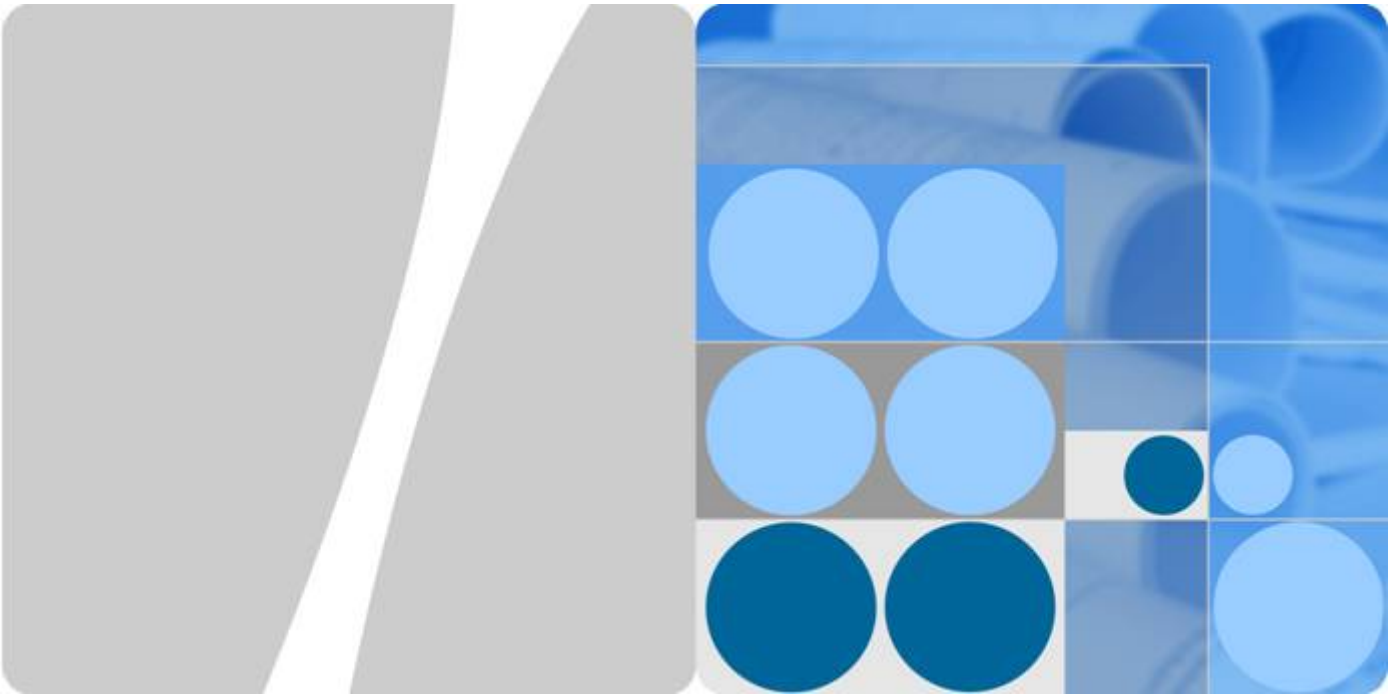


Quidway S5700 系列以太网交换机

V100R005C01

配置指南-基础配置

文档版本　03

发布日期　2011-01-30

华为技术有限公司

版权所有 © 华为技术有限公司 2011。 保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

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： 0755-28560000 4008302118

客户服务传真： 0755-28560111

前 言

读者对象

本文档介绍了 S5700 的基础特性，从配置过程和配置举例两方面对特性进行介绍。

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。

华为专有和保密信息
版权所有 © 华为技术有限公司

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。

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 03 (2011-01-30)

相对于文档版本 02（2010-12-01）的变化如下：

修改了部分图形。

文档版本 02 (2010-12-01)

相对于文档版本 01（2010-08-15）的变化如下：

增加：

- 命令行介绍中 **2.4 快捷键**部分。

修改：

- 修改 Web 网管配置中的配置参数的缺省值。

文档版本 01 (2010-08-15)

第一次正式发布。

版权所有 © 华为技术有限公司

目 录

前 言 iii

1 登录交换机 1-1

1.1 简介 1-2

1.1.1 通过 Console 口登录交换机 1-2

1.1.2 通过 Telnet 登录交换机 1-2

1.2 通过 Console 口登录交换机 1-2

1.2.1 建立配置任务 1-3

1.2.2 建立物理连接 1-3

1.2.3 配置终端 1-4

1.2.4 登录交换机 1-4

1.3 通过 Telnet 登录交换机 1-4

1.3.1 建立配置任务 1-5

1.3.2 建立物理连接 1-5

1.3.3 配置登录用户参数 1-6

1.3.4 从 Telnet 客户端登录 1-6

1.4 配置举例 1-6

1.4.1 配置通过 Console 口登录示例 1-6

1.4.2 配置通过 Telnet 登录示例 1-9

2 命令行介绍 2-1

2.1 命令行简介 2-2

2.1.1 命令行接口 2-2

2.1.2 命令级别 2-2

2.1.3 命令视图 2-3

2.2 在线帮助 2-5

2.2.1 完全帮助 2-5

2.2.2 部分帮助 2-6

2.2.3 命令行错误信息 2-6

2.3 命令行特性 2-7

2.3.1 编辑特性 2-7

2.3.2 显示特性 2-8

2.3.3 正则表达式 2-8

2.3.4 历史命令 2-11

版权所有 © 华为技术有限公司

2.4 快捷键.....2-12
2.4.1 系统快捷键.....2-12
2.4.2 快捷键的使用.....2-13
2.5 配置举例.....2-13
2.5.1 Tab 键使用示例.....2-14
3 如何使用接口.....3-1
3.1 接口概述.....3-2
3.2 配置接口基本参数.....3-4
3.2.1 建立配置任务.....3-4
3.2.2 进入接口视图.....3-5
3.2.3 查看接口下所有命令.....3-5
3.2.4 配置接口描述.....3-6
3.2.5 启动和关闭接口.....3-6
3.2.6 进一步配置接口.....3-6
3.2.7 检查配置结果.....3-7
3.3 配置 Loopback 接口.....3-7
3.3.1 建立配置任务.....3-7
3.3.2 配置 Loopback 接口 IPv4 相关项.....3-8
3.3.3 检查配置结果.....3-8
3.4 维护接口.....3-8
3.4.1 清除接口统计信息.....3-9
3.4.2 调试接口.....3-9
4 基本配置.....4-1
4.1 基本配置简介.....4-2
4.2 配置系统的基本环境.....4-2
4.2.1 建立配置任务.....4-2
4.2.2 设置设备名称.....4-3
4.2.3 设置系统时钟.....4-3
4.2.4 设置标题文本.....4-4
4.2.5 设置命令级别.....4-4
4.3 配置用户的基本环境.....4-5
4.3.1 建立配置任务.....4-5
4.3.2 配置切换用户级别的口令.....4-6
4.3.3 切换用户级别.....4-6
4.3.4 锁定用户界面.....4-7
4.4 显示系统基本配置信息.....4-7
4.4.1 显示系统配置信息.....4-8
4.4.2 显示系统运行状态.....4-8
4.4.3 收集系统诊断信息.....4-8
5 用户管理.....5-1
5.1 用户管理简介.....5-2

版权所有 © 华为技术有限公司

5.1.1 用户界面.....5-2
5.1.2 用户验证.....5-3
5.2 通过 Console 口首次登录 S5700.....5-5
5.2.1 建立登录任务.....5-5
5.2.2 通过 Console 口登录 S5700.....5-5
5.3 配置 Console 用户界面.....5-8
5.3.1 建立配置任务.....5-9
5.3.2 配置 Console 接口属性.....5-9
5.3.3 配置 Console 终端属性.....5-10
5.3.4 配置用户的优先级.....5-10
5.3.5 配置用户验证方式.....5-11
5.3.6 检查配置结果.....5-11
5.4 配置 VTY 用户界面.....5-12
5.4.1 建立配置任务.....5-12
5.4.2 配置 VTY 用户界面的最大个数.....5-13
5.4.3 （可选）配置呼入呼出限制.....5-13
5.4.4 配置 VTY 终端属性.....5-14
5.4.5 配置用户验证方式.....5-14
5.4.6 检查配置结果.....5-15
5.5 管理用户界面.....5-15
5.5.1 建立配置环境.....5-16
5.5.2 发送消息给其它用户界面.....5-16
5.5.3 清除在线用户.....5-17
5.5.4 检查配置结果.....5-17
5.6 配置用户管理.....5-17
5.6.1 建立配置任务.....5-18
5.6.2 配置验证用户的方式.....5-18
5.6.3 配置 Password 方式的口令.....5-19
5.6.4 配置 AAA 方式用户名和密码.....5-19
5.6.5 配置登录不验证.....5-19
5.6.6 设置用户的优先级.....5-20
5.6.7 检查配置结果.....5-20
5.7 配置举例.....5-21
5.7.1 配置用户通过 Password 方式登录交换机示例.....5-21
5.7.2 配置用户通过 AAA 方式登录交换机示例.....5-22
6 管理文件系统.....6-1
6.1 文件系统简介.....6-2
6.2 管理存储设备.....6-2
6.2.1 建立配置任务.....6-2
6.2.2 （可选）格式化存储设备.....6-3
6.3 管理目录.....6-3
6.3.1 建立配置任务.....6-3

版权所有 © 华为技术有限公司

6.3.2 查看当前的工作目录.....6-4
6.3.3 改变当前目录.....6-4
6.3.4 显示目录或文件信息.....6-4
6.3.5 创建目录.....6-5
6.3.6 删除目录.....6-5
6.4 管理文件.....6-5
6.4.1 建立配置任务.....6-6
6.4.2 显示文件的内容.....6-7
6.4.3 拷贝文件.....6-7
6.4.4 移动文件.....6-7
6.4.5 重新命名文件.....6-7
6.4.6 压缩文件.....6-8
6.4.7 删除文件.....6-8
6.4.8 彻底删除回收站中的文件.....6-8
6.4.9 恢复删除文件.....6-8
6.4.10 运行批处理文件.....6-9
6.4.11 配置文件系统提示方式.....6-9
7 管理配置文件.....7-1
7.1 管理配置文件简介.....7-2
7.1.1 配置文件.....7-2
7.1.2 配置文件和当前配置.....7-2
7.2 管理配置文件.....7-2
7.2.1 建立配置任务.....7-3
7.2.2 配置交换机下次启动时加载的系统软件.....7-4
7.2.3 配置交换机下次启动时加载的配置文件.....7-4
7.2.4 保存配置文件.....7-5
7.2.5 清除配置文件的内容.....7-5
7.2.6 比较配置文件.....7-5
7.2.7 检查配置结果.....7-6
8 FTP 和 TFTP.....8-1
8.1 FTP 和 TFTP 简介.....8-2
8.1.1 FTP.....8-2
8.1.2 TFTP.....8-2
8.2 配置交换机作为 FTP 服务器.....8-2
8.2.1 建立配置任务.....8-3
8.2.2 （可选）指定 FTP 服务器端口号.....8-4
8.2.3 使能 FTP 服务器.....8-4
8.2.4 （可选）配置 FTP 服务器超时断开连接的时间.....8-4
8.2.5 配置本地用户名和口令.....8-5
8.2.6 配置服务类型及授权信息.....8-5
8.2.7 检查配置结果.....8-5

版权所有 © 华为技术有限公司

8.3 配置 FTP 访问控制列表.....8-6
8.3.1 建立配置任务.....8-6
8.3.2 使能 FTP 服务器.....8-7
8.3.3 配置基本访问控制列表.....8-7
8.3.4 配置 FTP 基本访问控制列表.....8-8
8.3.5 检查配置结果.....8-8
8.4 配置交换机作为 FTP 客户端.....8-8
8.4.1 建立配置任务.....8-9
8.4.2 登录 FTP 服务器.....8-10
8.4.3 配置文件传输方式.....8-10
8.4.4 查看 FTP 命令的在线帮助.....8-11
8.4.5 上传、下载文件.....8-12
8.4.6 管理目录.....8-13
8.4.7 管理文件.....8-14
8.4.8 更改登录用户.....8-15
8.4.9 断开 FTP 连接.....8-15
8.4.10 检查配置结果.....8-16
8.5 配置交换机作为 TFTP 客户端.....8-17
8.5.1 建立配置任务.....8-17
8.5.2 使用 TFTP 下载文件.....8-18
8.5.3 使用 TFTP 上传文件.....8-18
8.6 限制对 TFTP 服务器的访问.....8-18
8.6.1 建立配置任务.....8-19
8.6.2 配置基本访问控制列表.....8-19
8.6.3 配置 TFTP 基本访问控制列表.....8-20
8.7 配置举例.....8-20
8.7.1 配置 FTP 服务器端示例.....8-20
8.7.2 配置 FTP 访问控制列表示例.....8-22
8.7.3 配置 FTP 客户端示例.....8-24
8.7.4 配置 TFTP 客户端示例.....8-26
9 Telnet 及 SSH.....9-1
9.1 Telnet 及 SSH 简介.....9-2
9.1.1 用户登录概述.....9-2
9.1.2 Telnet 终端服务基本概念.....9-2
9.1.3 SSH 终端服务基本概念.....9-3
9.2 配置 Telnet 终端服务.....9-4
9.2.1 建立配置任务.....9-4
9.2.2 使能 Telnet 服务.....9-5
9.2.3 建立 Telnet 连接.....9-6
9.2.4 （可选）Telnet 连接的定时断开.....9-6
9.2.5 检查配置结果.....9-6
9.3 配置 SSH 用户.....9-7

版权所有 © 华为技术有限公司

9.3.1 建立配置任务.....9-7
9.3.2 创建 SSH 用户.....9-8
9.3.3 配置 VTY 用户界面支持 SSH 协议.....9-9
9.3.4 生成本地 RSA 密钥对.....9-9
9.3.5 配置 SSH 用户的认证方式.....9-9
9.3.6 （可选）配置 SSH 用户基本验证信息.....9-10
9.3.7 （可选）配置 SSH 用户按命令行授权.....9-11
9.3.8 配置 SSH 用户的服务方式.....9-11
9.3.9 （可选）配置 SSH 用户的 SFTP 服务授权目录.....9-12
9.3.10 检查配置结果.....9-12
9.4 配置 SSH 服务器功能.....9-13
9.4.1 建立配置任务.....9-13
9.4.2 使能 STelnet 服务.....9-14
9.4.3 使能 SFTP 服务.....9-14
9.4.4 （可选）使能兼容低版本功能.....9-14
9.4.5 （可选）配置 SSH 服务器端监听端口号.....9-15
9.4.6 （可选）配置服务器密钥对更新时间.....9-15
9.4.7 检查配置结果.....9-16
9.5 配置 STelnet 客户端功能.....9-16
9.5.1 建立配置任务.....9-16
9.5.2 使能 SSH 客户端首次认证功能.....9-17
9.5.3 （可选）SSH 客户端为 SSH 服务器分配 RSA 公钥.....9-18
9.5.4 启动 STelnet 客户端.....9-19
9.5.5 检查配置结果.....9-19
9.6 配置 SFTP 客户端功能.....9-20
9.6.1 建立配置任务.....9-21
9.6.2 使能 SSH 客户端首次认证功能.....9-21
9.6.3 （可选）SSH 客户端为 SSH 服务器分配 RSA 公钥.....9-22
9.6.4 启动 SFTP 客户端.....9-23
9.6.5 （可选）管理目录.....9-23
9.6.6 （可选）管理文件.....9-24
9.6.7 （可选）SFTP 客户端命令帮助.....9-25
9.6.8 检查配置结果.....9-26
9.7 配置举例.....9-26
9.7.1 配置 Telnet 终端服务示例.....9-27
9.7.2 配置 PC 作为 STelnet 客户端连接 SSH 服务器的示例.....9-29
9.7.3 配置交换机作为 STelnet 客户端连接 SSH 服务器的示例.....9-32
9.7.4 配置 SFTP 客户端连接 SSH 服务器的示例.....9-38
9.7.5 配置 SSH 服务器支持其他端口号访问的示例.....9-44
9.7.6 配置 SSH 支持 RADIUS 认证的示例.....9-50
10 Web 网管配置.....10-1
10.1 Web 网管概述.....10-2

版权所有 © 华为技术有限公司

10.2 启用 Web 网管.....10-2
10.2.1 通过 Console 口登录 S5700.....10-3
10.2.2 设置 S5700 的管理 IP 地址.....10-6
10.2.3 上传 Web 网页文件.....10-6
10.2.4 加载 Web 网页文件.....10-7
10.2.5 创建 Web 网管帐号.....10-7
10.2.6 登录 Web 网管.....10-8

版权所有 © 华为技术有限公司

插图目录

图 1-1 配置通过 Console 口登录组网图.....1-7
图 1-2 新建连接.....1-7
图 1-3 连接端口设置.....1-8
图 1-4 端口通信参数设置.....1-8
图 1-5 配置通过 Telnet 登录组网图.....1-9
图 1-6 PC 上的 Telnet 界面.....1-10
图 5-1 S5700 用户界面的编号.....5-3
图 5-2 通过 Console 口登录到 S5700.....5-5
图 5-3 新建连接.....5-6
图 5-4 连接端口设置.....5-6
图 5-5 端口通信参数设置.....5-7
图 5-6 终端类型选择.....5-8
图 8-1 Switch 作为 FTP 服务器的组网图.....8-21
图 8-2 配置 FTP 访问控制列表组网图.....8-23
图 8-3 Switch 作为 FTP 客户端的组网图.....8-25
图 8-4 配置 TFTP 组网图.....8-27
图 9-1 提供 Telnet client 服务.....9-2
图 9-2 PC 与 S5700 建立本地 SSH 连接.....9-3
图 9-3 Ethernet 网络用户远程登录组网图.....9-27
图 9-4 配置 PC 作为 STelnet 客户端连接 SSH 服务器组网图.....9-29
图 9-5 配置 STelnet 客户端连接 SSH 服务器组网图.....9-32
图 9-6 配置 SFTP 客户端连接 SSH 服务器组网图.....9-38
图 9-7 配置 SSH 服务器支持其他端口号访问组网图.....9-44
图 9-8 配置 SSH 支持 RADIUS 认证组网图.....9-50
图 10-1 Web 网管运行环境.....10-2
图 10-2 新建连接.....10-3
图 10-3 连接端口设置.....10-4
图 10-4 端口通信参数设置.....10-4
图 10-5 终端类型选择.....10-5
图 10-6 登录界面.....10-8

版权所有 © 华为技术有限公司

表格目录

表 2-1 命令行常见错误信息表.....2-7
表 2-2 编辑功能表.....2-7
表 2-3 显示功能表.....2-8
表 2-4 特殊字符及其语法意义描述.....2-9
表 2-5 访问历史命令.....2-11
表 2-6 系统快捷键.....2-12
表 3-1 各管理接口介绍.....3-2
表 3-2 各管理接口编号.....3-2
表 3-3 以太网接口编号规则.....3-3
表 5-1 用户界面类型.....5-2
表 5-2 登录用户的类型.....5-3
表 5-3 登录用户的验证方式.....5-4
表 5-4 通信参数.....5-7
表 10-1 通信参数.....10-5

版权所有 © 华为技术有限公司

1 登录交换机

关于本章

配置交换机之前需要首先登录交换机。

1.1 简介
可以通过 Console 口、Telnet 登录交换机。

1.2 通过 Console 口登录交换机
通过 Console 口配置终端与交换机的连接，搭建配置环境。

1.3 通过 Telnet 登录交换机
通过 Telnet 配置终端与交换机的连接，搭建配置环境。

1.4 配置举例
配置通过 Console 口、Telnet 登录交换机的实例分析。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。

版权所有 © 华为技术有限公司

1.1 简介

可以通过 Console 口、Telnet 登录交换机。

1.1.1 通过 Console 口登录交换机
通过 Console 口登录主要用于交换机第一次上电或本地配置。

1.1.2 通过 Telnet 登录交换机
如果已知待登录交换机的 IP 地址，用户可以通过 Telnet 方式登录到交换机上，进行本地或者远程配置。

1.1.1 通过 Console 口登录交换机

通过 Console 口登录主要用于交换机第一次上电或本地配置。

有两种情况，只能通过 Console 口对交换机进行配置：

- 交换机第一次上电；
- 无法通过 Telnet 登录交换机。

1.1.2 通过 Telnet 登录交换机

如果已知待登录交换机的 IP 地址，用户可以通过 Telnet 方式登录到交换机上，进行本地或者远程配置。

用户需要通过 Console 口方式预先正确配置交换机接口的 IP 地址，配置用户账号以及正确的登录验证方式和呼入呼出受限规则，并且终端与交换机之间直连或有可达路由。

目标交换机根据配置的登录参数对用户进行验证，包括三种方式：

- password 验证：登录用户需要输入正确的口令
- AAA 本地验证：登录用户需要输入正确的用户名和口令
- 不验证：登录用户不需要输入用户名或口令

登录成功后，Telnet 客户端界面上出现命令行提示符（如<Quidway>）。

此时可以键入命令，查看交换机运行状态，或对交换机进行配置，需要帮助可以随时键入“?”。

说明

通过 Telnet 配置交换机时，请不要轻易改变交换机的 IP 地址（修改可能导致 Telnet 连接断开）。如有必要修改，须在修改后输入交换机的新 IP 地址，重新建立连接。

1.2 通过 Console 口登录交换机

通过 Console 口配置终端与交换机的连接，搭建配置环境。

1.2.1 建立配置任务
在进行通过 Console 口登录交换机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。

1.2.2 建立物理连接

华为专有和保密信息
版权所有 © 华为技术有限公司

通过 Console 口登录交换机的物理连接方法。

1.2.3 配置终端
通过 Console 口登录交换机配置终端的方法。

1.2.4 登录交换机
通过 Console 口登录交换机的方法。

1.2.1 建立配置任务

在进行通过 Console 口登录交换机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

通过 Console 口登录主要用于交换机第一次上电或本地配置。

说明

当交换机无法远程访问时，可通过 Console 口登录。

前置任务

在配置通过 Console 口配置交换机之前，需要完成以下任务：

- 准备好 PC/终端（含串口和 RS-232 电缆）
- PC 已安装终端仿真程序（如 Windows XP 的超级终端）

数据准备

在通过 Console 口配置交换机之前，需要准备以下数据。

说明

如果通过 Console 口登录交换机时配置了 AAA 验证方式，需要登录用户名和密码。

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）
2	（可选）AAA 验证方式下的登录用户名和密码

1.2.2 建立物理连接

通过 Console 口登录交换机的物理连接方法。

背景信息

请在登录交换机上进行以下配置。

操作步骤

步骤 1 使用配置电缆将 PC 的 COM 口和交换机的 Console 口连接。

版权所有 © 华为技术有限公司

步骤 2 所有设备上电，自检正常。

----结束

1.2.3 配置终端

通过 Console 口登录交换机配置终端的方法。

背景信息

请在 PC 上进行以下配置。

操作步骤

步骤 1 在 PC 上运行终端仿真程序，设置终端通信参数为：

- 波特率：9600 bps
- 数据位：8
- 停止位：1
- 校验：无
- 流控：无

----结束

1.2.4 登录交换机

通过 Console 口登录交换机的方法。

背景信息

请在 PC 上进行以下配置。

操作步骤

步骤 1 按 Enter 键，直到出现用户视图的命令行提示符，如<Quidway>；至此用户进入了用户视图配置环境。

说明

如果通过 Console 口登录交换机时配置了 AAA 或 Password 验证方式，需要在登录之前输入登录用户名和密码。

----结束

1.3 通过 Telnet 登录交换机

通过 Telnet 配置终端与交换机的连接，搭建配置环境。

1.3.1 建立配置任务
在进行通过 Telnet 登录交换机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。

