0 version information:
1. PCB      Version  : AR01BAK1A VER.C
2. If Supporting PoE : Yes
3. Board    Type     : AR3260
4. MPU Slot Quantity : 1
5. LPU Slot Quantity : 2

MPU 0(Master) : uptime is 0 week, 0 day, 3 hours, 59 minutes
Flash Memory Size    : 16     M bytes
NVRAM Memory Size    : 512     K bytes
SD Card1 Memory Size : 1887    M bytes
MPU version information :
1. PCB      Version  : AR01SRU1A VER.A
2. MAB      Version  : 0
3. Board    Type     : AR3260
4. CPLD1    Version  : 100
5. BootROM  Version  : -

LPU 1 : uptime is 0 week, 0 day, 3 hours, 53 minutes
SDRAM Memory Size    : 256     M bytes
Flash Memory Size    : 64      M bytes
LPU version information :
1. PCB      Version  : AR01SDCE2A VER.A
2. MAB      Version  : 0
3. Board    Type     : 2T1/T1-M
4. CPLD1    Version  : 0
5. CPLD2    Version  : 0
6. BootROM  Version  : 906

LPU 2 : uptime is 0 week, 0 day, 3 hours, 53 minutes
SDRAM Memory Size    : 256     M bytes
Flash Memory Size    : 64      M bytes
LPU version information :
1. PCB      Version  : AR01SDSA2A VER.A
2. MAB      Version  : 0
3. Board    Type     : 1SA
4. CPLD1    Version  : 0
5. CPLD2    Version  : 0
6. BootROM  Version  : 906
```

----结束

配置文件

```
#
 ftp server enable
#
aaa
 local-user user1 password N`C55QK<`=/Q=^Q`MAF4<1!!
 local-user user1 ftp-directory sd1:
 local-user user1 service-type ftp
#
 Startup system software:                  sd1:/V200R001C00.cc
 Next startup system software:             sd1:/V200R002C00.cc
#
return
```

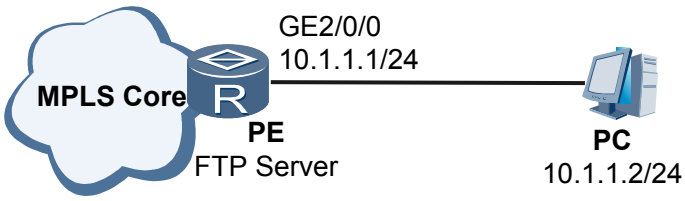
9.7.2 为系统安装补丁示例

通过介绍如何为系统打补丁实现不中断业务的情况下安装补丁文件。

组网需求

如图 9-7 所示，网络中的某设备的版本系统需要优化时，华为公司提供满足优化需求的补丁文件。

图 9-7 为系统安装补丁组网图



配置思路

采用以下思路为系统安装补丁：

1. 将补丁文件上传到主控板的存储介质中。
2. 加载并运行补丁。
3. 检查配置结果。

数据准备

为完成此配置项，需准备以下数据：

- 补丁的文件名是“SPH-1.1.952.pat”。
- 补丁在主控板存储路径是“sd1:/”。

操作步骤

步骤 1 上传与系统软件相对应的补丁文件。

将 PC 上与当前系统软件相对应的补丁文件上传到设备中。

```
ftp> put SPH-1.1.952.pat
200 Port command okay.
226 Transfer complete.
```

步骤 2 加载、激活并运行补丁。

```
<Huawei> patch load SPH-1.1.952.pat all run
Patch operation succeeded
```

步骤 3 检查配置结果。

通过上述配置后，执行命令 **display patch-information** 可以看到设备当前正在运行的补丁状态。

```
<Huawei> display patch-information
Patch version    :    ARV200R001C00SPH100
Patch packet name:    sd1:/SPH-1.1.952.pat
```

----结束