1.3.2 建立物理连接

华为专有和保密信息
版权所有 © 华为技术有限公司

通过 Telnet 登录交换机的物理连接方法。

1.3.3 配置登录用户参数
通过 Telnet 登录交换机配置登录用户参数的方法。

1.3.4 从 Telnet 客户端登录
通过 Telnet 登录交换机的方法。

1.3.1 建立配置任务

在进行通过 Telnet 登录交换机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

如果已知待登录交换机的 IP 地址，用户可以通过 Telnet 方式登录到交换机上，进行本地或者远程配置。

前置任务

在配置通过 Telnet 登录交换机之前，需要完成以下任务：

- 设备上电自检正常
- 准备好 PC（含串口和 Ethernet 交叉/直通网线）

数据准备

在配置通过 Telnet 配置交换机之前，需要准备以下数据。

序号	数据
1	PC 的 IP 地址
2	待配置交换机以太网接口的 IP 地址
3	Telnet 访问的用户信息（用户名、口令和验证方式）

1.3.2 建立物理连接

通过 Telnet 登录交换机的物理连接方法。

前提条件

完成物理连接的建立。

操作步骤

步骤 1 通过网线把交换机和 PC 直连或 PC 和交换机分别通过网线连接入网络中。

----结束

版权所有 © 华为技术有限公司

1.3.3 配置登录用户参数

通过 Telnet 登录交换机配置登录用户参数的方法。

背景信息

请在登录交换机上进行以下配置。

操作步骤

步骤 1 配置登录用户的验证方式。

步骤 2 配置登录用户的权限限制。

配置的具体步骤请参见 **5.4 配置 VTY 用户界面**和 **5.6 配置用户管理**。

----结束

1.3.4 从 Telnet 客户端登录

通过 Telnet 登录交换机的方法。

背景信息

请在 PC 上进行以下配置。

操作步骤

步骤 1 在 PC 上运行 Telnet 客户端程序，键入目标交换机提供 Telnet 服务的接口 IP 地址。

步骤 2 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<Quidway>。至此用户进入了用户视图配置环境。

----结束

1.4 配置举例

配置通过 Console 口、Telnet 登录交换机的实例分析。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。

1.4.1 配置通过 Console 口登录示例
配置通过 Console 口登录交换机的示例。在本示例中，在 PC 端进行登录的设置，实现通过 Console 口登录交换机。

1.4.2 配置通过 Telnet 登录示例
配置通过 Telnet 登录交换机的示例。在本示例中，通过配置用户登录参数，实现从客户端登录交换机。

1.4.1 配置通过 Console 口登录示例

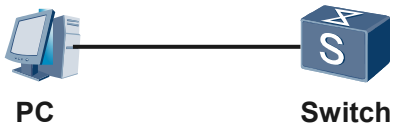
配置通过 Console 口登录交换机的示例。在本示例中，在 PC 端进行登录的设置，实现通过 Console 口登录交换机。

华为专有和保密信息
版权所有 © 华为技术有限公司

组网需求

交换机第一次上电，需要通过串口对交换机进行初始的配置。

图 1-1 配置通过 Console 口登录组网图



配置思路

1. 通过 Console 口连接 PC 和交换机。
2. 在 PC 端进行登录的设置。
3. 登录交换机。

数据准备

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）。

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 配置电缆与交换机的 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 9600bps、8 位数据位、1 位停止位、无校验和无流控，如图 1-2 至图 1-4 所示。

图 1-2 新建连接

华为专有和保密信息
版权所有 © 华为技术有限公司

图 1-3 连接端口设置

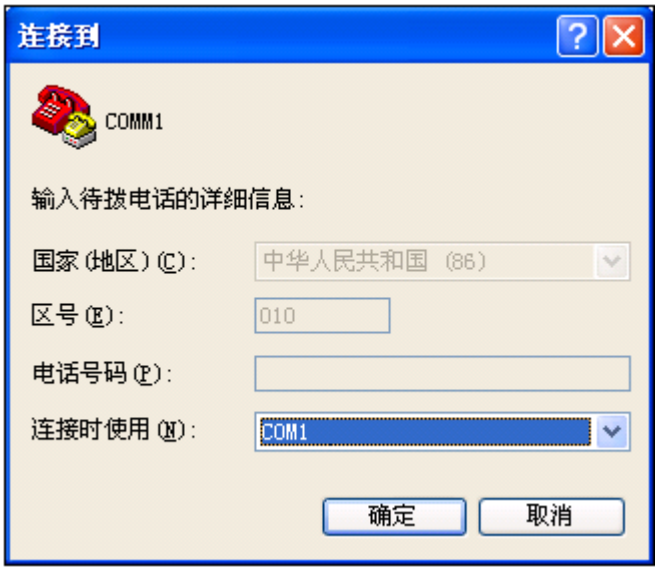
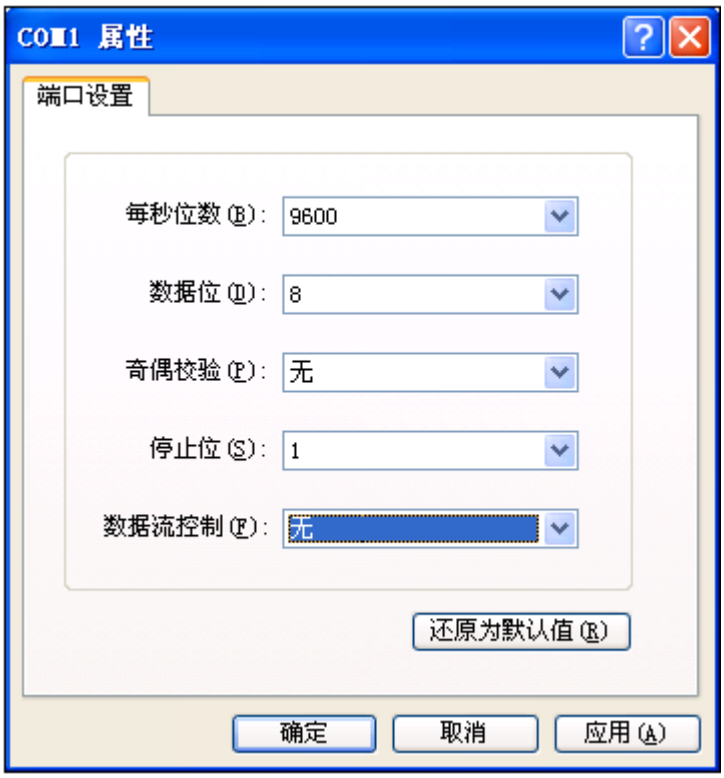


图 1-4 端口通信参数设置



步骤 3 交换机上电自检，系统自动进行配置，自检结束后提示用户键入回车，直到出现命令行提示符（如<Quidway>）。

华为专有和保密信息
版权所有 © 华为技术有限公司

此时可以键入命令，查看交换机运行状态，或对交换机进行配置，需要帮助可以随时键入“?”，关于具体的操作请参考以后各章节。

----结束

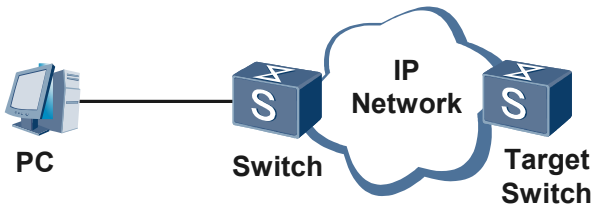
1.4.2 配置通过 Telnet 登录示例

配置通过 Telnet 登录交换机的示例。在本示例中，通过配置用户登录参数，实现从客户端登录交换机。

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交换机，进行远程维护。

图 1-5 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. 从客户端登录交换机

数据准备

- PC 的 IP 地址
- 待配置交换机以太网接口的 IP 地址
- Telnet 访问的用户信息（用户名、口令和验证方式）

操作步骤

步骤 1 在 PC 端和交换机端分别和网络连接。

步骤 2 在 Target 交换机端配置登录用户参数。

配置登录地址

```
<Quidway> system-view
[Quidway] vlan 10
[Quidway-vlan10] quit
[Quidway] interface gigabitethernet 0/0/1
[Quidway-GigabitEthernet0/0/1] port link-type hybrid
[Quidway-GigabitEthernet0/0/1] port hybrid untagged vlan 10
[Quidway-GigabitEthernet0/0/1] quit
[Quidway]interface vlanif 10
[Quidway-vlanif10] ip address 202.38.160.92 255.255.0.0
[Quidway-vlanif10] quit
```


版权所有 © 华为技术有限公司

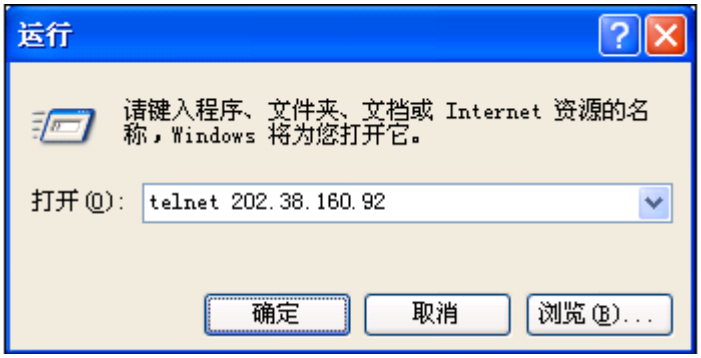
配置登录验证方式

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

步骤 3 配置客户端登录

在 PC 上运行 Telnet，如下图所示。

图 1-6 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<Quidway>。至此用户进入了用户视图配置环境。

说明

登录交换机前，需要保证 PC 和交换机能够 ping 通，否则无法登录交换机。

----结束

版权所有 © 华为技术有限公司

2 命令行介绍

关于本章

用户对设备的日常操作，主要通过输入命令行来实现。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
命令行接口是用户对命令行使用的常用工具。

2.2 在线帮助
输入命令行或进行配置业务时，在线帮助可以提供在配置手册之外的实时帮助。

2.3 命令行特性
命令行的特性包括编辑特性、显示特性、正则表达式的使用以及历史命令。

2.4 快捷键
介绍 S5700 设备提供的快捷键。

2.5 配置举例
通过以下几个举例，您可以了解到命令行的基本使用。

版权所有 © 华为技术有限公司

2.1 命令行简介

命令行接口是用户对命令行使用的常用工具。

2.1.1 命令行接口
通过命令行接口输入命令，您可以对交换机进行配置和管理。

2.1.2 命令级别
系统命令采用分级保护方式，命令从低到高划分为 16 个级别。

2.1.3 命令视图
命令视图就是执行命令行的界面环境。系统的所有命令都注册在某个（或某些）命令视图下，只有在相应的视图下才能执行该视图下的命令。

2.1.1 命令行接口

通过命令行接口输入命令，您可以对交换机进行配置和管理。

用户登录到交换机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交换机进行交互的常用工具。

系统向用户提供一系列命令，用户可以通过命令行接口输入命令，对交换机进行配置和管理。

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。
- 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。
- 通过不认证、password、AAA 三种验证方式，确保未授权用户无法侵入交换机，保证系统的安全。
- 用户可以随时键入“?”而获得在线帮助。
- 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。
- 用 **telnet** 命令直接登录并管理其它交换机。
- 提供 FTP 服务，方便用户上传、下载文件。
- 提供类似 DosKey 的功能，可以执行某条历史命令。
- 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。

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。
- 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

系统命令采用分级保护方式，命令从低到高划分为 16 个级别。

华为专有和保密信息
版权所有 © 华为技术有限公司

缺省情况下，命令按如下 0 ～ 3 级进行注册：

- 0 级，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 级，监控级：用于系统维护，包括 display 等命令。
- 2 级，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 级，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、Xmodem 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。

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。关于命令级别的提升请参见“**设置命令级别**”。

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。
- 登录用户也划分为 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。关于用户分级请参见“**用户管理**”。

2.1.3 命令视图

命令视图就是执行命令行的界面环境。系统的所有命令都注册在某个（或某些）命令视图下，只有在相应的视图下才能执行该视图下的命令。

命令视图基本概念

与交换机建立连接，如果此交换机是缺省配置，则进入用户视图，在屏幕上显示：

```
<Quidway>
```

键入 **system-view** 后回车，进入系统视图。

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

在系统视图下键入 **aaa**，则可进入 AAA 视图。

```
[Quidway] aaa
[Quidway-aaa]
```

说明

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

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。

常用视图

S5700 的命令视图有很多，下面提到的视图是最常用的视图。其他视图的进入方式在具体的命令中都有说明，请参见*《Quidway S5700 T 比特路由交换机 命令参考》*。

- 用户视图

版权所有 © 华为技术有限公司

项目	解释
功能	查看 S5700 的简单运行状态和统计信息。
进入命令	连接建立后直接进入
进入后提示符	<Quidway>
退出命令	<Quidway> **quit**
退出后提示符	无

- 系统视图

项目	解释
功能	配置 S5700 的系统参数，并通过该视图进入其他功能的配置视图。
进入命令	<Quidway> **system-view**
进入后提示符	[Quidway]
退出命令	[Quidway] **quit**
退出后提示符	<Quidway>

- 以太网接口视图
  - GE 接口视图

项目	解释
功能	配置 S5700 千兆以太网接口的相关参数，管理千兆以太网接口。
进入命令	[Quidway] interface GigabitEthernet *X/Y/Z*
进入后提示符	[Quidway-GigabitEthernet*X/Y/Z*]
退出命令	[Quidway-GigabitEthernet*X/Y/Z*] **quit**
退出后提示符	[Quidway]

说明

X/Y/Z 为需要配置的千兆以太网接口的接口编号，分别对应“槽位号/子卡号/以太网接口序号”。

- VLAN 视图

项目	解释
功能	将接口加入 VLAN 或从 VLAN 中删除接口，配置 VLAN 使能组播等功能。

版权所有 © 华为技术有限公司

项目	解释
进入命令	[Quidway] **vlan 10**
进入后提示符	[Quidway-vlan10]
退出命令	[Quidway-vlan10] **quit**
退出后提示符	[Quidway]

- VLANIF 接口视图

项目	解释
功能	配置 VLANIF 接口的 IP 地址，管理 VLANIF 接口
进入命令	[Quidway] **interface vlanif 10**
进入后提示符	[Quidway-Vlanif10]
退出命令	[Quidway-Vlanif10] **quit**
退出后提示符	[Quidway]

说明

10 为需要配置的 VLANIF 接口编号。进入 VLANIF 接口视图之前必须先创建对应的 VLAN。

2.2 在线帮助

输入命令行或进行配置业务时，在线帮助可以提供在配置手册之外的实时帮助。

背景信息

S5700 的命令行接口提供如下三种在线帮助：

- 完全帮助
- 部分帮助
- 命令行错误信息

2.2.1 完全帮助
应用完全帮助，系统可以协助您在输入命令行时，给予全部关键字或参数的提示。

2.2.2 部分帮助
应用部分帮助，系统可以协助您在输入命令行时，给予以该字符串开头的所有关键字或参数的提示。

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。

2.2.1 完全帮助

应用完全帮助，系统可以协助您在输入命令行时，给予全部关键字或参数的提示。

版权所有 © 华为技术有限公司

命令行的完全帮助可以通过以下 3 种方式获取：

- 在所有命令视图下，键入“?”获取该命令视图下所有的命令及其简单描述。
```
<Quidway> ?
```
- 键入命令，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描述。举例如下。
```
[Quidway-ui-vty0] authentication-mode ?
  aaa       AAA authentication
  none      Login without checking
  password  Authentication through the password of a user terminal interface
[Quidway-ui-vty0] authentication-mode aaa ?
<cr>
[Quidway-ui-vty0] authentication-mode aaa
```
其中 aaa、none 和 password 是关键字，AAA authentication、Login without checking 和 Authentication through the password of a user terminal interface 是对关键字的分别描述。

<cr>表示该位置没有关键字或参数，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。
- 键入命令，后接以空格分隔的“?”，如果该位置为参数，则列出有关的参数名和参数描述。举例如下。
```
<Quidway> system-view
[Quidway] sysname ?
TEXT  Host name(1 to 246 characters)
```
其中 TEXT 是参数名，Host name(1 to 246 characters)是对参数的描述。

2.2.2 部分帮助

应用部分帮助，系统可以协助您在输入命令行时，给予以该字符串开头的所有关键字或参数的提示。

背景信息

命令行的部分帮助可以通过以下三种方式获取。

操作步骤

- 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。
```
<Quidway> d?
  debugging                           delete
  dir                                 display
```
- 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。
```
<Quidway> display b?
  bfd                                 bgp
  bootrom                             bpdu
  bpdu-tunnel                         buffer
```
- 输入命令的某个关键字的前几个字母，按下<tab>键，可以显示出完整的关键字，前提是这几个字母可以唯一标示出该关键字，否则，连续按下<tab>键，可出现不同的关键字，用户可以从中选择所需要的关键字。

----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。

版权所有 © 华为技术有限公司

常见错误信息参见表 2-1。

表 2-1 命令行常见错误信息表

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

2.3 命令行特性

命令行的特性包括编辑特性、显示特性、正则表达式的使用以及历史命令。

2.3.1 编辑特性
命令行编辑功能有助于您利用某些特定的键进行命令的编辑或者获得帮助。

2.3.2 显示特性
所有的命令行有共同的显示特性，并且可以根据您的需求，灵活构建显示方式。

2.3.3 正则表达式
正则表达式是一种模式匹配工具，用户根据一定的规则构建匹配模式，然后将匹配模式与目标对象进行匹配。

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，用户可以随时调用命令行接口保存的历史命令，并重复执行。

2.3.1 编辑特性

命令行编辑功能有助于您利用某些特定的键进行命令的编辑或者获得帮助。

S5700 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 2-2 所示。

表 2-2 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。

华为专有和保密信息
版权所有 © 华为技术有限公司

功能键	功能
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，并且可以根据您的需求，灵活构建显示方式。

S5700 的命令行接口提供如下显示特性：

- 提示信息和帮助信息提供中、英文两种语言显示。
- 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 2-3 所示。

表 2-3 显示功能表

功能键	功能
键入<Ctrl_C>	停止显示和命令执行。 **说明** 也可以键入除空格键、回车键等的其他键停止显示和命令执行。
键入空格键	继续显示下一屏信息。
键入回车键	继续显示下一行信息。

2.3.3 正则表达式

正则表达式是一种模式匹配工具，用户根据一定的规则构建匹配模式，然后将匹配模式与目标对象进行匹配。

版权所有 © 华为技术有限公司

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。

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 2-4 是对特殊字符及其语法意义的使用描述。

表 2-4 特殊字符及其语法意义描述

特殊字符	功能	举例
\	转义字符。将下一个字符（特殊字符或者普通字符）标记为普通字符。	*匹配*
^	匹配行首的位置。	^10 匹配 10.10.10.1，不匹配 20.10.10.1
$	匹配行尾的位置。	1$匹配 10.10.10.1，不匹配 10.10.10.2
*	匹配前面的子正则表达式零次或多次。	10*可以匹配 1、10、100、1000、…… (10)*可以匹配空、10、1010、101010、……
+	匹配前面的子正则表达式一次或多次。	10+可以匹配 10、100、1000、…… (10)+可以匹配 10、1010、101010、……
?	匹配前面的子正则表达式零次或一次。	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、……

华为专有和保密信息
版权所有 © 华为技术有限公司

特殊字符	功能	举例
()	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。

版权所有 © 华为技术有限公司

在命令中指定过滤方式

注意

Quidway S5700 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。

在分屏显示时指定过滤方式

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

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

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，用户可以随时调用命令行接口保存的历史命令，并重复执行。

缺省情况下，为每个登录用户保存 10 条历史命令。对历史命令的操作如表 2-5 所示。

表 2-5 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。

版权所有 © 华为技术有限公司

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：

- S5700 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，S5700 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 ip routing** 和 **display ip routing-table**，将保存为两条历史命令。

2.4 快捷键

介绍 S5700 设备提供的快捷键。

2.4.1 系统快捷键

2.4.2 快捷键的使用

2.4.1 系统快捷键

系统快捷键是系统中固定的快捷键，不由用户定义，代表固定功能。系统包括的主要快捷键如**表 2-6** 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 2-6 系统快捷键

功能键	功能
CTRL_A	光标移动到当前行的开头
CTRL_B	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	光标移动到当前行的末尾
CTRL_F	光标向右移动一个字符
CTRL_H	删除光标左侧的一个字符
CTRL_K	停止呼出的连接
CTRL_N	查看历史命令缓冲区中的后一条命令
CTRL_P	查看历史命令缓冲区中的前一条命令
CTRL_R	重新显示当前行信息

版权所有 © 华为技术有限公司

功能键	功能
CTRL_U	删除光标左侧所有的字符
CTRL_V	粘贴剪贴板的内容
CTRL_W	删除光标左侧的一个字
CTRL_X	删除光标左侧所有的字符
CTRL_Y	删除光标右侧所有的字符
CTRL_Z	回到用户视图
CTRL_]	终止呼入的连接或重定向连接
ESC_B	光标向左移动一个字
ESC_D	删除光标右侧的一个字
ESC_F	光标向右移动一个字
ESC_N	光标向下移动一行
ESC_P	光标向上移动一行
ESC_<	将光标所在位置指定为剪贴板的开始位置
ESC_>	将光标所在位置指定为剪贴板的结束位置

2.4.2 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 S5700 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。

2.5 配置举例

通过以下几个举例，您可以了解到命令行的基本使用。

2.5.1 Tab 键使用示例

输入 Tab 键可以提示所有相关的关键字，或者检查关键字是否正确。

版权所有 © 华为技术有限公司

2.5.1 Tab 键使用示例

输入 Tab 键可以提示所有相关的关键字，或者检查关键字是否正确。

操作步骤

- 如果与不完整的关键字匹配的关键字唯一。

  请在 S5700 上执行以下配置。

  1. 输入不完整的关键字。

     ```
     [Quidway] 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。

     ```
     [Quidway] info-center
     ```

- 如果不匹配或者匹配的关键字不唯一。

  请在 S5700 上进行以下配置。

  # 关键字 info-center 后面可以跟如下 2 个关键字。

  ```
  [Quidway] info-center log?
    logbuffer                               loghost
  ```

  1. 输入不完整的关键字。

     ```
     [Quidway] info-center l
     ```

  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”。

     ```
     [Quidway] info-center log
     ```

  3. 继续按 Tab 键循环翻词，此时光标距词尾不空格。

     ```
     [Quidway] info-center loghost
     [Quidway] info-center logbuffer
     ```

     找到所需要的关键字 **logbuffer** 后，停止按 Tab 键。

  4. 按空格键，然后输入下一个单词 channel。

     ```
     [Quidway] info-center logbuffer channel
     ```

----结束

华为专有和保密信息
版权所有 © 华为技术有限公司

3 如何使用接口

关于本章

介绍接口的概念及接口的常用基础配置。

3.1 接口概述
接口是 S5700 提供给用户操作或配置的单元，主要用于接收和发送数据。

3.2 配置接口基本参数
介绍如何对接口进行初步配置。

3.3 配置 Loopback 接口
介绍初步配置 Loopback 接口的方法。

3.4 维护接口
介绍如何维护接口。

华为专有和保密信息
版权所有 © 华为技术有限公司

3.1 接口概述

接口是 S5700 提供给用户操作或配置的单元，主要用于接收和发送数据。

接口从功能上可以划分为管理接口和业务接口，从物理形态上可以划分为物理接口和逻辑接口。

说明

物理接口有时也被称为端口，为便于描述，在本手册中，统一描述为接口。

管理接口

管理接口，是一种人为的划分，主要是相对于业务接口而言的。管理接口主要为用户提供配置管理支持，也就是用户通过此类接口可以登录到 S5700，并进行配置和管理操作。管理接口不承担业务传输。

S5700 提供 Console、MEth 两种管理接口。

表 3-1 各管理接口介绍

接口名称	接口描述	接口用途
Console 口	遵循 EIA/TIA-232 标准，接口类型是 DCE。	该接口和配置终端的 COM 串口连接，用于搭建现场配置环境。
MEth 口	遵循 10/100BASE-TX 标准。	该接口和配置终端或网管站的网口连接，用于搭建现场或远程配置环境。

管理接口的编号规则如下：

表 3-2 各管理接口编号

接口名称	管理接口编号
Console 口	通常描述为用户界面接口“console 0”
MEth 口	描述为接口“MEth 0/0/1”

业务接口分类

业务接口就是承担业务传输的各类接口，按照接口速率可以分为千兆接口和万兆接口；按照接口电气属性可以分为电接口、光接口。

业务接口的编号规则如下：

非堆叠情况下，S5700 采用“槽位号/子卡号/接口序号”的编号规则来定义接口。

- 槽位号：表示当前交换机的槽位，取值为 0。
- 子卡号：表示业务接口板支持的子卡号，值为 0 或 1。

华为专有和保密信息
版权所有 © 华为技术有限公司

子卡号为“1”表示前插卡。

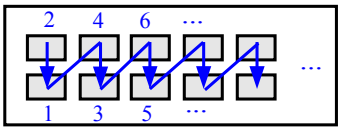
- 接口序号：表示设备上各接口的编排顺序号。

堆叠情况下，S5700 采用“堆叠号/子卡号/接口序号”的编号规则来定义接口。

- 堆叠号：表示堆叠 ID，取值为 0 ～ 8。
- 子卡号：表示业务接口板支持的子卡号，值为 0 或 1。

  子卡号为“1”表示前插卡。
- 接口序号：表示设备上各接口的编排顺序号。

表 3-3 以太网接口编号规则

接口编排规则示意图	说明
	设备有两排业务接口，左下接口从 1 起始编号，依据从下到上，再从左到右的规则依次递增编号。 例如，左上第一个接口编号为 0/0/2。

物理接口

物理接口是实际存在的接口。

物理接口包括各管理接口和各业务接口。

S5700 目前支持物理接口包括：

- Console 口
- 千兆以太网 GE（Gigabit Ethernet）接口
- 万兆以太网 10GE 接口

逻辑接口

逻辑接口是指物理上不存在且需要通过配置建立的接口。

S5700 目前支持的逻辑接口包括：

- Eth-Trunk 接口

  Eth-Trunk 只能由以太网链路构成。

  Eth-Trunk 技术有如下优点：

  - 增加带宽：Eth-Trunk 接口的带宽是各成员接口带宽的总和。
  - 提高可靠性：当某个成员链路出现故障时，流量会自动的切换到其他可用的链路上，从而提高整个 Eth-Trunk 链路的可靠性。

  具体配置方法请参见《Quidway S5700 系列 以太网交换机 配置指南-以太网》中的“配置 Eth-Trunk 接口”
- Loopback 接口

  Loopback 是一种虚拟接口。TCP/IP 协议规定，127.0.0.0 网段的地址属于环回地址，包含这类地址的接口属于环回接口。

版权所有 © 华为技术有限公司

系统在启动时自动创建一个使用环回地址 127.0.0.1 的接口，用来接收所有发送给本机的数据包。

但是有些应用（如配置 VPN 互访）需要在不影响物理接口配置的情况下，配置一个带有指定 IP 地址的本地接口；要求该本地接口的 IP 地址为 32 位掩码（节约 IP 地址），并且能够被路由协议发布出去。

利用 Loopback 接口永远 Up 的特性，还可以用做 Router ID、LSR ID、Tunnel 隧道借用 Loopback 的 IP 地址等。

具体的配置方法请参见**配置 Loopback 接口**。

- NULL 接口

  Null 接口类似于一些操作系统中支持的空设备（Null Devices），任何送到该接口的网络数据报文都会被丢弃。 Null 接口主要应用在路由选择和策略路由中。比如在路由选择的过程，如果匹配不到路由，就会把报文送到该接口。

- Tunnel 接口

  Tunnel 接口是一种逻辑接口，可以用于其他接口的备份接口、建立 GRE 隧道或 MPLS TE 隧道。

- VLANIF 接口

  当 S5700 需要与网络层的设备通信时，可以在 S5700 上创建基于 VLAN 的逻辑接口，即 VLANIF 接口。VLANIF 接口是网络层接口，可以配置 IP 地址。借助 VLANIF 接口，S5700 就能与其它网络层的设备互相通信。

  具体配置方法请参见《Quidway S5700 系列 以太网交换机 配置指南-以太网》中的“配置 VLANIF 接口”

3.2 配置接口基本参数

介绍如何对接口进行初步配置。

3.2.1 建立配置任务
在配置接口工作方式、路由等高级配置前，需要对接口进行基本配置。

3.2.2 进入接口视图
对接口进行基本配置前，需要进入接口视图。

3.2.3 查看接口下所有命令
进入接口视图后，可以查看接口视图下的所有命令。

3.2.4 配置接口描述
S5700 对于接口有一个接口描述，用来帮助识别和记忆接口的用途，以便管理。

3.2.5 启动和关闭接口
当某物理接口闲置，没有连接电缆时，请使用关闭该接口，以防止由于干扰导致接口异常；当需要使用关闭的接口时，请启动相应的接口。

3.2.6 进一步配置接口
配置完基本参数后，请根据需要进一步配置接口。

3.2.7 检查配置结果
基本参数配置完后，可以使用相关的 display 命令显示配置结果。

3.2.1 建立配置任务

在配置接口工作方式、路由等高级配置前，需要对接口进行基本配置。

华为专有和保密信息
版权所有 © 华为技术有限公司

应用环境

为了便于对接口进行配置和维护，在 S5700 中配置了接口视图，与接口有关的各种命令都必须在相应的接口视图下使用。

接口的基础配置包括：进入接口、配置接口描述信息、启动和关闭接口等。

前置任务

在 S5700 上正确安装接口板卡。

数据准备

在配置接口之前，需准备以下数据：

序号	数据
1	需配置接口的接口类型和接口编号
2	接口的描述信息

3.2.2 进入接口视图

对接口进行基本配置前，需要进入接口视图。

背景信息

请在 S5700 上进行以下配置。

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** *interface-type interface-number*，进入指定接口的接口视图。

其中，*interface-type* 为接口类型；*interface-number* 为接口编号。

----结束

3.2.3 查看接口下所有命令

进入接口视图后，可以查看接口视图下的所有命令。

背景信息

请在 S5700 上进行以下配置。

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** *interface-type interface-number* 进入指定的接口视图。

版权所有 © 华为技术有限公司

步骤 3 执行命令**?**，查看指定接口视图下所有命令。

----结束

3.2.4 配置接口描述

S5700 对于接口有一个接口描述，用来帮助识别和记忆接口的用途，以便管理。

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** *interface-type interface-number*，进入指定接口的接口视图。

步骤 3 执行命令 **description** *description*，配置接口描述。

----结束

3.2.5 启动和关闭接口

当某物理接口闲置，没有连接电缆时，请使用关闭该接口，以防止由于干扰导致接口异常；当需要使用关闭的接口时，请启动相应的接口。

背景信息

说明

- Null 接口一直处于 Up 状态，不能使用命令关闭 Null 接口。
- Loopback 接口一旦被创建，将一直保持 Up 状态，不能使用命令关闭 Loopback 接口。

操作步骤

- 关闭接口

  请在 S5700 上进行以下配置。

  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface** *interface-type interface-number*，进入指定接口的接口视图。
  3. 执行命令 **shutdown**，关闭接口。

  说明

  缺省情况下，接口处于打开状态。

- 启动接口

  请在 S5700 上进行以下配置。

  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface** *interface-type interface-number*，进入指定接口的接口视图。
  3. 执行命令 **undo shutdown**，启动接口。

----结束

3.2.6 进一步配置接口

配置完基本参数后，请根据需要进一步配置接口。

版权所有 © 华为技术有限公司

背景信息

用户要通过接口访问网络，除了需要完成接口的基本配置外，还需要详细了解组网需求，进一步配置接口的多项参数（高级配置）。

进一步配置接口包括：

- 配置接口工作方式
- 配置路由配置

具体配置请参见《Quidway S5700 系列 以太网交换机 配置指南-以太网》和《Quidway S5700 系列 以太网交换机 配置指南-IP 路由》

3.2.7 检查配置结果

基本参数配置完后，可以使用相关的 display 命令显示配置结果。

操作步骤

步骤 1 执行命令 **display interface** [*interface-type* [*interface-number*]]，查看接口当前运行状态和统计信息。

步骤 2 执行命令 **display interface description**，查看接口的描述信息。

步骤 3 执行命令 **display ip interface** [*interface-type interface-number*]，查看接口 IP 的主要配置信息。

步骤 4 执行命令 **display ip interface brief** [*interface-type interface-number*]，查看接口 IP 的简要状态信息。

----结束

3.3 配置 Loopback 接口

介绍初步配置 Loopback 接口的方法。

3.3.1 建立配置任务
用户可以创建或删除 Loopback 接口。Loopback 接口一旦被创建，将一直保持 Up 状态，直到被删除。

3.3.2 配置 Loopback 接口 IPv4 相关项
Loopback 接口可以配置 IPv4 地址，可以用于绑定 VPN 实例、对源 IPv4 地址进行校验。

3.3.3 检查配置结果
配置完 Loopback 接口后，请检查配置是否正确。

3.3.1 建立配置任务

用户可以创建或删除 Loopback 接口。Loopback 接口一旦被创建，将一直保持 Up 状态，直到被删除。

版权所有 © 华为技术有限公司

应用环境

有些应用（比如配置 VPN 互访）需要在不影响物理接口配置的情况下，配置一个带有指定 IP 地址的本地接口，并且需要将这个接口上的地址通过路由协议发布出去。Loopback 接口也常用来提高配置的可靠性。

前置任务

在配置 Loopback 接口之前，需完成 S5700 加电启动正常。

数据准备

在配置 Loopback 接口之前，需准备以下数据。

序号	数据
1	Loopback 接口的接口编号
2	Loopback 接口的 IP 地址

3.3.2 配置 Loopback 接口 IPv4 相关项

Loopback 接口可以配置 IPv4 地址，可以用于绑定 VPN 实例、对源 IPv4 地址进行校验。

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 loopback** *interface-number*，创建 Loopback 接口。

interface-number 取值范围为 0 ～ 1023，最多可创建 1024 个 Loopback 接口。

步骤 3 执行命令 **ip address** *ip-address* { *mask* | *mask-length* } [**sub**]，配置 Loopback 接口的 IPv4 地址。

步骤 4 （可选）执行命令 **ip verify source-address**，配置 Loopback 接口对源 IPv4 地址校验。

----结束

3.3.3 检查配置结果

配置完 Loopback 接口后，请检查配置是否正确。

操作步骤

步骤 1 执行命令 **display interface loopback** [*number*]，查看 Loopback 接口的状态信息。

----结束

3.4 维护接口

介绍如何维护接口。

版权所有 © 华为技术有限公司

3.4.1 清除接口统计信息
接口统计信息清除后，不能恢复。操作前请仔细确认。

3.4.2 调试接口
在接口异常的情况下，可以对接口进行调试。

3.4.1 清除接口统计信息

接口统计信息清除后，不能恢复。操作前请仔细确认。

操作步骤

步骤 1 在确认需要清除接口的统计信息后，请在用户视图下，执行命令 **reset counters interface** [*interface-type* [*interface-number*]]清除接口信息。

----结束

3.4.2 调试接口

在接口异常的情况下，可以对接口进行调试。

背景信息

有关 **debugging** 命令输出信息的解释请参考《Quidway S5700 系列 以太网交换机 Debugging 参考》。

各种接口的 **debugging** 命令请参看后续各章中对具体接口的维护介绍。

注意

打开调试开关将影响系统的性能。调试完毕后，应在用户视图下及时执行 **undo debugging all** 命令关闭调试开关。

版权所有 © 华为技术有限公司

4 基本配置

关于本章

基本配置包括系统基本环境和用户基本环境的配置。

4.1 基本配置简介
基本配置的意义和范围。

4.2 配置系统的基本环境
配置系统基本配置环境，以符合用户使用习惯或实际环境的需求。

4.3 配置用户的基本环境
配置用户基本配置环境，以切换用户级别。

4.4 显示系统基本配置信息
显示系统基本配置信息有相应的 display 命令。

版权所有 © 华为技术有限公司

4.1 基本配置简介

基本配置的意义和范围。

在配置业务之前，用户往往需要根据系统运行时的环境要求进行一些基本配置，以满足运行维护需求。

S5700 提供两方面的基本环境配置：

- 系统基本环境：主要包括语言模式、主机名、系统时间、标题文字和命令级别。
- 用户基本环境：主要包括级别切换的口令设置和终端锁定设置。

4.2 配置系统的基本环境

配置系统基本配置环境，以符合用户使用习惯或实际环境的需求。

4.2.1 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。

4.2.2 设置设备名称
设备名称可以根据需要进行更改，更改后立即生效。

4.2.3 设置系统时钟
为了保证网络中的设备在同一时钟下工作，需要设置或更改系统时钟。

4.2.4 设置标题文本
如果用户需要对登录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。

4.2.5 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。

4.2.1 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。

缺省情况下，S5700 支持的命令级别为 0 ～ 3 级，依次分别为：访问级、监控级、配置级和管理级。

如果用户需要在设备端定义更多级别，实现权限的更精细管理，可以采用命令行级别扩展功能，将命令级别由 0 ～ 3 级批量提升到 0 ～ 15 级。

前置任务

在配置系统环境之前，需要完成以下任务：

华为专有和保密信息
版权所有 © 华为技术有限公司

- 交换机上电自检正常

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

4.2.2 设置设备名称

设备名称可以根据需要进行更改，更改后立即生效。

背景信息

请在交换机上进行如下的配置。

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 **sysname** *host-name*，设置设备名称。

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。

缺省情况下，交换机主机名为 Quidway。

----结束

4.2.3 设置系统时钟

为了保证网络中的设备在同一时钟下工作，需要设置或更改系统时钟。

背景信息

为了保证与其他设备协调工作，需要准确设置系统的时间。S5700 支持时区和夏时制的设置。

说明

UTC（Universal Time Coordinated）指通用协调时间。

请在交换机上进行如下的配置。

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。

版权所有 © 华为技术有限公司

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。

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。

----结束

4.2.4 设置标题文本

如果用户需要对登录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。

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。

标题文本是用户在连接到交换机、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。为用户登录提供明确的指示信息时，使用此配置。

----结束

4.2.5 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

如果用户没有对某条命令单独调整过命令级别，命令级别批量提升后，原注册的所有命令行按以下原则自动调整：

- 0 级和 1 级命令保持级别不变。
- 2 级命令提升到 10 级；3 级命令提升到 15 级。
- 2 ～ 9 级和 11 ～ 14 级这些命令级别中没有命令行。用户可以单独调整命令行到这些级别中，以实现权限的精细化管理。

说明

2 级提升到 10 级，3 级提升到 15 级，并不是两次单独提升，而是一次批量提升。

请在交换机上进行如下的配置。

版权所有 © 华为技术有限公司

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 rearrange**，批量提升命令的级别。

如果用户没有设置相应切换到 15 级用户级别的密码，系统会提示用户设置 15 级用户的 super 密码，并询问用户是否继续执行命令级别提升，此时应选择“N”，设置密码。如果选择了“Y”，那么命令的级别就会直接批量提升，导致非 Console 口用户无法提升自己的级别。

步骤 3 执行命令 **command-privilege level** *level* **view** *view-name command-key*，设置命令级别。

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

4.3 配置用户的基本环境

配置用户基本配置环境，以切换用户级别。

4.3.1 建立配置任务
在进行用户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。

4.3.2 配置切换用户级别的口令
用户由低级别切换到高级别前，需要设置口令。

4.3.3 切换用户级别
用户由低级别切换到高级别，需要输入设置好的口令。

4.3.4 锁定用户界面
用户可以使用设置好的口令，锁定用户界面。

4.3.1 建立配置任务

在进行用户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

用户可以以较低级别身份登录到交换机，进行简单配置或者查看。当需要较复杂配置时，需要切换到较高级别身份。因此，需要配置用户进行此切换的基本环境。

前置任务

在配置用户的基本环境之前，需要完成以下任务：

- 交换机上电自检正常

数据准备

在配置用户的基本环境之前，需要准备以下数据。

版权所有 © 华为技术有限公司

序号	数据
1	用户级别切换密码

4.3.2 配置切换用户级别的口令

用户由低级别切换到高级别前，需要设置口令。

背景信息

如果用户以较低级别的身份登录到交换机后，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。

注意

如果使用 **simple** 选项，密码将以明文形式保存在配置文件中，以低级别登录的用户可以通过查看配置方式获取切换密码，造成安全问题。因此，一般情况下，应使用 cipher 选项，将密码加密保存。

同时，使用 **cipher** 选项设置了密码后，无法从系统取回。请妥善保管，以免遗忘或者遗失。

在交换机上进行如下的配置。

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

----结束

4.3.3 切换用户级别

用户由低级别切换到高级别，需要输入设置好的口令。

背景信息

请在交换机上进行如下的配置。

操作步骤

步骤 1 执行命令 **super** [*level*]，切换用户级别。

步骤 2 根据系统提示，输入切换口令。

如果输入的口令正确，将切换到更高级别。如果连续三次输入错误的口令，将退回用户视图，仍保持现有登录级别。

版权所有 © 华为技术有限公司

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

4.3.4 锁定用户界面

用户可以使用设置好的口令，锁定用户界面。

背景信息

在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，可以锁定用户界面。

请在交换机上进行如下的配置。

操作步骤

步骤 1 执行命令 **lock**，锁定用户界面。

步骤 2 根据系统提示，输入解除锁定的口令，并确认口令。

```
<Quidway> 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

4.4 显示系统基本配置信息

显示系统基本配置信息有相应的 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
- 显示主控板重启信息的 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。

4.4.1 显示系统配置信息
用户可以查看系统版本、系统时钟、起始配置信息、当前配置信息等信息。

4.4.2 显示系统运行状态
用户可以查看调试开关状态、当前视图的运行配置等信息。

版权所有 © 华为技术有限公司

4.4.3 收集系统诊断信息
用户可以查看系统诊断信息。

4.4.1 显示系统配置信息

用户可以查看系统版本、系统时钟、起始配置信息、当前配置信息等信息。

背景信息

已完成基本配置。

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。

----结束

4.4.2 显示系统运行状态

用户可以查看调试开关状态、当前视图的运行配置等信息。

背景信息

已完成基本配置。

操作步骤

步骤 1 执行命令 **display debugging** [**interface** *interface-type interface-number*] [*module-name*]，显示调试开关状态。

步骤 2 执行命令 **display this**，显示当前视图的运行配置。

----结束

4.4.3 收集系统诊断信息

用户可以查看系统诊断信息。

背景信息

已完成基本配置。

操作步骤

步骤 1 执行命令 **display diagnostic-information** [*file-name*]，显示系统诊断信息。

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。

华为专有和保密信息
版权所有 © 华为技术有限公司

display diagnostic-information 命令一次性收集了如下命令后的终端显示的信息，包括：**display clock**、**display version**、**display cpu-usage**、**display interface**、**display current-configuration**、**display saved-configuration**、**display history-command** 等。

----结束

版权所有 © 华为技术有限公司

5 用户管理

关于本章

用户管理包括用户界面和用户登录时的配置。

5.1 用户管理简介
用户界面和用户管理的基本概念。

5.2 通过 Console 口首次登录 S5700
介绍如何通过 Console 口登录 S5700。

5.3 配置 Console 用户界面
配置 Console 用户界面，实现在本地维护交换机。

5.4 配置 VTY 用户界面
配置 VTY 用户界面，实现在远程维护交换机。

5.5 管理用户界面
配置用户管理，保证操作用户能够安全管理交换机。

5.6 配置用户管理
配置用户管理，实现为交换机创建用户，并为用户设置口令，对用户进行管理。

5.7 配置举例
配置用户通过不同方式登录交换机的示例。配置示例中包括组网需求、配置注意事项和配置思路等。

华为专有和保密信息
版权所有 © 华为技术有限公司

5.1 用户管理简介

用户界面和用户管理的基本概念。

5.1.1 用户界面
用户界面 UI（User Interface）是 S5700 提供用户登录服务的一种视图。借助用户界面视图，可以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参数，实现对登录用户的管理、验证和验证后的授权级别。

5.1.2 用户验证
对于登录到 S5700 的用户，系统需要根据配置对其进行验证以保证系统的安全性。

5.1.1 用户界面

用户界面 UI（User Interface）是 S5700 提供用户登录服务的一种视图。借助用户界面视图，可以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参数，实现对登录用户的管理、验证和验证后的授权级别。

用户界面的类型

S5700 支持的用户界面类型如**表 5-1** 所示。

表 5-1 用户界面类型

类型	用途	说明
CON	适用于从 Console 接口进行本地登录	CON 表示一种线设备接口，符合 EIA/TIA-232 标准，接口类型为 DCE。每个设备上提供一个 Console 接口。
VTY	适用于通过 Telnet 或 SSH 方式进行本地或远程登录	VTY 是一种虚拟接口，表示逻辑终端线。当用户终端以 Telnet、FTP 或 SSH 方式登录到 S5700，就建立了一条 VTY 连接。

用户界面的编号

同一用户界面可以采用两种编号方式：相对编号和绝对编号。

- 相对编号

  相对编号是在每种类型用户界面的内部进行编号。相对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。

  用户界面的相对编号的形式为“用户界面类型+编号”。相对编号规则如下：

  - CON 的相对编号为 console0
  - VTY 缺省的相对编号分别为 vty0、vty1、vty2、vty3 和 vty4

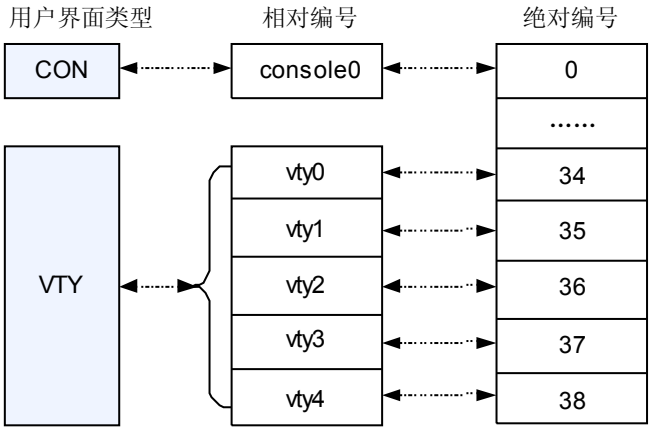
- 绝对编号

  S5700 为 CON 和各 VTY 用户界面分别指定了唯一的缺省固定编号，分别命名为 0、34、……、38，通过缺省固定编号可以进入指定的用户界面视图。

版权所有 © 华为技术有限公司

- 相对编号和绝对编号之间的关系
  同一用户界面的相对编号和绝对编号之间的对应关系如图 5-1 所示。

图 5-1 S5700 用户界面的编号



从图中可以看出，相对编号和绝对编号之间存在对应关系，例如相对编号 console0 和绝对编号 0 对应相同的用户界面，vty1 和 35 对应相同的用户界面。

说明

在 S5700 上，用户界面绝对编号的取值范围是 0、34 ~ 48。

5.1.2 用户验证

对于登录到 S5700 的用户，系统需要根据配置对其进行验证以保证系统的安全性。

首次启动 S5700 时，系统内没有预存登录验证信息，此时从 Console 接口登录 S5700 时无需用户验证。

如果不是初次登录，而是从以太网口通过 Telnet 方式登录，出于安全性考虑，需要对登录用户进行验证。只有验证通过的用户才能登录到 S5700，并进行各种配置和维护操作。

因此，需要在 S5700 上规划登录用户，为用户设置登录密码和登录级别，从而实现对登录用户的管理。

规划登录用户的类型

按照用户登录到 S5700 后获得的服务类型和权限，可以将登录用户按照表 5-2 进行划分。

表 5-2 登录用户的类型

用户类型	登录描述	用户验证需求
超级用户	从 Console 接口通过配置电缆直接登录，拥有所有权限。	初次不验证登录用户，后续建议验证。
Telnet 用户	从以太网口通过 Telnet 方式登录，拥有受控权限。在用户终端和 S5700 之间建立 Telnet 连接。	建议验证登录用户。

版权所有 © 华为技术有限公司

用户类型	登录描述	用户验证需求
SSH 用户	从以太网口通过 SSH 方式登录，拥有受控权限。在用户终端和 S5700 之间建立 SSH 连接。	建议验证登录用户。
FTP 用户	从以太网口通过 FTP 方式登录，拥有受控权限。在用户终端和 S5700 之间建立 FTP 连接。	建议验证登录用户。

用户通过 Telnet、SSH 和 FTP 等方式登录，能获得的权限取决于登录连接所在用户界面的优先级。同时，S5700 支持同一用户能同时获得多种服务。因此，需要合理的规划登录用户类型和用户级别，兼顾登录便捷性和安全性。

用户的优先级

系统支持对超级用户和 Telnet 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。

说明

如果不对用户进行优先级规划，默认用户登录级别为 0 ~ 3 级，四个级别。

用户所能访问命令的级别由用户的级别决定。

- 如果对用户采用不验证或 password 验证，登录到 S5700 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 S5700 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。

用户所能访问的命令包括用户所在用户级别的命令以及低于用户级别的命令。

例如：如果目前系统中用户级别只有 0 ～ 3 级，级别为 2 的用户可以访问级别为 0、1、2 的命令。级别为 3 的用户可以访问所有命令。

验证登录用户

在 S5700 上配置了用户后，系统会对新登录用户进行身份验证。S5700 提供了三种验证方式，如表 5-3 所示。

表 5-3 登录用户的验证方式

验证方式	登录描述
不验证	登录用户不需要输入用户名和密码，就可以直接登录 S5700。存在很大的安全隐患。
Password 验证	登录用户只需要输入密码，无需用户名，可以获得一定的安全性。
AAA 验证	登录用户需要提供用户名和密码，由 S5700 根据本地配置的用户信息进行验证。进一步改善了安全性，提供了基于用户的安全管理，适用于通过 Console 接口和 Telnet 登录的用户。

华为专有和保密信息
版权所有 © 华为技术有限公司

5.2 通过 Console 口首次登录 S5700

介绍如何通过 Console 口登录 S5700。

5.2.1 建立登录任务

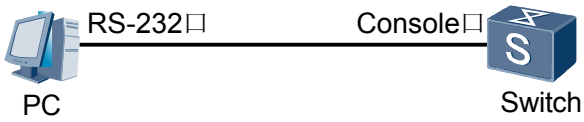
5.2.2 通过 Console 口登录 S5700

5.2.1 建立登录任务

应用环境

用户需要通过 Console 口登录到 S5700，如图 5-2 所示。图中，S5700 用 Switch 表示。

图 5-2 通过 Console 口登录到 S5700



说明

如果 S5700 是首次上电，并且用户需要管理和配置 S5700，则用户只能通过 Console 口登录到 S5700。

前置任务

在通过 Console 口登录到 S5700 前，需要完成以下任务：

- 正确连接 PC 机和 S5700
- S5700 正常启动

数据准备

无

5.2.2 通过 Console 口登录 S5700

背景信息

在通过 Console 口搭建本地配置环境时，用户可以在 PC 上通过 Windows 系统中的“超级终端”与 S5700 建立连接。

操作步骤

步骤 1 请在 PC 上启动超级终端

版权所有 © 华为技术有限公司

选择“开始 > 程序 > 附件 > 通讯 > 超级终端”菜单项，Windows 系统启动超级终端。

步骤 2 新建连接

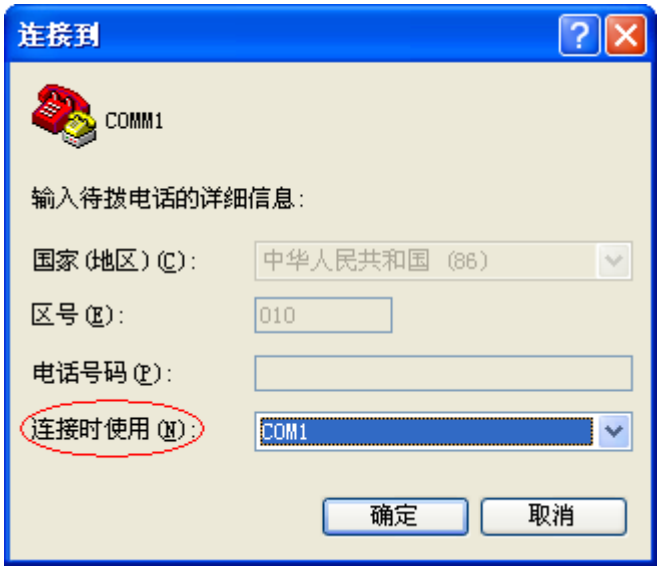
如图 5-3 所示。在“名称”文本框中输入新建连接的名称；选择图标。然后单击“确定”按钮。

图 5-3 新建连接

步骤 3 设置连接端口

进入如图 5-4 所示的 [连接到] 窗口后，请根据 PC（或配置终端）实际使用的端口在“连接时使用”下拉列表框中进行选择。然后单击“确定”按钮。

图 5-4 连接端口设置



华为专有和保密信息
版权所有 © 华为技术有限公司

步骤 4 设置通信参数

进入如图 5-5 所示的 [端口属性] 窗口后，请按表 5-4 中的描述进行通信参数的设置。

说明

在其它的 Windows 操作系统中，“每秒位数”可能被描述为“波特率”；“数据流控制”可能被描述为“流量控制”。

图 5-5 端口通信参数设置

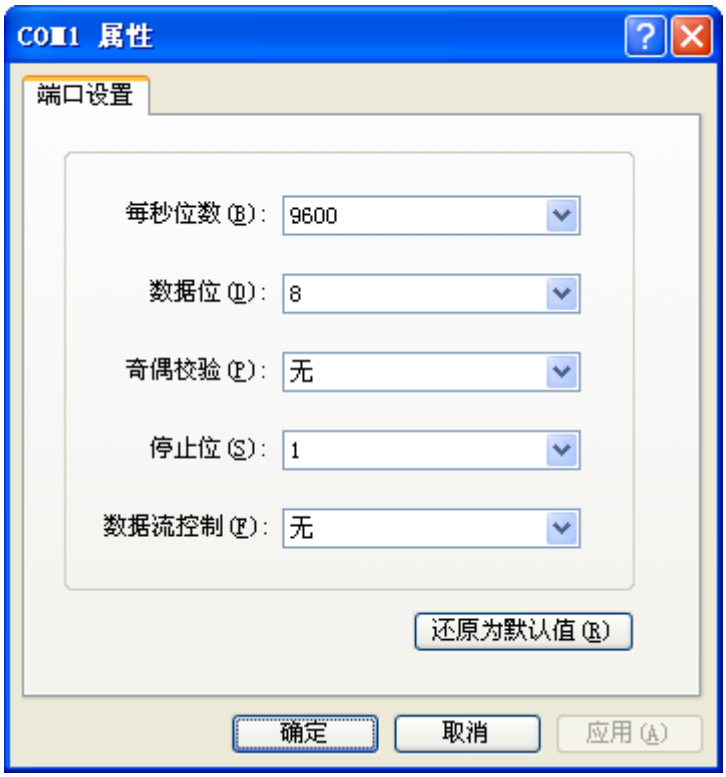


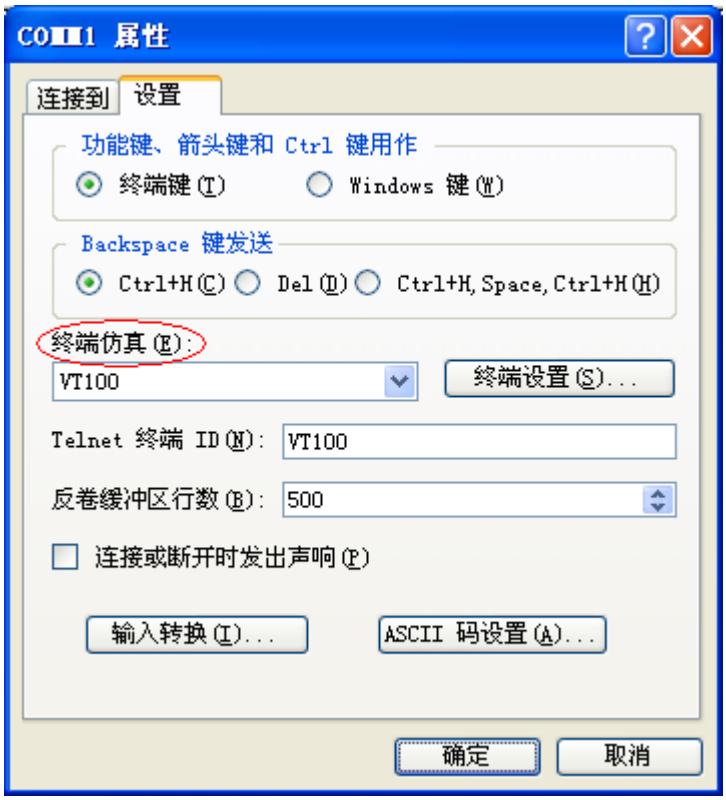
表 5-4 通信参数

参数	取值
每秒位数（波特率）	9600
数据位	8
奇偶校验	无
停止位	1
数据流控制（流量控制）	无

步骤 5 启动超级终端后，选择“文件 > 属性”菜单项，进入如图 5-6 所示的 [连接属性] 窗口。选择“设置”页签，在“终端仿真”下拉列表框中选择“自动检测”或“VT100”。单击“确定”按钮结束设置。

华为专有和保密信息
版权所有 © 华为技术有限公司

图 5-6 终端类型选择



按照以上 5 个步骤结束设置后，按下“Enter”键，屏幕出现<Quidway>提示符，表示登录到 S5700。此时就可输入命令，配置或管理 S5700。

----结束

5.3 配置 Console 用户界面

配置 Console 用户界面，实现在本地维护交换机。

5.3.1 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。

5.3.2 配置 Console 接口属性

用户可以配置 Console 接口的传输速率、流控方式、校验位、停止位和数据位。

5.3.3 配置 Console 终端属性

用户可以配置 Console 接口的用户超时断连功能、终端屏幕的显示长度以及历史命令缓冲区大小。

5.3.4 配置用户的优先级

用户可以配置通过 Console 接口登录的用户优先级。

5.3.5 配置用户验证方式

系统提供 AAA 本地验证、密码验证和不验证三种方式。

版权所有 © 华为技术有限公司

5.3.6 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。

5.3.1 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

当用户需要在本地维护交换机时，需要配置 Console 用户界面。

前置任务

在配置 Console 用户界面之前，需要完成以下任务：

- 交换机上电并启动正常
- PC 机与交换机通过异步接口连接正常

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、终端屏幕的一屏长度、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

以上数据交换机均有缺省值，一般不需要单独配置。

5.3.2 配置 Console 接口属性

用户可以配置 Console 接口的传输速率、流控方式、校验位、停止位和数据位。

背景信息

请在用户端登录到的交换机上进行如下的配置。

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

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

版权所有 © 华为技术有限公司

缺省情况下，传输速率为 9600bit/s。

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

缺省情况下，流控方式为 None。

步骤 5 （可选）执行命令 **parity** { **even** | **mark** | **none** | **odd** | **space** }，设置校验位。

缺省情况下，校验位为 None。

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

缺省情况下，数据位为 8。

说明

当用户通过 Console 接口登录交换机时，超级终端的上述属性要和交换机的接口属性保持一致，否则不能登录到交换机。

----结束

5.3.3 配置 Console 终端属性

用户可以配置 Console 接口的用户超时断连功能、终端屏幕的显示长度以及历史命令缓冲区大小。

背景信息

请在用户端登录的交换机上进行如下配置。

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 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。

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*，设置终端屏幕每屏显示的行数。

缺省情况下，终端屏幕显示的行数为 24 行。

执行命令 **screen-length** *screen-length* **temporary** 可以指定终端屏幕的临时显示行数。

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

5.3.4 配置用户的优先级

用户可以配置通过 Console 接口登录的用户优先级。

华为专有和保密信息
版权所有 © 华为技术有限公司

背景信息

请在用户端登录的交换机上进行如下配置。

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

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

用户的优先级和命令的优先级是相对应的，即用户只能使用和自己级别相对应的命令。

命令优先级请参见**命令级别**。

----结束

5.3.5 配置用户验证方式

系统提供 AAA 本地验证、密码验证和不验证三种方式。

操作步骤

- 设置 AAA 本地验证
  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 **quit**，退出 Console 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** { **simple** | **cipher** } *password*，配置本地用户名和密码。
- 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。
  4. 执行命令 **set authentication password** { **cipher** | **simple** } *password*，设置 password 验证的口令。
- 设置不对用户验证
  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 none**，设置用户验证方式为不验证。

----结束

5.3.6 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。

版权所有 © 华为技术有限公司

前提条件

已完成 Console 用户界面的所有配置。

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。
- 使用 **display access-user** 命令查看在线用户。

----结束

5.4 配置 VTY 用户界面

配置 VTY 用户界面，实现在远程维护交换机。

5.4.1 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。

5.4.2 配置 VTY 用户界面的最大个数
用户可以配置同时登录到交换机的 VTY 类型用户界面的最大个数。

5.4.3 （可选）配置呼入呼出限制
用户可以配置 VTY 类型用户界面的呼入呼出限制。

5.4.4 配置 VTY 终端属性
用户可以配置 VTY 接口的用户超时断连功能、终端屏幕的显示长度以及历史命令缓冲区的大小。

5.4.5 配置用户验证方式
系统提供 AAA 本地验证、密码验证和不验证三种方式。

5.4.6 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。

5.4.1 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

当用户需要配置和管理 Telnet 或 SSH 登录交换机时，需要配置 VTY 用户界面。

前置任务

在配置 VTY 用户界面之前，需要完成以下任务：

- 交换机上电并启动正常

版权所有 © 华为技术有限公司

- PC 机与交换机连接正常

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、终端屏幕的一屏长度和历史命令缓冲区大小
4	用户验证方式、用户名、口令

5.4.2 配置 VTY 用户界面的最大个数

用户可以配置同时登录到交换机的 VTY 类型用户界面的最大个数。

背景信息

请在用户端登录到的交换机上进行如下的配置。

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 maximum-vty** *number*，配置可以同时登录到交换机的 VTY 类型用户界面的最大个数。

说明

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）都无法登录到交换机。

如果要配置的 VTY 用户接口的最大数小于当前的最大数量，则不需要其它配置。

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，就需要为新增加的用户接口配置验证方式和密码。因为对于新增用户接口系统默认为使用密码验证。

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 就需要使用 **authentication-mode** 和 **set authentication password** 命令配置验证方式和密码，配置如下：

```
<Quidway> system-view
[Quidway] user-interface maximum-vty 15
[Quidway] user-interface vty 5 14
[Quidway-ui-vty5-14] authentication-mode password
[Quidway-ui-vty5-14] set authentication password cipher huawei
```

----结束

5.4.3 （可选）配置呼入呼出限制

用户可以配置 VTY 类型用户界面的呼入呼出限制。

版权所有 © 华为技术有限公司

背景信息

请在用户端登录到的交换机上进行如下的配置。

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** [*ui-type*] *first-ui-number* [*last-ui-number*]，进入用户界面视图。

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交换机时，使用 **inbound**；当需要限制已经登录的用户登录到其它交换机时，使用 **outbound**。

----结束

5.4.4 配置 VTY 终端属性

用户可以配置 VTY 接口的用户超时断连功能、终端屏幕的显示长度以及历史命令缓冲区的大小。

背景信息

在交换机上进行如下配置。

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** *number1* [*number2*]，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。

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

缺省情况下，终端屏幕显示的行数为 24 行。

执行命令 **screen-length** *screen-length* **temporary** 可以指定终端屏幕的临时显示行数。

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。

----结束

5.4.5 配置用户验证方式

系统提供 AAA 本地验证、密码验证和不验证三种方式。

背景信息

交换机提供三种验证方式：

- AAA 验证：需要设置用户名和密码。

版权所有 © 华为技术有限公司

- 密码验证（password)：不需要设置用户名，但一定要设置密码，否则将只能通过Console 口登录交换机。
- 不验证（none）：不需要设置用户名和密码，登录交换机时也不进行验证。

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** *number1* [*number2*]，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** { **simple** | **cipher** } *password*，配置本地用户名和密码。
- 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** *number1* [*number2*]，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。
  4. 执行命令 **set authentication password** { **cipher** | **simple** } *password*，设置密码验证的口令。
- 设置不对用户验证
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **user-interface vty** *number1* [*number2*]，进入 VTY 用户界面视图。
  3. 执行命令 **authentication-mode none**，设置用户验证方式为不验证。

----结束

5.4.6 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。

----结束

5.5 管理用户界面

配置用户管理，保证操作用户能够安全管理交换机。

版权所有 © 华为技术有限公司

5.5.1 建立配置环境
在进行管理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。

5.5.2 发送消息给其它用户界面
用户可以通过配置实现在用户界面间传递消息。

5.5.3 清除在线用户
用户可以通过配置实现清除指定的在线用户。

5.5.4 检查配置结果
管理用户界面配置成功后，可以查看用户界面的使用信息。

5.5.1 建立配置环境

在进行管理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

为了保证操作用户能够安全管理交换机，可以在用户界面间发送消息、清除指定用户等。

前置任务

在管理用户界面之前，需要完成以下任务：

- 交换机上电并正常启动
- PC 机与交换机连接正常

数据准备

在管理用户界面之前，需要准备以下数据。

序号	数据
1	用户界面类型和编号
2	要发送的消息内容

5.5.2 发送消息给其它用户界面

用户可以通过配置实现在用户界面间传递消息。

背景信息

在交换机上进行如下配置。

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。

版权所有 © 华为技术有限公司

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。

----结束

5.5.3 清除在线用户

用户可以通过配置实现清除指定的在线用户。

背景信息

在交换机上进行如下配置。

操作步骤

步骤 1 执行命令 **free user-interface** { *ui-number* | *ui-type ui-number1* }，清除在线用户。

步骤 2 根据系统提示，确定是否清除指定的在线用户。

----结束

5.5.4 检查配置结果

管理用户界面配置成功后，可以查看用户界面的使用信息。

前提条件

已完成管理用户界面的所有配置。

操作步骤

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

----结束

5.6 配置用户管理

配置用户管理，实现为交换机创建用户，并为用户设置口令，对用户进行管理。

5.6.1 建立配置任务
在进行用户管理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。

5.6.2 配置验证用户的方式
系统提供 AAA 本地验证、密码验证和不验证三种方式。

5.6.3 配置 Password 方式的口令
用户可以配置密码验证的口令，以及明文或密文的显示方式。

5.6.4 配置 AAA 方式用户名和密码
用户可以配置 AAA 本地验证的口令，以及明文或密文的显示方式。

5.6.5 配置登录不验证
用户可以配置登录交换机的方式为不验证方式。

5.6.6 设置用户的优先级

版权所有 © 华为技术有限公司

用户可以配置优先级。

5.6.7 检查配置结果
用户管理配置成功后，可以查看用户界面的使用信息、本地用户列表和在线用户等信息。

5.6.1 建立配置任务

在进行用户管理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

当配置了主控板或接口板的 IP 地址后，任何远端用户均可使用 Telnet 登录到交换机，或与交换机建立 PPP 连接而访问网络，增加了不安全性。为防止这种现象，需要为交换机创建用户，并为用户设置口令，对用户进行管理。

前置任务

在配置用户之前，需要完成以下任务：

- 交换机上电并正常启动
- PC 机与交换机连接正常

数据准备

在配置用户之前，需要准备以下数据。

序号	数据
1	验证用户的方式
2	用户名和口令
3	用户优先级

5.6.2 配置验证用户的方式

系统提供 AAA 本地验证、密码验证和不验证三种方式。

背景信息

请在用户端需要登录的交换机上进行如下的配置。

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** [*ui-type*] *first-ui-number* [*last-ui-number*]，进入用户界面视图。

步骤 3 执行命令 **authentication-mode** { **aaa** | **password** | **none** }，设置用户验证方式。

----结束

版权所有 © 华为技术有限公司

5.6.3 配置 Password 方式的口令

用户可以配置密码验证的口令，以及明文或密文的显示方式。

背景信息

请在用户端需要登录的交换机上进行如下的配置。

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** [*ui-type*] *first-ui-number* [*last-ui-number*]，进入用户界面视图。

步骤 3 执行命令 **authentication-mode password**，设置用户验证方式为 Password 验证。

步骤 4 执行命令 **set authentication password** { **cipher** | **simple** } *password*，设置密码验证的密文口令或明文口令。

说明

交换机默认的验证方式是密码验证。

----结束

5.6.4 配置 AAA 方式用户名和密码

用户可以配置 AAA 本地验证的口令，以及明文或密文的显示方式。

背景信息

请在用户端需要登录的交换机上进行如下的配置。

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** [*ui-type*] *first-ui-number* [*last-ui-number*]，进入用户界面视图。

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

步骤 4 执行命令 **quit**，返回系统视图。

步骤 5 执行命令 **aaa**，进入 AAA 视图。

步骤 6 执行命令 **local-user** *user-name* **password** { **simple** | **cipher** } *password*，配置本地用户名和密码。

----结束

5.6.5 配置登录不验证

用户可以配置登录交换机的方式为不验证方式。

版权所有 © 华为技术有限公司

背景信息

注意

设置登录方式为不验证，会引起交换机的安全问题。

请在用户端需要登录的交换机上进行如下的配置。

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** [*ui-type*] *first-ui-number* [*last-ui-number*]，进入用户界面视图。

步骤 3 执行命令 **authentication-mode none**，配置用户登录不验证。

说明

- 如果配置的验证方式为采用不验证或 password 验证，则用户登录到系统后所能访问的命令级别由用户界面的优先级确定。
- 如果配置的验证方式需要用户名和口令，则用户登录系统后所能访问的命令级别由用户的优先级确定。

----结束

5.6.6 设置用户的优先级

用户可以配置优先级。

背景信息

具体请参见《Quidway S5700 系列 以太网交换机 配置指南-安全》。

5.6.7 检查配置结果

用户管理配置成功后，可以查看用户界面的使用信息、本地用户列表和在线用户等信息。

前提条件

已完成用户管理的所有配置。

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 local-user** 命令查看本地用户列表。
- 使用 **display access-user** 命令查看在线用户。

----结束

版权所有 © 华为技术有限公司

5.7 配置举例

配置用户通过不同方式登录交换机的示例。配置示例中包括组网需求、配置注意事项和配置思路等。

背景信息

注意

以下第一个和第二个配置举例执行完毕后，当前用户 VTY0，不能对设备进行优先级为 2 以上的配置命令的操作，请确认可以通过其他方式登录交换机并删除配置。

5.7.1 配置用户通过 Password 方式登录交换机示例
配置通过 Password 方式登录交换机的示例。在本示例中，通过配置 VTY0 的优先级、验证方式和断开连接的时间，实现使用 Password 方式登录交换机。

5.7.2 配置用户通过 AAA 方式登录交换机示例
配置通过 AAA 方式登录交换机的示例。在本示例中，通过配置 VTY0 的优先级、断开连接的时间以及打开本地用户的闲置切断开关等操作，实现使用 AAA 方式登录交换机。

5.7.1 配置用户通过 Password 方式登录交换机示例

配置通过 Password 方式登录交换机的示例。在本示例中，通过配置 VTY0 的优先级、验证方式和断开连接的时间，实现使用 Password 方式登录交换机。

组网需求

PC 机的 COM 口与交换机的 Console 口相连。

配置 VTY0 的优先级为 2，对从 VTY0 登录的用户进行 password 验证，用户登录时需要输入口令“huawei”。

登录后，如果用户超过 30 分钟未对交换机进行操作，将断开与交换机的连接。

配置思路

采用如下的思路配置登录交换机：

1. 进入用户接口视图，配置 VTY0 的优先级为 2。
2. 配置明文验证和断开连接的时间。

数据准备

为完成此配置例，需准备如下的数据：

- 验证方式密码
- 断开连接的时间

版权所有 © 华为技术有限公司

操作步骤

步骤 1 配置 VTY0 的优先级为 2。

```
<Quidway> system-view
[Quidway] user-interface vty0
[Quidway-ui-vty0] user privilege level 2
```

步骤 2 配置明文验证和断开连接的时间。

```
[Quidway-ui-vty0] authentication-mode password
[Quidway-ui-vty0] set authentication password simple huawei
[Quidway-ui-vty0] idle-timeout 30
```

----结束

配置文件

```
#
 sysname Quidway
#
aaa
 authentication-scheme default
 #
 authorization-scheme default
 #
 accounting-scheme default
 #
 domain default
#
user-interface vty 0
 user privilege level 2
 set authentication password simple huawei
 idle-timeout 30
#
return
```

5.7.2 配置用户通过 AAA 方式登录交换机示例

配置通过 AAA 方式登录交换机的示例。在本示例中，通过配置 VTY0 的优先级、断开连接的时间以及打开本地用户的闲置切断开关等操作，实现使用 AAA 方式登录交换机。

组网需求

PC 机的 COM 口与交换机的 Console 口相连。

配置 VTY0 的优先级为 2，对从 VTY0 登录的用户进行 AAA 验证，用户登录时需要输入用户名“huawei”，密码“huawei”。

登录后，如果用户超过 30 分钟未对交换机进行操作，将断开与交换机的连接。

配置思路

采用如下的思路配置登录交换机：

1. 进入用户接口视图，配置 VTY0 的优先级为 2 和断开连接的时间。
2. 进入 AAA 视图，配置用户名、密码和用户等级。
3. 在 AAA 视图下打开本地用户的闲置切断开关。

数据准备

为完成此配置例，需准备如下的数据：

华为专有和保密信息
版权所有 © 华为技术有限公司

- 验证时需要的用户名和密码
- 断开连接的时间

操作步骤

步骤 1 交换机上配置 VTY0 的优先级为 2，验证方式为 aaa，断开连接时间为 30 分钟。

```
<Quidway> system-view
[Quidway] user-interface vty0
[Quidway-ui-vty0] user privilege level 2
[Quidway-ui-vty0] authentication-mode aaa
[Quidway-ui-vty0] idle-timeout 30
[Quidway-ui-vty0] quit
```

步骤 2 配置用户名、密码和用户等级。

```
[Quidway] aaa
[Quidway-aaa] local-user huawei password cipher huawei
[Quidway-aaa] local-user huawei privilege level 2
```

----结束

配置文件

```
#
 sysname Quidway
#
aaa
local-user huawei password cipher N`C55QK<`=/Q=^Q`MAF4<1!!
 local-user huawei privilege level 2
 #
 authorization-scheme default
 #
 accounting-scheme default
 #
 domain default
#
user-interface vty 0
 authentication-mode aaa
 user privilege level 2
 idle-timeout 30
#
return
```


版权所有 © 华为技术有限公司

6 管理文件系统

关于本章

介绍了文件系统的基础知识，主要包括管理文件、管理目录和管理存储设备的方法。

6.1 文件系统简介
简单介绍文件系统的概念。

6.2 管理存储设备
介绍格式化存储设备的方法。

6.3 管理目录
可以通过管理目录在逻辑上将文件分级存放。

6.4 管理文件
可以通过管理文件，对其进行查看、删除、重命名等操作。

版权所有 © 华为技术有限公司

6.1 文件系统简介

简单介绍文件系统的概念。

基本概念

文件系统包括对存储设备中的文件、目录的管理，包括创建文件系统，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。

存储设备

存储设备是指用于存储数据的硬件。

S5700 目前支持的存储设备为 Flash Memory。

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，目录是文件逻辑上的容器。

6.2 管理存储设备

介绍格式化存储设备的方法。

6.2.1 建立配置任务
需要清空 S5700 的信息时，可以对存储设备进行格式化。

6.2.2 （可选）格式化存储设备
格式化会清空存储器中的所有文件和目录。

6.2.1 建立配置任务

需要清空 S5700 的信息时，可以对存储设备进行格式化。

前置任务

在配置管理存储设备之前，需要完成以下任务：

- S5700 安装完毕并加电启动正常
- 客户端可以登录到 S5700 上

数据准备

在配置管理存储设备之前，需要准备以下数据。

版权所有 © 华为技术有限公司

序号	数据
1	设备的名称

6.2.2 （可选）格式化存储设备

格式化会清空存储器中的所有文件和目录。

背景信息

说明

执行 **format flash:**命令后，S5700 会清空 Flash 存储器中的所有文件和目录，并且不可恢复，请谨慎使用此命令！

操作步骤

步骤 1 在用户视图下执行 **format flash:**命令，格式化存储设备。

----结束

6.3 管理目录

可以通过管理目录在逻辑上将文件分级存放。

6.3.1 建立配置任务
在管理目录之前，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。

6.3.2 查看当前的工作目录
当需要了解当前所在的目录节点信息时，可以进行查看当前工作目录的操作。

6.3.3 改变当前目录
当需要变更到别的目录节点时，可以进行改变当前目录的操作。

6.3.4 显示目录或文件信息
当需要查看某一目录及该目录下的文件时，可以进行显示目录或文件信息的操作。

6.3.5 创建目录
当希望新建一个目录时，可以进行创建目录的操作，在指定存储设备的指定目录下创建目录。

6.3.6 删除目录
当需要舍弃某一目录时，可以进行删除目录的操作。

6.3.1 建立配置任务

在管理目录之前，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

当需要在客户端与服务器端进行文件传输时，需要使用文件系统对目录进行配置。

版权所有 © 华为技术有限公司

前置任务

在配置文件系统的基本功能之前，需要完成以下任务：

- 交换机安装完毕并上电启动正常
- 已正确连接客户端与服务器端

数据准备

在配置管理目录的基本功能之前，需要准备以下数据。

序号	数据
1	需要创建的目录名
2	需要删除的目录名

6.3.2 查看当前的工作目录

当需要了解当前所在的目录节点信息时，可以进行查看当前工作目录的操作。

背景信息

请在交换机上进行如下配置。

操作步骤

步骤 1 执行命令 **pwd**，屏幕上显示当前所处的目录。

----结束

6.3.3 改变当前目录

当需要变更到别的目录节点时，可以进行改变当前目录的操作。

背景信息

请在交换机上进行如下配置。

操作步骤

步骤 1 执行命令 **cd** *directory*，改变当前所处的目录。

步骤 2 执行命令 **pwd**，查看当前所处的目录。

----结束

6.3.4 显示目录或文件信息

当需要查看某一目录及该目录下的文件时，可以进行显示目录或文件信息的操作。

版权所有 © 华为技术有限公司

背景信息

请在交换机上进行如下配置。

操作步骤

步骤 1 执行命令 **cd** *directory*，进入想要显示的文件所在的目录。

步骤 2 执行命令 **dir** [**/all**] [*filename* | **flash:**]，显示目录中的文件和子目录的列表。

所有路径都支持绝对路径或相对于当前工作路径的相对路径。

----结束

6.3.5 创建目录

当希望新建一个目录时，可以进行创建目录的操作，在指定存储设备的指定目录下创建目录。

背景信息

请在交换机上进行如下配置。

操作步骤

步骤 1 执行命令 **cd** *directory*，改变当前目录到所要创建目录的父目录。

步骤 2 执行命令 **mkdir** *directory*，创建目录。

----结束

6.3.6 删除目录

当需要舍弃某一目录时，可以进行删除目录的操作。

背景信息

请在交换机上进行如下配置。

操作步骤

步骤 1 执行命令 **cd** *directory*，改变当前目录到所要删除目录的父目录。

步骤 2 执行命令 **rmdir** *directory*，删除目录。

----结束

6.4 管理文件

可以通过管理文件，对其进行查看、删除、重命名等操作。

6.4.1 建立配置任务
在管理文件之前，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。

版权所有 © 华为技术有限公司

6.4.2 显示文件的内容
当需要查看文件内容时，可以进行显示文件内容的操作，系统将以文本形式显示。

6.4.3 拷贝文件
当需要复制某一文件时，可以进行拷贝文件的操作。

6.4.4 移动文件
当需要将文件转移存放路径时，可以进行移动文件的操作。

6.4.5 重新命名文件
当需要修改某一文件名称时，可以进行重新命名文件的操作。

6.4.6 压缩文件
当需要减小某一文件大小时，可以进行压缩文件的操作。

6.4.7 删除文件
当需要丢弃某一文件时，可以进行删除文件的操作。

6.4.8 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。

6.4.9 恢复删除文件
当需要还原某一已丢弃的文件时，可以进行恢复删除文件的操作。

6.4.10 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。

6.4.11 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。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。

6.4.1 建立配置任务

在管理文件之前，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

如需要查看、删除、重命名交换机上的文件时，需要使用文件系统对文件进行配置。

前置任务

在配置文件系统之前，需要完成以下任务：

- 交换机安装完毕并上电启动正常
- 已正确连接客户端与服务器端

数据准备

在配置文件系统之前，需要准备以下数据。

序号	数据
1	需要查看的文件名
2	需要删除的文件名

华为专有和保密信息
版权所有 © 华为技术有限公司

6.4.2 显示文件的内容

当需要查看文件内容时，可以进行显示文件内容的操作，系统将以文本形式显示。

操作步骤

步骤 1 执行命令 **cd** *directory*，改变当前目录到文件所处的目录。

步骤 2 执行命令 **more** *filename*，显示文件的内容。

----结束

6.4.3 拷贝文件

当需要复制某一文件时，可以进行拷贝文件的操作。

背景信息

请在交换机上进行如下的配置。

操作步骤

步骤 1 执行命令 **cd** *directory*，改变当前目录到文件所处的目录。

步骤 2 执行命令 **copy** *source-filename destination-filename*，拷贝文件。

说明

拷贝的文件必须大于 0 字节，否则不能执行。

----结束

6.4.4 移动文件

当需要将文件转移存放路径时，可以进行移动文件的操作。

背景信息

请在交换机上进行如下的配置。

操作步骤

步骤 1 执行命令 **cd** *directory*，改变当前目录到文件所处的目录。

步骤 2 执行命令 **move** *source-filename destination-filename*，移动文件。

----结束

6.4.5 重新命名文件

当需要修改某一文件名称时，可以进行重新命名文件的操作。

背景信息

请在交换机上进行如下的配置。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 执行命令 **cd** *directory*，改变当前目录到文件所处的目录。

步骤 2 执行命令 **rename** *source-filename destination-filename*，重新命名文件。

----结束

6.4.6 压缩文件

当需要减小某一文件大小时，可以进行压缩文件的操作。

操作步骤

步骤 1 执行命令 **zip** *source-filename destination-filename*，压缩文件。

----结束

6.4.7 删除文件

当需要丢弃某一文件时，可以进行删除文件的操作。

背景信息

请在交换机上进行如下的配置。

操作步骤

步骤 1 执行命令 **cd** *directory*，改变当前目录到文件所处的目录。

步骤 2 执行命令 **delete** [**/unreserved**] *filename*，删除文件。

----结束

6.4.8 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。

背景信息

请在交换机上进行如下的配置。

操作步骤

步骤 1 执行命令 **reset recycle-bin** [*filename*]，删除文件。

----结束

6.4.9 恢复删除文件

当需要还原某一已丢弃的文件时，可以进行恢复删除文件的操作。

背景信息

请在交换机上进行如下的配置。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 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。
- 对于执行删除命令行时使用参数[**/unreserved**]后的文件不可恢复。

----结束

6.4.10 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。

前提条件

在客户端编辑的批处理文件，已经上传到交换机。

背景信息

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。

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 **execute** *filename*，运行批处理文件。

----结束

6.4.11 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。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。

前提条件

在配置文件系统之前，需要完成以下任务：

- 交换机安装完毕并上电启动正常
- 客户端可以登录到交换机上

背景信息

在操作文件时，如可能导致数据丢失或破坏，则需配置系统给出提示信息。

操作步骤

步骤 1 执行 **system-view** 命令，进入到系统视图。

步骤 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**。

版权所有 © 华为技术有限公司

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

华为专有和保密信息
版权所有 © 华为技术有限公司

7 管理配置文件

关于本章

管理配置文件包括当前配置和配置文件，以及主备配置一致性检测和恢复。

7.1 管理配置文件简介
配置文件是本次或下次启动交换机时加载的配置项。

7.2 管理配置文件
管理配置文件，保证交换机正常启动。

版权所有 © 华为技术有限公司

7.1 管理配置文件简介

配置文件是本次或下次启动交换机时加载的配置项。

7.1.1 配置文件
配置文件的基本概念。

7.1.2 配置文件和当前配置
配置文件和当前配置的基本概念。

7.1.1 配置文件

配置文件的基本概念。

配置文件是本次或下次启动交换机时加载的配置项。

配置文件为一文本文件，其格式如下：

- V100R005 版本的配置文件必须以类似“!Software Version V100R005C01SPC001”的版本信息开头。
- 以命令格式保存。
- 为了节省空间，只保存非缺省的参数（各配置参数的缺省值请详见以后各章节）。
- 命令的组织以命令视图为基本框架，同一命令视图的命令组织在一起，形成一节，节与节之间通常用空行或注释行隔开（以#开始的为注释行）。空行或注释行可以是一行或多行。
- 节的顺序安排通常为：全局配置、物理接口配置、逻辑接口配置、路由协议配置等。

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。
- 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。

7.1.2 配置文件和当前配置

配置文件和当前配置的基本概念。

- 起始配置：交换机上电时，从默认存储路径中读取配置文件进行交换机的初始化工作，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，则交换机用缺省参数初始化。
- 当前配置：与起始配置相对应，交换机运行过程中正在生效的配置称为当前配置。
- 用户通过命令行接口可以修改交换机当前配置，为了使当前配置能够作为交换机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

管理配置文件，保证交换机正常启动。

7.2.1 建立配置任务

华为专有和保密信息
版权所有 © 华为技术有限公司

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。

7.2.2 配置交换机下次启动时加载的系统软件
用户在需要升级设备的系统软件等情况时，可以指定交换机下次启动时加载的系统软件。

7.2.3 配置交换机下次启动时加载的配置文件
用户在重启设备之前，可以指定交换机下次启动时加载的配置文件。

7.2.4 保存配置文件
为了降低由于交换机掉电或者意外重启导致配置信息的丢失，系统提供实时保存配置的功能。

7.2.5 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，也可以清除指定的不在位单板的非激活配置信息。

7.2.6 比较配置文件
用户可以比较当前配置和初始配置。

7.2.7 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、交换机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。

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

如下情况下，用户会进行管理配置文件的操作。

- 为了让交换机正常启动，用户需要正确选择交换机在启动时加载的 S5700 系统软件和配置文件。
- 用户在修改当前配置后，需要保存修改的内容。
- 用户需要查看交换机的配置信息。

前置任务

在对配置文件进行管理之前，需要完成以下任务：

- 交换机安装完毕并上电启动正常

数据准备

管理配置文件之前，需准备以下数据。

序号	数据
1	S5700 系统软件及其文件名
2	配置文件及其文件名

版权所有 © 华为技术有限公司

序号	数据
3	配置文件比较的开始行数

7.2.2 配置交换机下次启动时加载的系统软件

用户在需要升级设备的系统软件等情况时，可以指定交换机下次启动时加载的系统软件。

背景信息

请在交换机上进行如下配置。

操作步骤

步骤 1 在用户视图下执行命令 **startup system-software** *system-filename* [**all** | **slave-board** | **slot** *slot-id*]，配置交换机下次启动时加载的 S5700 系统软件。

系统软件的文件名必须以“.cc”作为扩展名，而且必须存放在 Flash 的根目录下。

指定 S5700 下次启动加载的系统文件时，如果待升级的软件对应的 BOOTROM 版本和当前设备 BOOTROM 版本不一致，设备会自动提醒升级设备 BOOTROM。

----结束

7.2.3 配置交换机下次启动时加载的配置文件

用户在重启设备之前，可以指定交换机下次启动时加载的配置文件。

背景信息

V100R005 版本的配置文件必须以类似“!Software Version V100R005C01SPC001”的版本信息开头。

请在交换机上进行如下配置。

操作步骤

步骤 1 执行 **startup saved-configuration** *configuration-file* 命令，配置交换机下次启动时加载的配置文件。

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。

交换机上电时，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，则交换机用缺省参数初始化。

与初始配置相对应，交换机运行过程中正在生效的配置称为当前配置。

----结束

版权所有 © 华为技术有限公司

7.2.4 保存配置文件

为了降低由于交换机掉电或者意外重启导致配置信息的丢失，系统提供实时保存配置的功能。

操作步骤

- 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交换机的当前配置，为了使当前配置能够作为交换机下次上电时的初始配置，需要用 **save** 命令保存当前配置到 Flash 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。

  说明

  在第一次保存配置文件时，如果不指定可选参数 *configuration-file*，则交换机将提示是否将文件名保存为“vrpcfg.zip”。

----结束

7.2.5 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，也可以清除指定的不在位单板的非激活配置信息。

背景信息

- 在交换机软件升级之后，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。

要清除配置文件，需要在交换机上进行如下配置。

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。

  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，则交换机下次启动时，将采用缺省的配置参数进行初始化。
- 在系统视图下，执行命令 **clear inactive-configuration slot** *slot-id*，清除指定的不在位单板的非激活配置信息。

----结束

7.2.6 比较配置文件

用户可以比较当前配置和初始配置。

版权所有 © 华为技术有限公司

背景信息

在交换机上进行如下配置。

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 150 个字符），如果该不同之处到文件末尾不足 150 个字符，将显示到文件尾为止。

比较当前配置和下次配置文件时，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

7.2.7 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、交换机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** 命令查看当前配置文件。
- 使用 **display saved-configuration** [**last**]命令配置交换机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。
- 使用 **dir** [**/all**] [*filename*]命令查看存储设备中的文件信息。

----结束

任务示例

在配置成功时，执行上面的命令，应能得到如下的结果：

- 交换机的当前配置信息正确，无多余配置。
- 交换机的当前配置信息已经被保存在存储设备中。
- 交换机下次启动时加载的 S5700 系统软件和配置文件正确，且已经保存在存储设备的根目录中。

版权所有 © 华为技术有限公司

8 FTP 和 TFTP

关于本章

FTP 和 TFTP 是常用的文件传输协议。

8.1 FTP 和 TFTP 简介
介绍 FTP 和 TFTP 的基本概念。

8.2 配置交换机作为 FTP 服务器
配置 FTP 服务器的基本功能。

8.3 配置 FTP 访问控制列表
配置 FTP 访问控制列表，实现只允许指定的客户端登录到交换机。

8.4 配置交换机作为 FTP 客户端
配置交换机作为 FTP 客户端，登录 FTP 服务器。

8.5 配置交换机作为 TFTP 客户端
配置交换机作为 TFTP 客户端，登录 TFTP 服务器。

8.6 限制对 TFTP 服务器的访问
配置限制客户端登录 TFTP 交换机，实现允许本设备以 TFTP 方式登录到哪些 TFTP 服务器。

8.7 配置举例
通过示例介绍 FTP 和 TFTP 的常见应用。

版权所有 © 华为技术有限公司

8.1 FTP 和 TFTP 简介

介绍 FTP 和 TFTP 的基本概念。

8.1.1 FTP
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。

8.1.2 TFTP
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。

8.1.1 FTP

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。

FTP（File Transfer Protocol）在 TCP/IP 协议族中属于应用层协议，主要向用户提供本地与远程主机之间的文件传输。FTP 协议基于相应的文件系统实现。

系统提供的 FTP 服务包括：

- FTP Server：用户可以运行 FTP 客户端程序登录到交换机，访问交换机上的文件。
- FTP Client：用户在 PC 上通过终端仿真程序或 Telnet 程序建立与交换机的连接后，可以输入 FTP 命令建立与远程 FTP Server 的连接并访问远程主机上的文件。

8.1.2 TFTP

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。

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，S5700 只能作为 TFTP 客户端，且只能使用二进制模式传输文件。

8.2 配置交换机作为 FTP 服务器

配置 FTP 服务器的基本功能。

版权所有 © 华为技术有限公司

8.2.1 建立配置任务
在进行交换机作为 FTP 服务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。

8.2.2 （可选）指定 FTP 服务器端口号
用户可以配置或变更 FTP 服务器监听端口号。变更后，只有用户知道 FTP 服务使用的当前端口号，确保安全性。

8.2.3 使能 FTP 服务器
缺省情况下 FTP 服务器功能关闭，使用 FTP 功能之前需要首先使能 FTP 服务器。

8.2.4 （可选）配置 FTP 服务器超时断开连接的时间
用户可以配置 FTP 连接空闲时间，长时间没有操作的时候释放 FTP 连接资源。

8.2.5 配置本地用户名和口令
用户可以配置 FTP 用户的验证信息，保证安全性，无权限的用户将不能操作设备。

8.2.6 配置服务类型及授权信息
用户可以配置 FTP 用户的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。

8.2.7 检查配置结果
交换机作为 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。

8.2.1 建立配置任务

在进行交换机作为 FTP 服务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

把交换机作为 FTP 服务器。客户端通过 FTP 登录到交换机以后，可以在客户端与服务器端之间实现远程传输文件。

前置任务

在配置交换机作为 FTP 服务器之前，需要完成以下任务：

- 交换机安装完毕并上电启动正常
- 客户端与交换机路由可达

数据准备

如果配置交换机作为 FTP 服务器，需要准备以下数据。

序号	数据
1	（可选）FTP 服务器指定监听端口号
2	（可选）FTP 服务器的超时断开连接时间
3	FTP 用户名和口令
4	FTP 用户的授权工作目录

版权所有 © 华为技术有限公司

8.2.2 （可选）指定 FTP 服务器端口号

用户可以配置或变更 FTP 服务器监听端口号。变更后，只有用户知道 FTP 服务使用的当前端口号，确保安全性。

背景信息

FTP 服务未使能情况下，可以按照用户指定端口进行 FTP 端口变更。

如果变更端口前 FTP 服务已经启动，需执行 **undo ftp server** 命令关闭 FTP 服务，再进行端口变更。

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。缺省情况下，FTP 服务器端监听端口号是 21。

----结束

8.2.3 使能 FTP 服务器

缺省情况下 FTP 服务器功能关闭，使用 FTP 功能之前需要首先使能 FTP 服务器。

背景信息

请在作为 FTP 服务器的交换机上进行如下的配置。

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。

----结束

8.2.4 （可选）配置 FTP 服务器超时断开连接的时间

用户可以配置 FTP 连接空闲时间，长时间没有操作的时候释放 FTP 连接资源。

背景信息

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。

请在作为 FTP 服务器的交换机上进行如下的配置。

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**] **timeout** *minutes*，配置 FTP 服务器超时断连时间。

版权所有 © 华为技术有限公司

缺省情况下，系统的连接空闲时间为 30 分钟。

----结束

8.2.5 配置本地用户名和口令

用户可以配置 FTP 用户的验证信息，保证安全性，无权限的用户将不能操作设备。

背景信息

请在作为 FTP 服务器的交换机上进行如下的配置。

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** { **simple** | **cipher** } *password*，配置本地用户名和密码。

----结束

8.2.6 配置服务类型及授权信息

用户可以配置 FTP 用户的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

请在作为 FTP 服务器的交换机上进行如下的配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 （可选）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* **service-type ftp**，配置 FTP 服务类型。

步骤 5 执行命令 **local-user** *user-name* **ftp-directory** *directory*，配置 FTP 用户的授权目录。

----结束

8.2.7 检查配置结果

交换机作为 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

已完成交换机作为 FTP 服务器的所有配置

版权所有 © 华为技术有限公司

背景信息

- 使用 **display [ipv6] ftp-server** 命令查看 FTP 服务器的配置和状态信息。
- 使用 **display ftp-users** 命令查看登录的 FTP 用户信息。

任务示例

配置 FTP 服务器完毕，执行命令 **display [ipv6] ftp-server**，可以看到 FTP 服务器正在运行。

```
<Quidway> display ftp-server
  FTP server is running
  Max user number                5
  User count                     0
  Timeout value(in minute)       30
  Listening Port                 1080
  Acl number                     0
```

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。

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

8.3 配置 FTP 访问控制列表

配置 FTP 访问控制列表，实现只允许指定的客户端登录到交换机。

8.3.1 建立配置任务
在进行 FTP 访问控制列表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。

8.3.2 使能 FTP 服务器
FTP 服务器缺省情况下关闭，使用 FTP 功能之前需要首先使能 FTP 服务器。

8.3.3 配置基本访问控制列表
用户可以配置 ACL 规则。使用源地址信息，作为定义 ACL 规则的信息。

8.3.4 配置 FTP 基本访问控制列表
用户可以配置 FTP 基本访问控制列表。

8.3.5 检查配置结果
FTP 访问控制列表配置成功后，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。

8.3.1 建立配置任务

在进行 FTP 访问控制列表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

当交换机作为 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。

华为专有和保密信息
版权所有 © 华为技术有限公司

前置任务

在配置 FTP 访问控制列表之前，需要完成以下任务：

- 交换机安装完毕并上电启动正常
- 客户端和作为 FTP 服务器的交换机路由可达。

数据准备

在配置 FTP 访问控制列表之前，需要准备以下数据。

序号	数据
1	访问控制列表号

8.3.2 使能 FTP 服务器

FTP 服务器缺省情况下关闭，使用 FTP 功能之前需要首先使能 FTP 服务器。

背景信息

请在作为 FTP 服务器的交换机上进行如下的配置。

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。

----结束

8.3.3 配置基本访问控制列表

用户可以配置 ACL 规则。使用源地址信息，作为定义 ACL 规则的信息。

背景信息

请在作为 FTP 服务器的交换机上进行如下的配置。

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** | **logging** | **source** { *source-address source-wildcard* | **any** } | **time-range** *time-name*] *，配置 ACL 规则。

说明

FTP 只支持基本访问控制列表。

----结束

版权所有 © 华为技术有限公司

8.3.4 配置 FTP 基本访问控制列表

用户可以配置 FTP 基本访问控制列表。

背景信息

请在作为 FTP 服务器的交换机上进行如下的配置。

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**] **acl** *acl-number*，配置 FTP 基本访问控制列表。

----结束

8.3.5 检查配置结果

FTP 访问控制列表配置成功后，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 FTP 访问控制列表的所有配置

操作步骤

- 使用 **display** [**ipv6**] **ftp-server** 命令查看 FTP 服务器的配置和状态信息。

----结束

任务示例

配置 FTP 服务器完毕，执行命令 **display** [**ipv6**] **ftp-server**，可以看到 FTP 基本访问控制列表号是 2345。

```
<Quidway> display ftp-server
  FTP server is running
  Max user number              5
  User count                   0
  Timeout value(in minute)     30
  Listening Port               1080
  Acl number                   2345
```

8.4 配置交换机作为 FTP 客户端

配置交换机作为 FTP 客户端，登录 FTP 服务器。

8.4.1 建立配置任务
在进行交换机作为 FTP 客户端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。

8.4.2 登录 FTP 服务器
用户视图和 FTP 视图下，用户均可以登录 FTP 服务器。

8.4.3 配置文件传输方式

华为专有和保密信息
版权所有 © 华为技术有限公司

用户可以配置传输的文件的数据类型和文件传输方式。

8.4.4 查看 FTP 命令的在线帮助
用户可以在 FTP 客户端视图下查看 FTP 命令的在线帮助。

8.4.5 上传、下载文件
用户可以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。

8.4.6 管理目录
用户可以在 FTP 服务器上进行创建、删除目录等管理操作。

8.4.7 管理文件
用户可以显示 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。

8.4.8 更改登录用户
用户可以更改当前的登录用户，重新进行登录 FTP 服务器。

8.4.9 断开 FTP 连接
用户可以终止与服务器的连接，并退回到用户视图或 FTP 视图。

8.4.10 检查配置结果
交换机作为 FTP 客户端配置成功后，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。

8.4.1 建立配置任务

在进行交换机作为 FTP 客户端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

可以配置交换机作为 FTP 客户端，然后从交换机登录到 FTP 服务器，执行诸如传输文件、管理服务器目录等操作。

前置任务

在配置交换机作为 FTP 客户端之前，需要完成以下任务：

- 交换机安装完毕并上电启动正常
- 交换机与服务器路由可达

数据准备

如果配置交换机作为 FTP 客户端，需要准备以下数据：

序号	数据
1	FTP 服务器的主机名或 IP 地址
2	建立 FTP 连接使用的端口号
3	FTP 协议命令
4	本地的文件名和远程 FTP 服务器上的文件名

版权所有 © 华为技术有限公司

序号	数据
5	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
6	登录时需要的用户名及密码

8.4.2 登录 FTP 服务器

用户视图和 FTP 视图下，用户均可以登录 FTP 服务器。

背景信息

请在作为客户端的交换机上进行如下的配置。

在不同的视图下，与 FTP 服务器建立连接的方式也不同。

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。
    - 用户视图下，建立与 FTP 服务器的连接。

      执行命令 **ftp** [*host* [*port-number*] [**public-net** | **vpn-instance** *vpn-instance-name*]，与 FTP 服务器建立连接。
    - FTP 视图下，建立与 FTP 服务器的连接。
      1. 执行命令 **ftp**，进入 FTP 视图。
      2. 执行命令 **open** *host* [*port-number*] [**public-net** | **vpn-instance** *vpn-instance-name*]，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。
  - 服务器端是 IPv6 地址。
    - 用户视图下，建立与 FTP 服务器的连接。

      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。
      1. 执行命令 **ftp**，进入 FTP 视图。
      2. 执行命令 **open ipv6** *host* [*port-number*]，与 FTP 服务器建立连接。

----结束

8.4.3 配置文件传输方式

用户可以配置传输的文件的数据类型和文件传输方式。

背景信息

请在作为客户端的交换机上进行如下的配置。

华为专有和保密信息
版权所有 © 华为技术有限公司

操作步骤

步骤 1 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。
  - 用户视图下，建立与 FTP 服务器的连接。

    执行命令 **ftp** [*host* [*port-number*] [**public-net** | **vpn-instance** *vpn-instance-name*]，与 FTP 服务器建立连接。
  - FTP 视图下，建立与 FTP 服务器的连接。
    1. 执行命令 **ftp**，进入 FTP 视图。
    2. 执行命令 **open** *host* [*port-number*] [**public-net** | **vpn-instance** *vpn-instance-name*]，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。
- 服务器端是 IPv6 地址。
  - 用户视图下，建立与 FTP 服务器的连接。

    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。
    1. 执行命令 **ftp**，进入 FTP 视图。
    2. 执行命令 **open ipv6** *host* [*port-number*]，与 FTP 服务器建立连接。

步骤 2 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。

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。

步骤 3 执行命令 **passive**，配置文件传输方式为被动方式。

----结束

8.4.4 查看 FTP 命令的在线帮助

用户可以在 FTP 客户端视图下查看 FTP 命令的在线帮助。

背景信息

请在作为客户端的交换机上进行如下的配置。

操作步骤

步骤 1 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。
  - 用户视图下，建立与 FTP 服务器的连接。

版权所有 © 华为技术有限公司

执行命令 **ftp** [*host* [*port-number*] [**public-net** | **vpn-instance** *vpn-instance-name*]，与 FTP 服务器建立连接。

- FTP 视图下，建立与 FTP 服务器的连接。

  1. 执行命令 **ftp**，进入 FTP 视图。
  2. 执行命令 **open** *host* [*port-number*] [**public-net** | **vpn-instance** *vpn-instance-name*]，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。

- 服务器端是 IPv6 地址。
  - 用户视图下，建立与 FTP 服务器的连接。

    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。

    1. 执行命令 **ftp**，进入 FTP 视图。
    2. 执行命令 **open ipv6** *host* [*port-number*]，与 FTP 服务器建立连接。

步骤 2 执行命令 **remotehelp** [*command*]，查看 FTP 命令的在线帮助。

----结束

8.4.5 上传、下载文件

用户可以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。

背景信息

请在作为客户端的交换机上进行如下的配置。

操作步骤

步骤 1 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。
  - 用户视图下，建立与 FTP 服务器的连接。

    执行命令 **ftp** [*host* [*port-number*] [**public-net** | **vpn-instance** *vpn-instance-name*]，与 FTP 服务器建立连接。
  - FTP 视图下，建立与 FTP 服务器的连接。

    1. 执行命令 **ftp**，进入 FTP 视图。
    2. 执行命令 **open** *host* [*port-number*] [**public-net** | **vpn-instance** *vpn-instance-name*]，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。

- 服务器端是 IPv6 地址。
  - 用户视图下，建立与 FTP 服务器的连接。

版权所有 © 华为技术有限公司

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。
  1. 执行命令 **ftp**，进入 FTP 视图。
  2. 执行命令 **open ipv6** *host* [*port-number*]，与 FTP 服务器建立连接。

步骤 2 上传或者下载文件。

- 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。

----结束

8.4.6 管理目录

用户可以在 FTP 服务器上进行创建、删除目录等管理操作。

背景信息

请在作为客户端的交换机上进行如下的配置。

操作步骤

步骤 1 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。
  - 用户视图下，建立与 FTP 服务器的连接。

    执行命令 **ftp** [*host* [*port-number*] [**public-net** | **vpn-instance** *vpn-instance-name*]，与 FTP 服务器建立连接。
  - FTP 视图下，建立与 FTP 服务器的连接。
    1. 执行命令 **ftp**，进入 FTP 视图。
    2. 执行命令 **open** *host* [*port-number*] [**public-net** | **vpn-instance** *vpn-instance-name*]，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。
- 服务器端是 IPv6 地址。
  - 用户视图下，建立与 FTP 服务器的连接。

    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。
    1. 执行命令 **ftp**，进入 FTP 视图。
    2. 执行命令 **open ipv6** *host* [*port-number*]，与 FTP 服务器建立连接。

步骤 2 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。

版权所有 © 华为技术有限公司

- 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。

----结束

8.4.7 管理文件

用户可以显示 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。

背景信息

请在作为客户端的交换机上进行如下的配置。

操作步骤

步骤 1 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。
  - 用户视图下，建立与 FTP 服务器的连接。

    执行命令 **ftp** [*host* [*port-number*] [**public-net** | **vpn-instance** *vpn-instance-name*]，与 FTP 服务器建立连接。
  - FTP 视图下，建立与 FTP 服务器的连接。
    1. 执行命令 **ftp**，进入 FTP 视图。
    2. 执行命令 **open** *host* [*port-number*] [**public-net** | **vpn-instance** *vpn-instance-name*]，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。
- 服务器端是 IPv6 地址。
  - 用户视图下，建立与 FTP 服务器的连接。

    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。
    1. 执行命令 **ftp**，进入 FTP 视图。
    2. 执行命令 **open ipv6** *host* [*port-number*]，与 FTP 服务器建立连接。

步骤 2 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，那么系统将在工作目录下搜索指定的文件。
- 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。

华为专有和保密信息
版权所有 © 华为技术有限公司

如果指定远程文件时没有指定路径名称，那么系统将在工作目录下搜索指定的文件。

- 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，那么系统将在工作目录下搜索指定的文件。

当指定 *local-filename* 时，可以把显示的文件的相关信息下载到本地。

----结束

8.4.8 更改登录用户

用户可以更改当前的登录用户，重新进行登录 FTP 服务器。

背景信息

请在作为客户端的交换机上进行如下的配置。

操作步骤

步骤 1 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。
  - 用户视图下，建立与 FTP 服务器的连接。

    执行命令 **ftp** [*host* [*port-number*] [**public-net** | **vpn-instance** *vpn-instance-name*]，与 FTP 服务器建立连接。
  - FTP 视图下，建立与 FTP 服务器的连接。

    1. 执行命令 **ftp**，进入 FTP 视图。
    2. 执行命令 **open** *host* [*port-number*] [**public-net** | **vpn-instance** *vpn-instance-name*]，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。
- 服务器端是 IPv6 地址。
  - 用户视图下，建立与 FTP 服务器的连接。

    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。

    1. 执行命令 **ftp**，进入 FTP 视图。
    2. 执行命令 **open ipv6** *host* [*port-number*]，与 FTP 服务器建立连接。

步骤 2 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，原用户的连接将断开。

----结束

8.4.9 断开 FTP 连接

用户可以终止与服务器的连接，并退回到用户视图或 FTP 视图。

版权所有 © 华为技术有限公司

背景信息

请在作为客户端的交换机上进行如下的配置。

操作步骤

步骤 1 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。
  - 用户视图下，建立与 FTP 服务器的连接。

    执行命令 **ftp** [*host* [*port-number*] [**public-net** | **vpn-instance** *vpn-instance-name*]，与 FTP 服务器建立连接。
  - FTP 视图下，建立与 FTP 服务器的连接。

    1. 执行命令 **ftp**，进入 FTP 视图。
    2. 执行命令 **open** *host* [*port-number*] [**public-net** | **vpn-instance** *vpn-instance-name*]，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。
- 服务器端是 IPv6 地址。
  - 用户视图下，建立与 FTP 服务器的连接。

    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。

    1. 执行命令 **ftp**，进入 FTP 视图。
    2. 执行命令 **open ipv6** *host* [*port-number*]，与 FTP 服务器建立连接。

步骤 2 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。

说明

上述配置步骤只能在 FTP 客户端视图下执行。

----结束

8.4.10 检查配置结果

交换机作为 FTP 客户端配置成功后，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

已完成交换机作为 FTP 客户端的所有配置

版权所有 © 华为技术有限公司

操作步骤

- 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-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。

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

8.5 配置交换机作为 TFTP 客户端

配置交换机作为 TFTP 客户端，登录 TFTP 服务器。

8.5.1 建立配置任务
在进行 TFTP 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。

8.5.2 使用 TFTP 下载文件
用户可以在 TFTP 客户端下载服务器上的文件。

8.5.3 使用 TFTP 上传文件
用户可以在 TFTP 客户端上传文件至服务器。

8.5.1 建立配置任务

在进行 TFTP 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传送文件且不需要复杂的交互环境时，可以使用 TFTP 协议。

前置任务

在配置 TFTP 之前，需要完成以下任务：

- 交换机安装完毕并上电启动正常
- 交换机和 TFTP 服务器路由可达

数据准备

在配置 TFTP 之前，需要准备以下数据。

序号	数据
1	TFTP 服务器 IP 地址

版权所有 © 华为技术有限公司

序号	数据
2	TFTP 服务器中特定文件的文件名
3	文件所在的目录

8.5.2 使用 TFTP 下载文件

用户可以在 TFTP 客户端下载服务器上的文件。

背景信息

请在作为 TFTP 客户端的交换机进行如下的配置。

操作步骤

步骤 1 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** *tftp-server* [**public-net** | **vpn-instance** *vpn-instance-name*] **get** *source-filename* [*destination-filename*]，使用 TFTP 下载文件。
- 服务器端是 IPv6 地址，执行命令 **tftp ipv6** *tftp-server-ipv6* [**-i** *interface-type interface-number*] **get** *source-filename* [*destination-filename*]，使用 TFTP 下载文件。

----结束

8.5.3 使用 TFTP 上传文件

用户可以在 TFTP 客户端上传文件至服务器。

背景信息

请在作为 TFTP 客户端的交换机进行如下的配置。

操作步骤

步骤 1 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** *tftp-server* [**public-net** | **vpn-instance** *vpn-instance-name*] **put** *source-filename* [*destination-filename*]，使用 TFTP 下载文件。
- 服务器端是 IPv6 地址，执行命令 **tftp ipv6** *tftp-server-ipv6* [**-i** *interface-type interface-number*] **put** *source-filename* [*destination-filename*]，使用 TFTP 下载文件。

----结束

8.6 限制对 TFTP 服务器的访问

配置限制客户端登录 TFTP 交换机，实现允许本设备以 TFTP 方式登录到哪些 TFTP 服务器。

8.6.1 建立配置任务

华为专有和保密信息
版权所有 © 华为技术有限公司

在进行限制对 TFTP 服务器的访问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。

8.6.2 配置基本访问控制列表
用户可以配置 ACL 规则。

8.6.3 配置 TFTP 基本访问控制列表
用户可以配置 TFTP 基本访问控制列表。

8.6.1 建立配置任务

在进行限制对 TFTP 服务器的访问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

交换机作为 TFTP 客户端时，可以在交换机上配置访问控制列表，控制允许本设备以 TFTP 方式登录到哪些 TFTP 服务器。

前置任务

在配置限制对 TFTP 服务器的访问之前，需要完成以下任务：

- 交换机安装完毕并上电启动正常
- 交换机和 TFTP 服务器路由可达

数据准备

在配置限制对 TFTP 服务器的访问之前，需要准备以下数据。

序号	数据
1	TFTP 服务器 IP 地址
2	访问控制列表号

8.6.2 配置基本访问控制列表

用户可以配置 ACL 规则。

背景信息

说明

TFTP 只支持基本访问控制列表。

请在作为 TFTP 客户端的设备进行如下的配置。

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。

华为专有和保密信息
版权所有 © 华为技术有限公司

步骤 3 执行命令 **rule** [*rule-id*] { **deny** | **permit** } [**fragment** | **logging** | **source** { *source-address source-wildcard* | **any** } | **time-range** *time-name*] *，配置 ACL 规则。

----结束

8.6.3 配置 TFTP 基本访问控制列表

用户可以配置 TFTP 基本访问控制列表。

背景信息

请在作为 TFTP 客户端的交换机进行如下的配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 根据 TFTP 服务器的地址类型，选择执行如下 2 个配置之一。

- 如果是 IPv4 类型的地址

  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。

- 如果是 IPv6 类型的地址

  执行命令 **tftp-server ipv6 acl** *acl6-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

8.7 配置举例

通过示例介绍 FTP 和 TFTP 的常见应用。

8.7.1 配置 FTP 服务器端示例
在本示例中，通过使用正确的用户名和密码以 FTP 方式登录到 FTP 服务器，实现下载文件到交换机的存储器。

8.7.2 配置 FTP 访问控制列表示例
在本示例中，通过配置 ACL，实现 FTP 服务器只允许某一主机登录。

8.7.3 配置 FTP 客户端示例
在本示例中，通过登录 FTP 服务器，实现从 FTP 服务器中下载系统软件和配置软件到客户端中。

8.7.4 配置 TFTP 客户端示例
在本示例中，Switch 作为 TFTP 客户端实现从服务器端下载文件。

8.7.1 配置 FTP 服务器端示例

在本示例中，通过使用正确的用户名和密码以 FTP 方式登录到 FTP 服务器，实现下载文件到交换机的存储器。

组网需求

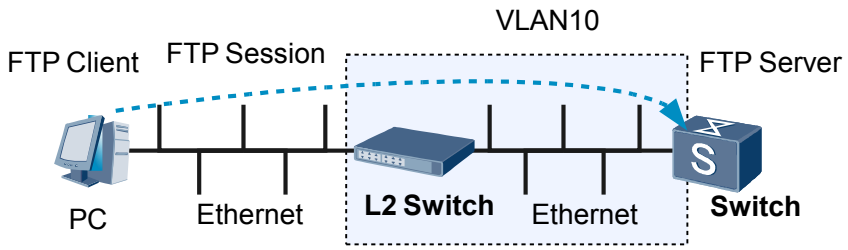
如**图 8-1** 所示。本端 PC 作为 FTP 客户端，IP 地址为 10.1.1.1/24。

华为专有和保密信息
版权所有 © 华为技术有限公司

Switch 作为 FTP Server。在 Switch 上配置 VLAN 10，将端口 GigabitEthernet0/0/1 加入 VLAN 10。配置 VLAN 10 的接口 IP 地址为 10.1.1.2/24。

PC 向 Switch 上传文件。

图 8-1 Switch 作为 FTP 服务器的组网图



Switch	接口	对应的 VLANIF	IP 地址
FTP Server	GigabitEthernet0/0/1	VLANIF 10	10.1.1.2/24

配置思路

采用如下的思路配置 FTP 服务器功能：

1. 在 FTP 服务器端 Switch 上建立正确的 FTP 用户名和密码。
2. PC 以 FTP 方式登录到 Switch 上。
3. 上传文件到 FTP 服务器端。

数据准备

为完成此配置例，需准备如下的数据：

- FTP 服务器端的 IP 地址。
- 在服务器端设置 FTP 用户名为 u1，密码为 ftppwd。
- 源文件在 PC 上正确的路径。
- 目标文件名和在 Switch 存放的位置。

操作步骤

步骤 1 在 Switch 上创建 VLAN 10，并配置 VLAN 10 的接口 IP 地址为 10.1.1.2/24

```
<Quidway> system-view
[Quidway] vlan 10
[Quidway-vlan10] quit
[Quidway] interface gigabitethernet 0/0/1
[Quidway-GigabitEthernet0/0/1] port hybrid pvid vlan 10
[Quidway-GigabitEthernet0/0/1] port hybrid untagged vlan 10
[Quidway-GigabitEthernet0/0/1] quit
[Quidway] interface vlanif 10
[Quidway-Vlanif10] ip address 10.1.1.2 24
```

步骤 2 在 Switch 上启动 FTP 服务，并配置 FTP 用户名 u1，口令 ftppwd

```
[Quidway] ftp server enable
[Quidway] aaa
```


版权所有 © 华为技术有限公司

```
[Quidway-aaa] local-user u1 password simple ftppwd
[Quidway-aaa] local-user u1 service-type ftp
[Quidway-aaa] local-user u1 ftp-directory flash:/
[Quidway-aaa] return
```

步骤 3 在 PC 机上，向 Switch 发起 FTP 连接，输入用户名 u1 和口令 ftppwd

PC 机上的 FTP 客户端以 Window XP 操作系统为例说明。

```
C:\WINDOWS\Desktop> ftp 10.1.1.2
Connected to 10.1.1.2.
220 FTP service ready
User (10.1.1.1:(none)): u1
331 Password required for u1.
Password:
230 User logged in.
ftp>
```

步骤 4 在 PC 机上，配置二进制传输格式和 PC 机本地目录

```
ftp> binary
200 Type set to I.
ftp> lcd c:\temp
Local directory now C:\temp.
```

步骤 5 在 PC 上，向 Switch 上传文件 d006.cc 和 vrpcfg.cfg

```
ftp> put d006.cc d006.cc
ftp> put vrpcfg.cfg vrpcfg.cfg
ftp> quit
C:\WINDOWS\Desktop>
```

----结束

配置文件

```
#
 sysname Quidway
#
 FTP server enable
#
 vlan batch 10
#
interface Vlanif10
 ip address 10.1.1.2 255.255.255.0
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
aaa
 local-user u1 password simple ftppwd
 local-user u1 service-type ftp
 local-user u1 ftp-directory flash:/
#
Return
```

8.7.2 配置 FTP 访问控制列表示例

在本示例中，通过配置 ACL，实现 FTP 服务器只允许某一主机登录。

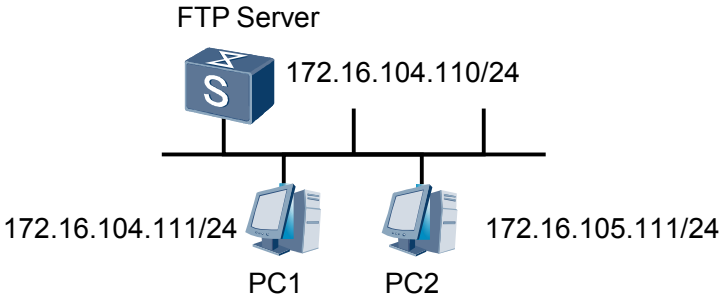
组网需求

如图 8-2 所示，FTP 服务器 IP 地址为 172.16.104.110/24。

华为专有和保密信息
版权所有 © 华为技术有限公司

客户端 PC1，PC2 和 FTP 服务器路由可达，在作为 FTP 服务器的 Switch 中，配置 ACL 后，实现 FTP 服务器只允许主机地址为：172.16.104.111 的 PC1 可以通过 FTP 方式下载和上传文件，PC2 无法连接 FTP 服务器。

图 8-2 配置 FTP 访问控制列表组网图



配置思路

采用如下的思路配置 FTP 服务器访问控制列表功能：

1. 在 FTP 服务器端进行基础配置。
2. 在 FTP 服务器端配置访问控制列表。

数据准备

为完成此配置举例，需准备如下的数据：

- 在服务器端设置 FTP 用户名为 u1，密码为 huawei。
- 访问控制列表号。

操作步骤

步骤 1 配置 FTP 基本功能

请参见 **8.7.1 配置 FTP 服务器端示例**。

步骤 2 配置 ACL 基本访问控制列表

```
<Quidway> system-view
[Quidway] acl number 2001
[Quidway-acl-basic-2001] rule permit source 172.16.104.111 0.0.0.0
[Quidway-acl-basic-2001] quit
```

步骤 3 配置 FTP 支持的 ACL 列表

```
[Quidway] ftp acl 2001
```

步骤 4 从 PC1 连接 FTP Server

```
c:\ ftp 172.16.104.110
Connected to 172.16.104.110
220 FTP service ready.
User (100.2.150.40:(none)):u1
331 Password required for u1
```


版权所有 © 华为技术有限公司

```
Password:
230 User logged in.
ftp>
```

步骤 5 从 PC2 连接 FTP Server

```
c:\ ftp 172.16.104.110
Connected to 172.16.104.110.
Info:Connection was denied by remote host according to ACL!
Connection closed by remote host.
```

----结束

配置文件

FTP 服务器的配置文件

```
#
 sysname Quidway
#
 FTP server enable
 FTP acl 2001
#
acl number 2001
 rule 5 permit source 172.16.104.111 0.0.0.0
#
 vlan batch 10
#
interface Vlanif10
 ip address 10.1.1.2 255.255.255.0
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
aaa
 local-user u1 password simple huawei
 local-user u1 service-type ftp
 local-user u1 ftp-directory flash:/
authentication-scheme default
#
 authorization-scheme default
#
 accounting-scheme default
#
 domain default
#
return
```

8.7.3 配置 FTP 客户端示例

在本示例中，通过登录 FTP 服务器，实现从 FTP 服务器中下载系统软件和配置软件到客户端中。

组网需求

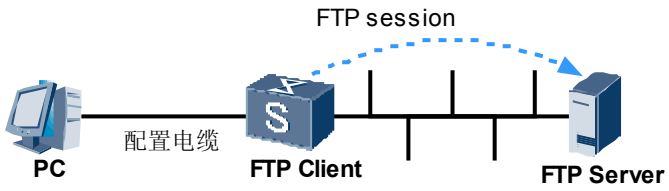
如图 8-3 所示。远端服务器提供 FTP 服务器功能，IP 地址为 10.1.1.2。

Switch 与 FTP Server 在直连网段，路由可达。Switch 作为 FTP 客户端，从端口 GigabitEthernet0/0/1 到 GigabitEthernet0/0/4 都可以向外发起 FTP 连接请求，这些端口对应的 IP 地址为 10.1.1.3/24。

Switch 从 FTP 服务器下载文件。

版权所有 © 华为技术有限公司

图 8-3 Switch 作为 FTP 客户端的组网图



配置思路

采用如下的思路配置 FTP 客户端功能：

1. 从 FTP 客户端登录到 FTP 服务器中。
2. 从服务端下载文件到客户端的存储设备中。

数据准备

为完成此配置例，需准备如下的数据：

- FTP 客户端的接口所属的 VLAN 号为 VLAN10，对应 VLANIF 接口的 IP 地址为 10.1.1.3/24。
- 目标文件名及在 Switch 中的位置。
- 客户端用于登录的用户名 u1 和密码 ftppwd。

操作步骤

步骤 1 在远端服务器上启动 FTP Server 服务应用，添加 FTP 用户名 u1，密码 ftppwd。

步骤 2 在 Switch 上创建 VLAN，并配置 IP 地址为 10.1.1.3/24。

```
<Quidway> system-view
[Quidway] vlan 10
[Quidway-vlan10] quit
[Quidway] interface gigabitethernet 0/0/1
[Quidway-GigabitEthernet0/0/1] port hybrid pvid vlan 10
[Quidway-GigabitEthernet0/0/1] port hybrid untagged vlan 10
[Quidway-GigabitEthernet0/0/1] quit
[Quidway] interface gigabitethernet 0/0/2
[Quidway-GigabitEthernet0/0/2] port hybrid pvid vlan 10
[Quidway-GigabitEthernet0/0/2] port hybrid untagged vlan 10
[Quidway-GigabitEthernet0/0/2] quit
[Quidway] interface gigabitethernet 0/0/3
[Quidway-GigabitEthernet0/0/3] port hybrid pvid vlan 10
[Quidway-GigabitEthernet0/0/3] port hybrid untagged vlan 10
[Quidway-GigabitEthernet0/0/3] quit
[Quidway] interface gigabitethernet 0/0/4
[Quidway-GigabitEthernet0/0/4] port hybrid pvid vlan 10
[Quidway-GigabitEthernet0/0/4] port hybrid untagged vlan 10
[Quidway-GigabitEthernet0/0/4] quit
[Quidway] interface vlanif 10
[Quidway-Vlanif10] ip address 10.1.1.3 24
```

步骤 3 在 Switch 上，向 FTP Server 发起连接，FTP Server 的 IP 地址为 10.1.1.2，输入用户名 u1 和口令 ftppwd。

```
<Quidway> ftp 10.1.1.2
```


版权所有 © 华为技术有限公司

```
Trying 10.1.1.2 ...
Press CTRL+K to abort
Connected to 10.1.1.2.
220 FTP service ready.
User(10.1.1.2:(none)):u1
331 Password required for u1.
Enter password:
230 User logged in.

[ftp]
```

步骤 4 在 Switch 上，配置二进制传输格式和 Flash 工作目录。

```
[ftp] binary
200 Type set to I.
[ftp] lcd flash:/
The current local directory is flash:.
```

步骤 5 在 Switch 上，从远端 FTP 服务器下载 vrpcfg.cfg 文件。

```
[ftp] get vrpcfg.cfg vrpcfg.cfg
200 Port command okay.
150 Opening BINARY mode data connection for vrpcfg.cfg.

226 Transfer complete.
FTP: 9124 byte(s) received in 3.100 second(s) 2.94Kbyte(s)/sec.
[ftp] quit
<Quidway>
```

----结束

配置文件

```
#
 sysname Quidway
#
 vlan batch 10
#
interface Vlanif10
 ip address 10.1.1.3 255.255.255.0
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface GigabitEthernet0/0/2
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface GigabitEthernet0/0/3
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface GigabitEthernet0/0/4
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
return
```

8.7.4 配置 TFTP 客户端示例

在本示例中，Switch 作为 TFTP 客户端实现从服务器端下载文件。

组网需求

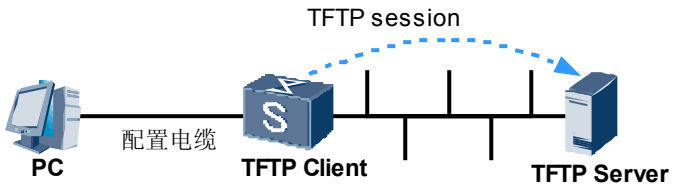
如图 8-4 所示。Switch 不能作为 TFTP 的服务器端。远端服务器提供 TFTP Server 功能，IP 地址为 10.1.1.2/24。

版权所有 © 华为技术有限公司

Switch 作为 TFTP 客户端。在 Switch 上配置 VLAN 10，将端口 GigabitEthernet0/0/1 加入 VLAN 10。配置 VLAN 10 的接口 IP 地址为 10.1.1.1/24。

Switch 从 TFTP 服务器端下载文件。

图 8-4 配置 TFTP 组网图



配置思路

采用如下的思路配置 TFTP 传输文件功能：

1. 在 TFTP 服务器端运行 TFTP 软件，并设置源文件在服务器中的位置。
2. 在 Switch 上使用 TFTP 命令下载文件。

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 Switch 上存放的路径。

操作步骤

步骤 1 在远端服务器上启动 TFTP Server 服务，确保 TFTP 服务应用软件处于启动状态

步骤 2 在 Switch 上创建 VLAN 10，并配置 VLAN 10 接口的 IP 地址为 10.1.1.1/24

```
<Quidway> system-view
[Quidway] vlan 10
[Quidway-vlan10] quit
[Quidway] interface gigabitethernet 0/0/1
[Quidway-GigabitEthernet0/0/1] port hybrid pvid vlan 10
[Quidway-GigabitEthernet0/0/1] port hybrid untagged vlan 10
[Quidway-GigabitEthernet0/0/1] quit
[Quidway] interface vlanif 10
[Quidway-Vlanif10] ip address 10.1.1.1 24
```

步骤 3 在 Switch 上，向 TFTP Server 发起连接，下载 8031.cc 文件

```
<Quidway> tftp 10.1.1.2 get 8031.cc 8031new.cc
Info:  Transfer file in binary mode.
Downloading the file from the remote tftp server, please wait...
```

----结束

配置文件

```
#
 sysname Quidway
```


版权所有 © 华为技术有限公司

```
#
 vlan batch 10
#
interface Vlanif10
 ip address 10.1.1.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
Return
```


华为专有和保密信息
版权所有 © 华为技术有限公司

9 Telnet 及 SSH

关于本章

Telnet 及 SSH 提供通过终端远程登录并访问服务器的方式。

9.1 Telnet 及 SSH 简介
用户登录、Telnet 及 SSH 基本概念。

9.2 配置 Telnet 终端服务
通过 Telnet 协议远程登录到交换机，对交换机进行配置。

9.3 配置 SSH 用户
配置 SSH 用户，保证 STelnet 或 SFTP 客户端能够登录到 SSH 服务器。

9.4 配置 SSH 服务器功能
SSH 服务器的配置方法。首先在 SSH 服务器上使能 STelnet 或者 SFTP，保证 Stelnet 和 SFTP 功能的使用。

9.5 配置 STelnet 客户端功能
STelnet 客户端的配置方法。客户端和服务器之间经过协商，建立安全连接，客户端可以像操作 Telnet 一样登录服务器。

9.6 配置 SFTP 客户端功能
SFTP 客户端的配置方法。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。

9.7 配置举例
配置 Telnet 及 SSH 的应用的示例。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。

华为专有和保密信息
版权所有 © 华为技术有限公司

9.1 Telnet 及 SSH 简介

用户登录、Telnet 及 SSH 基本概念。

9.1.1 用户登录概述
用户可以通过 Console 口、Telnet 或 SSH 进行本地或远程登录。

9.1.2 Telnet 终端服务基本概念
S5700 提供的 Telnet 服务包括 Telnet Server 和 Telnet Client。

9.1.3 SSH 终端服务基本概念
S5700 支持基本的 SSH 协议、客户端功能、SFTP 协议、STelnet 协议。

9.1.1 用户登录概述

用户可以通过 Console 口、Telnet 或 SSH 进行本地或远程登录。

配置了用户界面、用户管理和终端服务后，用户才能登录到设备，对本地或远端的 S5700 进行配置、监控和维护。

用户界面提供登录入口，用户管理确保登录安全，终端服务则提供登录协议支持。

目前 S5700 支持的登录方式包括：

- 通过 Console 口登录。
- 通过 Telnet 或 SSH 进行本地或远程登录。

9.1.2 Telnet 终端服务基本概念

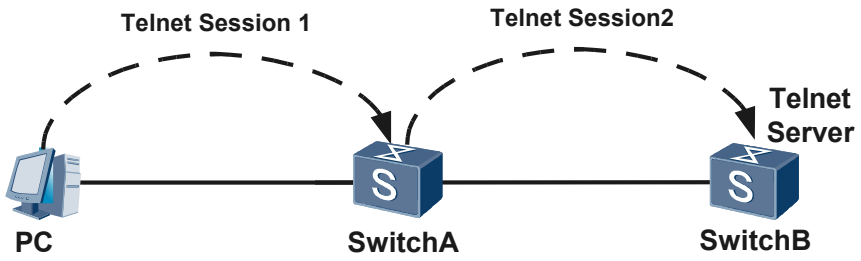
S5700 提供的 Telnet 服务包括 Telnet Server 和 Telnet Client。

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。

S5700 提供的 Telnet 服务包括：

- Telnet server：用户在 PC 上运行 Telnet 客户端程序登录到交换机，对交换机进行配置管理。此时，交换机提供 Telnet server 服务。
- Telnet client：用户在 PC 上通过终端仿真程序或 Telnet 客户端程序建立与交换机的连接后，再执行 **telnet** 命令登录到其它交换机，对其进行配置管理。如图 9-1 所示，SwitchA 此时既作为 Telnet server，也同时提供 Telnet client 服务。

图 9-1 提供 Telnet client 服务



版权所有 © 华为技术有限公司

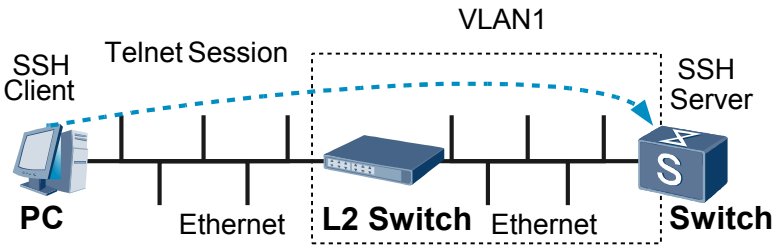
9.1.3 SSH 终端服务基本概念

S5700 支持基本的 SSH 协议、客户端功能、SFTP 协议、STelnet 协议。

SSH 简介

SSH（Secure Shell）在 TCP/IP 协议族中属于应用层协议，主要用于在需要保证安全的网络环境中提供远程登录和虚拟终端功能。SSH 基于 TCP 连接为传输信息提供强大的安全保障和验证功能，从而有效地抵御 IP 地址欺骗、明文密码截取、DoS（Denial of Service）等攻击。如图 9-2 所示。图中，S5700 用 Switch 表示。

图 9-2 PC 与 S5700 建立本地 SSH 连接



SSH 采用了客户/服务器体系模型，通过建立 SSH 连接构建多条安全的传输通路。例如，Switch 作为 SSH Server，可以接受来自多个用户 PC 机（SSH Client）的连接，用户 PC 机和 SSH Server 之间可能存在其它 L2 Switch 设备。实际组网时，要求 PC 和 Switch 之间有可达路由。

SSH 的优势

SSH 的应用包括 STelnet 和 SFTP，相对 Telnet、FTP 等终端服务，SSH 可以在没有安全保障的网络上提供安全的远程访问，优势如下：

- STelnet 客户端功能

  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（Revest-Shamir-Adleman Algorithm）验证方式
  - 支持 DES（Data Encryption Standard）、3DES 数据加密方式
  - 支持用户名/口令的加密传输
  - 支持交互数据的加密传输

  SSH 终端服务采用 RSA 算法，可以遵照非对称加密体系的加密原则，通过生成公钥和私钥，以加密方式传递密钥、用户名/口令、交互数据，最终实现了整个会话信息的端到端安全传递。

- SFTP 客户端功能

版权所有 © 华为技术有限公司

SFTP 是 Secure FTP 的简称，存在两种应用。

- 用户可以从远端安全地通过 S5700 登录到远程设备上，进行文件管理，应用于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。
- S5700 本身可以作为客户端，在本设备上安全 FTP 到远程设备，进行文件的安全传输。

SSH 连接的建立过程

SSH 连接的建立过程包括如下五个阶段：

1. 协商 SSH 版本号
2. 协商密钥
3. 验证用户身份
4. 请求会话
5. 交互会话

每个阶段具体的过程请参见《Quidway S5700 系列 以太网交换机 特性描述-基础配置》中的。

9.2 配置 Telnet 终端服务

通过 Telnet 协议远程登录到交换机，对交换机进行配置。

9.2.1 建立配置任务
在进行 Telnet 终端服务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。

9.2.2 使能 Telnet 服务
建立与服务器的 Telnet 连接之前，需要首先开启 Telnet 服务。

9.2.3 建立 Telnet 连接
用户可以通过 Telnet 连接，登录并管理交换机。

9.2.4 （可选）Telnet 连接的定时断开
用户可以配置 Telnet 连接空闲时间。在设定的时间内，如果 Telnet 连接始终处于空闲状态，系统将自动断开该 Telnet 连接。

9.2.5 检查配置结果
Telnet 终端服务配置成功后，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。

9.2.1 建立配置任务

在进行 Telnet 终端服务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

当用户通过 Telnet 协议远程登录到交换机进行维护管理时，需要配置 Telnet 终端服务。

版权所有 © 华为技术有限公司

前置任务

在配置 Telnet 终端服务之前，需要完成以下任务：

- 交换机运行正常
- 正确配置交换机接口的 IP 地址
- 配置了用户账号以及正确的登录验证方式和呼入呼出受限规则
- 终端与交换机之间有可达路由

数据准备

在配置 Telnet 终端服务之前，需要准备以下数据。

序号	数据
1	交换机 IP 地址
2	VPN 实例名
3	远端交换机的 IPv4/IPv6 地址或主机名
4	远端交换机提供 Telnet 服务的 TCP 端口号
5	（可选）用户界面断开连接的超时时间
6	（可选）设备作为 Telnet 客户端时的源地址（或者源接口）

9.2.2 使能 Telnet 服务

建立与服务器的 Telnet 连接之前，需要首先开启 Telnet 服务。

背景信息

请在作为 Telnet 服务器的交换机上进行如下的配置。

根据网络协议基于 IPv4 还是 IPv6，选择执行如下步骤之一。

操作步骤

- 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。

     说明

     - 缺省情况下，系统的 Telnet 服务功能是开启的。
     - 执行命令 **undo telnet server enable** 关闭 Telnet 服务器时，如果有通过 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。
- 网络协议基于 IPv6
  1. 执行命令 **system-view**，进入系统视图。

版权所有 © 华为技术有限公司

2. 执行命令 **telnet ipv6 server enable**，使能 Telnet 服务。

说明

- 缺省情况下，系统的 Telnet 服务功能是开启的。
- 执行命令 **telnet ipv6 server enable** 关闭 Telnet 服务器时，如果有通过 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

9.2.3 建立 Telnet 连接

用户可以通过 Telnet 连接，登录并管理交换机。

背景信息

请在作为 Telnet 客户端的交换机上进行如下的配置。

根据网络协议基于 IPv4 还是 IPv6，选择执行如下 2 个步骤之一：

操作步骤

- 执行命令 **telnet** [**vpn-instance** *vpn-instance-name*] *host-name* [*port-number*]，登录并管理其他交换机。
- 执行命令 **telnet ipv6** *host-name* [*port-number*]，登录并管理其他交换机。

----结束

9.2.4 （可选）Telnet 连接的定时断开

用户可以配置 Telnet 连接空闲时间。在设定的时间内，如果 Telnet 连接始终处于空闲状态，系统将自动断开该 Telnet 连接。

背景信息

请在作为 Telnet 服务器的交换机上进行如下的配置。

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** [*ui-type*] *first-ui-number* [*last-ui-number*]，进入用户界面视图。

步骤 3 执行命令 **idle-timeout** *minutes* [*seconds*]，允许定时断开 Telnet 连接。

----结束

9.2.5 检查配置结果

Telnet 终端服务配置成功后，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 Telnet 终端服务的所有配置。

版权所有 © 华为技术有限公司

背景信息

- 使用 **display users** 命令查看当前用户界面连接情况。
- 使用 **display users all** 命令查看每个用户界面连接情况。
- 使用 **display tcp status** 命令查看当前建立的所有 TCP 连接情况。

任务示例

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。

```
<Quidway> 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
```

9.3 配置 SSH 用户

配置 SSH 用户，保证 STelnet 或 SFTP 客户端能够登录到 SSH 服务器。

9.3.1 建立配置任务
在进行 SSH 用户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。

9.3.2 创建 SSH 用户
AAA 无法提供 RSA 认证，因此当认证方式为 RSA 或 password-rsa 时，用户需要创建 SSH 用户。如果认证方式为 password，可以使用 AAA 视图同名的 local-user 用户。

9.3.3 配置 VTY 用户界面支持 SSH 协议
用户可以在 VTY 用户界面配置 SSH。

9.3.4 生成本地 RSA 密钥对
在进行 SSH 配置之前，需要首先配置 RSA 密钥。

9.3.5 配置 SSH 用户的认证方式
用户可以配置对 SSH 用户进行 Password 验证或者 RSA 验证。

9.3.6 （可选）配置 SSH 用户基本验证信息
用户可以配置服务器密钥的更新时间、SSH 认证超时时间以及 SSH 验证重试次数。

9.3.7 （可选）配置 SSH 用户按命令行授权
配置验证方式为 RSA 时，需要配置 SSH 用户按命令行授权。

9.3.8 配置 SSH 用户的服务方式
用户可以配置 SSH 用户的服务方式为 sftp 或 stelnet 或 all。

9.3.9 （可选）配置 SSH 用户的 SFTP 服务授权目录
用户配置某一目录为授权目录，允许 SSH 用户使用 SFTP 服务。

9.3.10 检查配置结果
SSH 用户配置成功后，可以查看到 SSH 用户信息等内容。

9.3.1 建立配置任务

在进行 SSH 用户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。

版权所有 © 华为技术有限公司

应用环境

只有在 SSH 服务器端完成对 SSH 用户的正确配置后，STelnet 或 SFTP 客户端才能登录到 SSH 服务器，完成到相应的操作。

前置任务

在配置 SSH 用户之前，需完成以下任务：

- 创建本地用户
- SSH 服务器端配置客户端的 RSA 公钥

数据准备

在配置 SSH 用户之前，需准备以下数据。

序号	数据
1	SSH 用户的用户名和密码
2	SSH 用户的认证方式
3	SSH 用户的服务方式
4	为 SSH 用户分配的对端 RSA 公钥名
5	SSH 用户的 SFTP 工作目录

9.3.2 创建 SSH 用户

AAA 无法提供 RSA 认证，因此当认证方式为 RSA 或 password-rsa 时，用户需要创建 SSH 用户。如果认证方式为 password，可以使用 AAA 视图同名的 local-user 用户。

背景信息

说明

如果不单独创建 SSH 用户，还可以在进行如下配置的同时新建 SSH 用户：

- **配置 SSH 用户的认证方式**
- **配置 SSH 用户的服务方式**

请在作为 SSH 服务器的交换机上进行如下的配置。

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 user** *user-name*，创建 SSH 用户。

如果创建认证方式为 password 或 password-rsa 的 SSH 用户，则还需要在 AAA 视图下创建同名的 local-user 用户。

1. 执行命令 **aaa**，进入 AAA 视图。

版权所有 © 华为技术有限公司

2. 执行命令 **local-user** *user-name* **password** { **simple** | **cipher** } *password*，配置本地用户名和密码。

----结束

9.3.3 配置 VTY 用户界面支持 SSH 协议

用户可以在 VTY 用户界面配置 SSH。

背景信息

请在作为 SSH 服务器的交换机上进行如下的配置。

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。

说明

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。

----结束

9.3.4 生成本地 RSA 密钥对

在进行 SSH 配置之前，需要首先配置 RSA 密钥。

背景信息

请在作为客户端和服务器端的交换机上分别进行如下的配置。

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 local-key-pair create**，产生本地 RSA 密钥对。

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，必须完成 **rsa local-key-pair create** 配置，生成本地密钥对。

----结束

9.3.5 配置 SSH 用户的认证方式

用户可以配置对 SSH 用户进行 Password 验证或者 RSA 验证。

背景信息

请在作为 SSH 服务器的交换机上进行如下的配置。

版权所有 © 华为技术有限公司

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 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。
  - 执行命令 **ssh authentication-type default password**，对 SSH 用户配置缺省密码验证。

  采用本地认证或 HWTACACS 服务器认证时，如果用户数量少可以采用第一种配置；如果用户数量比较多，对 SSH 用户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。

   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。公共密钥生成后，可以执行 **display rsa local-key-pair public** 命令查看。
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 *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。

说明

- 进入公共密钥编辑视图后，即可将客户端上产生的 RSA 公共密钥传送到服务器端。请采用拷贝粘贴方式将 RSA 公共密钥配置到作为 SSH 服务器的交换机上。
- 在为 SSH 用户分配对端 RSA 公共密钥之前，所分配的对端 RSA 公共密钥必须是在 SSH 服务器端已经配置完成且来自 SSH 客户端的 RSA 公共密钥。

----结束

9.3.6 （可选）配置 SSH 用户基本验证信息

用户可以配置服务器密钥的更新时间、SSH 认证超时时间以及 SSH 验证重试次数。

背景信息

请在作为 SSH 服务器的交换机上进行如下的配置。

版权所有 © 华为技术有限公司

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 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。

步骤 3 执行命令 **ssh server timeout** *seconds*，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。

步骤 4 执行命令 **ssh server authentication-retries** *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

9.3.7 （可选）配置 SSH 用户按命令行授权

配置验证方式为 RSA 时，需要配置 SSH 用户按命令行授权。

背景信息

说明

SSH 用户有 4 种验证方式：password、rsa、password-rsa 和 all 方式。password 方式的命令行授权配置请参见《Quidway S5700 系列 以太网交换机 配置指南-安全》“AAA 及用户管理配置”。本节介绍 RSA 方式的命令行授权。

请在作为 SSH 服务器的交换机上进行如下的配置。

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 user** *user-name* **authorization-cmd aaa**，对指定 SSH 用户配置按命令行授权。

----结束

后续处理

对进行 RSA 验证的 SSH 用户配置命令行授权后，请再进行相关 AAA 授权配置。否则该 SSH 用户的命令行授权配置不能生效。

9.3.8 配置 SSH 用户的服务方式

用户可以配置 SSH 用户的服务方式为 sftp 或 stelnet 或 all。

背景信息

请在作为 SSH 服务器的交换机上进行如下的配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

版权所有 © 华为技术有限公司

步骤 2 执行命令 **ssh user** *username* **service-type** { **sftp** | **stelnet** | **all** }，配置 SSH 用户的服务方式。

缺省情况下，SSH 用户的服务方式是空，即不支持任何服务方式。

----结束

9.3.9 （可选）配置 SSH 用户的 SFTP 服务授权目录

用户配置某一目录为授权目录，允许 SSH 用户使用 SFTP 服务。

背景信息

请在作为 SSH 服务器的交换机上进行如下的配置。

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 user** *username* **sftp-directory** *directoryname*，配置 SSH 用户的 SFTP 服务授权目录。

缺省情况下，SSH 用户的 SFTP 服务授权目录为 Flash。

----结束

9.3.10 检查配置结果

SSH 用户配置成功后，可以查看到 SSH 用户信息等内容。

前提条件

已完成 SSH 用户的所有配置

背景信息

- 使用 **display ssh user-information** 命令在 SSH 服务器端查看所有 SSH 用户信息。
- 使用 **display ssh user-information** *username* 命令在 SSH 服务器端查看指定 SSH 用户信息。

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**。

```
<Quidway> display ssh user-information client001
User Name              : client001
Authentication-type    : password
User-public-key-name   : -
Sftp-directory         : -
Service-type           : sftp
Authorization-cmd      : No
```


版权所有 © 华为技术有限公司

9.4 配置 SSH 服务器功能

SSH 服务器的配置方法。首先在 SSH 服务器上使能 STelnet 或者 SFTP，保证 Stelnet 和 SFTP 功能的使用。

9.4.1 建立配置任务
在进行 SSH 服务器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。

9.4.2 使能 STelnet 服务
使用 STelnet 服务之前，需要首先进行使能操作。

9.4.3 使能 SFTP 服务
使用 SFTP 服务之前，需要首先进行使能操作。

9.4.4 （可选）使能兼容低版本功能
用户可以配置是否使能兼容低版本 SSH 协议。

9.4.5 （可选）配置 SSH 服务器端监听端口号
用户可以配置或变更 SSH 服务器监听端口号。变更后，只有用户知道 SSH 服务使用的当前端口号，确保安全性。

9.4.6 （可选）配置服务器密钥对更新时间
用户可以配置服务器密钥对更新时间，更新密钥可以保证安全性。

9.4.7 检查配置结果
SSH 服务器功能配置成功后，可以查看到 SSH 服务器的全局配置信息等内容。

9.4.1 建立配置任务

在进行 SSH 服务器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

必须在 SSH 服务器上使能 STelnet 或者 SFTP，才能完成到相应的操作。SSH 服务器还支持监听端口号的设定。通过设定 SSH 服务器端的监听端口号为其他端口，攻击者不知道 SSH 监听端口号的更改，有效防止攻击者对 SSH 服务标准端口访问消耗带宽和系统资源。

前置任务

在配置 SSH 服务器功能之前，需完成以下任务：

- SSH 客户端和服务器正确连接
- SSH 客户端和服务器之间有可达的路由
- SSH 服务器端配置 VTY 用户界面支持 SSH 协议
- SSH 服务器端配置 SSH 用户
- SSH 服务器端生成本地 RSA 密钥对

版权所有 © 华为技术有限公司

数据准备

在配置 SSH 服务器功能之前，需准备以下数据。

序号	数据
1	SSH 服务器端监听端口号

9.4.2 使能 STelnet 服务

使用 STelnet 服务之前，需要首先进行使能操作。

背景信息

请在作为 SSH 服务器的交换机上进行如下的配置。

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。

缺省情况下，STelnet 服务为关闭状态。

----结束

9.4.3 使能 SFTP 服务

使用 SFTP 服务之前，需要首先进行使能操作。

背景信息

请在作为 SSH 服务器的交换机上进行如下的配置。

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。

缺省情况下，SFTP 服务为关闭状态。

----结束

9.4.4 （可选）使能兼容低版本功能

用户可以配置是否使能兼容低版本 SSH 协议。

背景信息

请在作为 SSH 服务器的交换机上进行如下的配置。

版权所有 © 华为技术有限公司

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 server compatible-ssh1x enable**，使能兼容低版本功能。

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。

说明

- 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）。
- S5700 支持大于等于 1.3 且小于等于 2.0 之间的 SSH 协议版本。

----结束

9.4.5 （可选）配置 SSH 服务器端监听端口号

用户可以配置或变更 SSH 服务器监听端口号。变更后，只有用户知道 SSH 服务使用的当前端口号，确保安全性。

背景信息

请在作为 SSH 服务器的交换机上进行如下的配置。

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 server port** *port-number*，配置 SSH 服务器监听端口号。

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。

----结束

9.4.6 （可选）配置服务器密钥对更新时间

用户可以配置服务器密钥对更新时间，更新密钥可以保证安全性。

背景信息

请在作为 SSH 服务器的交换机上进行如下配置。

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 server rekey-interval** *interval*，配置服务器密钥对更新时间。

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。

----结束

版权所有 © 华为技术有限公司

9.4.7 检查配置结果

SSH 服务器功能配置成功后，可以查看到 SSH 服务器的全局配置信息等内容。

前提条件

已经完成 SSH 服务器功能的所有配置。

背景信息

使用 **display ssh server status** 命令查看 SSH 服务器的全局配置信息。

任务示例

运行命令 **display ssh server status**，可以看到 SSH 会话连接的协议版本号为 1.99、建立 SSH 会话连接的重试次数为 5 等。

```
<Quidway> 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
 SSH server port                      : 55535
```

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。

9.5 配置 STelnet 客户端功能

STelnet 客户端的配置方法。客户端和服务器之间经过协商，建立安全连接，客户端可以像操作 Telnet 一样登录服务器。

9.5.1 建立配置任务
在进行 Stelnet 客户端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。

9.5.2 使能 SSH 客户端首次认证功能
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。

9.5.3 （可选）SSH 客户端为 SSH 服务器分配 RSA 公钥
用户可以在 SSH 客户端为 SSH 服务器分配 RSA 公钥。

9.5.4 启动 STelnet 客户端
用户可以从 SSH 客户端以 STelnet 方式登录到 SSH 服务器上。

9.5.5 检查配置结果
Stelnet 客户端功能配置成功后，可以查看到 SSH 服务器的全局配置信息等内容。

9.5.1 建立配置任务

在进行 Stelnet 客户端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。

版权所有 © 华为技术有限公司

应用环境

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 STelnet 客户端连接 SSH 服务器之前，需完成以下任务：

- SSH 服务器端生成本地 RSA 密钥对
- SSH 服务器端配置 STelnet 用户
- SSH 服务器端 STelnet 服务使能

数据准备

在配置 STelnet 客户端连接 SSH2 服务器之前，需准备以下数据。

序号	数据
1	SSH 服务器名称
2	SSH 服务器当前监听的端口号
3	STelnet 客户端到 SSH 服务器端的首选加密算法
4	SSH 服务器端到 STelnet 客户端的首选加密算法
5	STelnet 客户端到 SSH 服务器端的首选 HMAC 算法
6	SSH 服务器端到 STelnet 客户端的首选 HMAC 算法
7	首选密钥交换算法
8	出接口名称
9	源地址

9.5.2 使能 SSH 客户端首次认证功能

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。

推荐使用使能 SSH 客户端首次认证功能，简化用户操作。

请在作为 SSH 客户端的交换机上进行如下的配置。

版权所有 © 华为技术有限公司

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，是为了当 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，则当 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，而导致登录服务器失败。

窍门

除了使能 SSH 客户端首次认证功能之外，如果 STelnet 客户端想第一次就能成功登录 SSH 服务器，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

9.5.3 （可选）SSH 客户端为 SSH 服务器分配 RSA 公钥

用户可以在 SSH 客户端为 SSH 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，那么需要在 STelnet 客户端登录 SSH 服务器之前分配 RSA 公钥。

请在作为 SSH 客户端的交换机上进行如下的配置。

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，由支持 SSH 的客户端软件随机生成。公共密钥生成后，可以执行 **display rsa local-key-pair public** 命令查看。

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 b 中指定的密 *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。

版权所有 © 华为技术有限公司

说明

- 在为 SSH 服务器分配对端 RSA 公钥之前，所分配的对端 RSA 公钥必须是在 SSH 客户端已经配置完成且来自 SSH 服务器端的 RSA 公钥，这样 STelnet 客户端对 SSH 服务器的 RSA 公钥进行有效性检查才会通过。
- 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

9.5.4 启动 STelnet 客户端

用户可以从 SSH 客户端以 STelnet 方式登录到 SSH 服务器上。

背景信息

说明

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。

请在作为 SSH 客户端的交换机上进行如下的配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 根据 SSH 服务器的地址类型，选择执行如下 2 个配置之一。

- 如果是 IPv4 类型的地址

  执行命令 **stelnet** *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。

- 如果是 IPv6 类型的地址

  执行命令 **stelnet ipv6** *host-ipv6* [**-i** *interface-type interface-number*] [*port*] [[**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

9.5.5 检查配置结果

Stelnet 客户端功能配置成功后，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 STelnet 客户端功能的所有配置

版权所有 © 华为技术有限公司

背景信息

- 使用 **display ssh server-info** 命令在 SSH 客户端查看 SSH 服务器与 RSA 公钥之间的对应关系。
- 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。

任务示例

运行命令 **display ssh server session**，可以看到客户端从 VTY3 登录上来，采用的服务方式是 Stelent，验证方式是 password 等。

```
<Quidway> display ssh server session
Session 1:
       Conn                 : VTY 3
       Version              : 2.0
       State                : started
       Username             : client001
       Retry                : 1
       CTOS Cipher          : aes128-cbc
       STOC Cipher          : aes128-cbc
       CTOS Hmac            : hmac-sha1-96
       STOC Hmac            : hmac-sha1-96
       Kex                  : diffie-hellman-group1-sha1
       Service Type         : stelnet
       Authentication Type  : password
```

9.6 配置 SFTP 客户端功能

SFTP 客户端的配置方法。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。

9.6.1 建立配置任务
在进行 SFTP 客户端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。

9.6.2 使能 SSH 客户端首次认证功能
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。

9.6.3 （可选）SSH 客户端为 SSH 服务器分配 RSA 公钥
用户可以在 SSH 客户端为 SSH 服务器分配 RSA 公钥。

9.6.4 启动 SFTP 客户端
用户可以从 SSH 客户端以 SFTP 方式登录到 SSH 服务器上。

9.6.5 （可选）管理目录
用户可以在 SFTP 客户端上创建、删除服务器上的目录。

9.6.6 （可选）管理文件
用户可以在 SFTP 客户端上显示 SFTP 服务器指定远程目录或文件的信息，或者删除 SFTP 服务器上的指定文件。

9.6.7 （可选）SFTP 客户端命令帮助
用户而可以查看 SFTP 客户端命令帮助。

9.6.8 检查配置结果
SFTP 客户端功能配置成功后，可以查看到 SSH 服务器的全局配置信息等内容。

版权所有 © 华为技术有限公司

9.6.1 建立配置任务

在进行 SFTP 客户端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

SFTP 使得用户可以从远端安全的登入设备进行文件管理，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。同时，由于提供了 Client 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。

前置任务

在 SFTP 客户端连接 SSH2 服务器之前，需完成以下任务：

- SSH 服务器端生成本地 RSA 密钥对
- SSH 服务器端配置 SFTP 用户
- SSH 服务器端 SFTP 服务使能

数据准备

在 SFTP 客户端连接 SSH2 服务器之前，需准备以下数据。

序号	数据
1	SSH 服务器名称
2	SSH 服务器当前监听的端口号
3	SFTP 客户端到 SSH 服务器端的首选加密算法
4	SSH 服务器端到 SFTP 客户端的首选加密算法
5	SFTP 客户端到 SSH 服务器端的首选 HMAC 算法
6	SSH 服务器端到 SFTP 客户端的首选 HMAC 算法
7	首选密钥交换算法
8	出接口名称
9	目录名称
10	文件名称

9.6.2 使能 SSH 客户端首次认证功能

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。

版权所有 © 华为技术有限公司

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。

推荐使用使能 SSH 客户端首次认证功能，简化用户操作。

请在作为 SSH 客户端的交换机上进行如下的配置。

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，是为了当 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，因为此时 SFTP 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，则当 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，而导致登录服务器失败。

窍门

除了使能 SSH 客户端首次认证功能之外，如果 SFTP 客户端想第一次就能成功登录 SSH 服务器，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

9.6.3 （可选）SSH 客户端为 SSH 服务器分配 RSA 公钥

用户可以在 SSH 客户端为 SSH 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，那么需要在 SFTP 客户端登录 SSH 服务器之前分配 RSA 公钥。

请在作为 SSH 客户端的交换机上进行如下的配置。

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，由支持 SSH 的客户端软件随机生成。公共密钥生成后，可以执行 **display rsa local-key-pair public** 命令查看。

步骤 5 执行命令 **public-key-code end**，退出公共密钥编辑视图。

版权所有 © 华为技术有限公司

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 *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

- 在为 SSH 服务器分配对端 RSA 公钥之前，所分配的对端 RSA 公钥必须是在 SSH 客户端已经配置完成且来自 SSH 服务器端的 RSA 公钥，这样 SFTP 客户端对 SSH 服务器的 RSA 公钥进行有效性检查才会通过。
- 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

9.6.4 启动 SFTP 客户端

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

说明

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 客户端的交换机上进行如下的配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 根据 SSH 服务器的地址类型，选择执行如下 2 个配置之一。

- 如果是 IPv4 类型的地址

  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。

- 如果是 IPv6 类型的地址

  执行命令 **sftp ipv6** [**-a** *source-address*] *host-ipv6* [**-i** *interface-type interface-number*] [*port*] [[**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。

----结束

9.6.5 （可选）管理目录

用户可以在 SFTP 客户端上创建、删除服务器上的目录。

版权所有 © 华为技术有限公司

背景信息

说明

当 SFTP 客户端登录到 SSH 服务器之后，在 SFTP 客户端可以创建并删除 SSH 服务器上的目录，以及显示当前的工作目录，显示指定目录下的文件或目录信息。

请在作为 SSH 客户端的交换机上进行如下的配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 根据 SSH 服务器的地址类型，选择执行如下 2 个配置之一。

- 如果是 IPv4 类型的地址

  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。

- 如果是 IPv6 类型的地址

  执行命令 **sftp ipv6** [**-a** *source-address*] *host-ipv6* [**-i** *interface-type interface-number*] [*port*] [[**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。

步骤 3 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 / ls** [*remote-directory*]，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。

----结束

9.6.6 （可选）管理文件

用户可以在 SFTP 客户端上显示 SFTP 服务器指定远程目录或文件的信息，或者删除 SFTP 服务器上的指定文件。

背景信息

说明

当 SFTP 客户端登录到 SSH 服务器之后，在 SFTP 客户端可以改变文件名、删除文件、显示文件列表、上传，下载文件。

请在作为 SSH 客户端的交换机上进行如下的配置。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 根据 SSH 服务器的地址类型，选择执行如下 2 个配置之一。

- 如果是 IPv4 类型的地址

  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。

- 如果是 IPv6 类型的地址

  执行命令 **sftp ipv6** [**-a** *source-address*] *host-ipv6* [**-i** *interface-type interface-number*] [*port*] [[**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。

步骤 3 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。

----结束

9.6.7 （可选）SFTP 客户端命令帮助

用户而可以查看 SFTP 客户端命令帮助。

背景信息

请在作为 SSH 客户端的交换机上进行如下的配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 根据 SSH 服务器的地址类型，选择执行如下 2 个配置之一。

- 如果是 IPv4 类型的地址

  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。

- 如果是 IPv6 类型的地址

  执行命令 **sftp ipv6** [**-a** *source-address*] *host-ipv6* [**-i** *interface-type interface-number*] [*port*] [[**prefer_kex** { **dh_group1** | **dh_exchange_group** }] | [**prefer_ctos_cipher**

版权所有 © 华为技术有限公司

{ **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。

步骤 3 执行命令 **help** [**all** | *command-name*]，显示 SFTP 客户端命令帮助。

----结束

9.6.8 检查配置结果

SFTP 客户端功能配置成功后，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 SFTP 客户端功能的所有配置

背景信息

- 使用 **display ssh server-info** 命令在 SSH 客户端查看 SSH 服务器与 RSA 公钥之间的对应关系。
- 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。

任务示例

运行命令 **display ssh server session**，可以看到客户端从 VTY4 登录上来，服务方式是 **sftp**，验证方式是 **rsa** 等。

```
<Quidway> display ssh server session
Session 2:
       Conn                 : VTY 4
       Version              : 2.0
       State                : started
       Username             : client002
       Retry                : 1
       CTOS Cipher          : aes128-cbc
       STOC Cipher          : aes128-cbc
       CTOS Hmac            : hmac-sha1-96
       STOC Hmac            : hmac-sha1-96
       Kex                  : diffie-hellman-group1-sha1
       Service Type         : sftp
       Authentication Type  : rsa
```

9.7 配置举例

配置 Telnet 及 SSH 的应用的示例。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。

9.7.1 配置 Telnet 终端服务示例
在本示例中，通过配置用户验证方式和密码，实现 Telnet 登录。

9.7.2 配置 PC 作为 STelnet 客户端连接 SSH 服务器的示例
配置 PC 作为 STelnet 客户端连接 SSH 服务器的示例。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 Stelnet 服务，实现 Stelnet 客户端连接 SSH 服务器。

华为专有和保密信息
版权所有 © 华为技术有限公司

9.7.3 配置交换机作为 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。

9.7.4 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。

9.7.5 配置 SSH 服务器支持其他端口号访问的示例
配置 SSH 服务器支持其他端口号访问的示例。在本示例中，通过设定 SSH 服务器端的监听端口号为其他端口号，实现只有合法的用户才能建立 SSH 连接。

9.7.6 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。

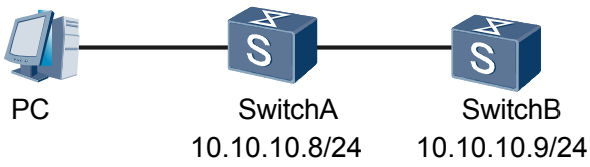
9.7.1 配置 Telnet 终端服务示例

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 9-3，用户登录到 SwitchA 后，通过在 SwitchA 上的 Telnet 程序登录到 SwitchB（使用默认接口号 23）。

图 9-3 Ethernet 网络用户远程登录组网图



Switch	接口	对应的 VLANIF	IP 地址
SwitchA	GigabitEthernet0/0/1	VLANIF 2	10.10.10.8/24
SwitchB	GigabitEthernet0/0/1	VLANIF 2	10.10.10.9/24

配置思路

采用如下的思路配置 Telnet 终端服务：

1. 在 SwitchA 和 SwitchB 上配置 IP 地址。
2. 在 SwitchB 上配置 Telnet 验证方式和密码。
3. 从 SwitchA 登录到 SwitchB 上。

数据准备

为完成此配置举例，需准备以下数据：

版权所有 © 华为技术有限公司

- VLAN 的 ID
- Telnet 客户端 SwitchA 的 IP 地址和接口号
- Telnet 服务器 SwitchB 的 IP 地址和接口号
- SwitchB Telnet 登录的验证方式和密码

操作步骤

步骤 1 配置 IP 地址

配置 Telnet 客户端 SwitchA 的 IP 地址。

```
<SwitchA> system-view
[SwitchA] vlan 2
[SwitchA-vlan2] quit
[SwitchA] interface GigabitEthernet 0/0/1
[SwitchA-GigabitEthernet0/0/1] port hybrid pvid vlan 2
[SwitchA-GigabitEthernet0/0/1] port hybrid untagged vlan 2
[SwitchA-GigabitEthernet0/0/1] quit
[SwitchA] interface vlanif 2
[SwitchA-Vlanif2] ip address 10.10.10.8 255.255.255.0
[SwitchA-Vlanif2] quit
[SwitchA]
```

配置 Telnet 服务器 SwitchB 的 IP 地址。

```
<SwitchB> system-view
[SwitchB] vlan 2
[SwitchB-vlan2] quit
[SwitchB] interface GigabitEthernet 0/0/1
[SwitchB-GigabitEthernet0/0/1] port hybrid pvid vlan 2
[SwitchB-GigabitEthernet0/0/1] port hybrid untagged vlan 2
[SwitchB-GigabitEthernet0/0/1] quit
[SwitchB] interface vlanif 2
[SwitchB-Vlanif2] ip address 10.10.10.9 255.255.255.0
[SwitchB-Vlanif2] quit
[SwitchB]
```

步骤 2 配置 Telnet 服务器 SwitchB 的 Telnet 验证方式和密码

```
[SwitchB] user-interface vty 0 4
[SwitchB-ui-vty0-4] authentication-mode password
[SwitchB-ui-vty0-4] set authentication password simple 123456
[SwitchB-ui-vty0-4] quit
[SwitchB]
```

步骤 3 检查配置结果

从 SwitchA 上 Telnet 到 SwitchB。

```
<SwitchA> telnet 10.10.10.9
Trying 10.10.10.9 ...
Press CTRL+K to abort
Connected to 10.10.10.9 ...

Login authentication


Password:
info: The max number of VTY users is 20, and the current number
      of VTY users on line is 1.
<SwitchB>
```

----结束

华为专有和保密信息
版权所有 © 华为技术有限公司

配置文件

- SwitchA 的配置文件

```
#
 sysname SwitchA
#
 vlan batch 2
#
interface Vlanif2
 ip address 10.10.10.8 255.255.255.0
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 2
 port hybrid untagged vlan 2
#
return
```

- SwitchB 的配置文件

```
#
 sysname SwitchB
#
 vlan batch 2
#
interface Vlanif2
 ip address 10.10.10.9 255.255.255.0
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 2
 port hybrid untagged vlan 2
#
user-interface vty 0 4
set authentication password simple 123456
#
return
```

9.7.2 配置 PC 作为 STelnet 客户端连接 SSH 服务器的示例

配置 PC 作为 STelnet 客户端连接 SSH 服务器的示例。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 Stelnet 服务，实现 Stelnet 客户端连接 SSH 服务器。

组网需求

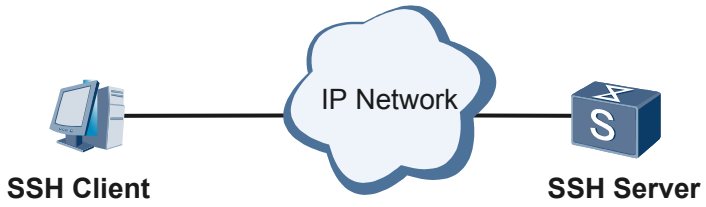
如图 9-4 所示，SSH 服务器端 STelnet 服务使能后，STelnet 客户端可以通过 Password、RSA、password-rsa 或 all 认证的方式登录到 SSH 服务器端。

配置登录用户 Client001，密码为“huawei”，登录验证方式为 password。

服务器端 IP 地址是 192.168.1.1。

用户界面仅支持 SSH 协议。

图 9-4 配置 PC 作为 STelnet 客户端连接 SSH 服务器组网图



版权所有 © 华为技术有限公司

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. 用户 Client001 的配置在 SSH 服务器上完成。
2. SSH 服务器端 STelnet 服务使能。
3. 配置 SSH 服务器端缺省的认证方式为 password。

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。
- SSH 服务器名。

操作步骤

步骤 1 在服务器端生成本地密钥对

```
<Quidway> system-view
[Quidway] sysname SSH Server
[SSH Server] rsa local-key-pair create
The key name will be: Quidway_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 S5700 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 cipher huawei
[SSH Server-aaa] local-user client001 privilege level 3
[SSH Server-aaa] local-user client001 service-type ssh
[SSH Server-aaa] quit
```

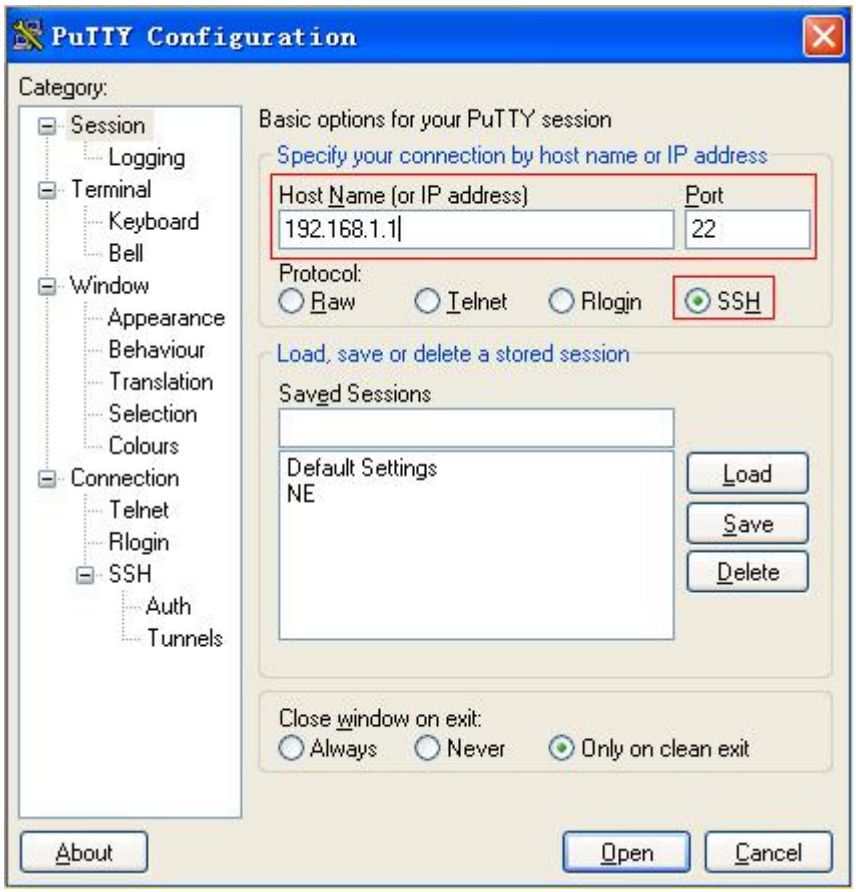
步骤 4 使能 STelent 功能，并配置用户的服务类型为 STelnet

```
[SSH Server] stelnet server enable
[SSH Server] ssh authentication-type default password
```

步骤 5 验证配置结果

通过 putty 软件登录设备，指定设备的 IP 地址 192.168.1.1，并指定登录方式为 SSH。

华为专有和保密信息
版权所有 © 华为技术有限公司



通过 putty 软件登录设备，输入用户名和密码，用户名 client001，密码 huawei。

版权所有 © 华为技术有限公司

----结束

配置文件

- SSH 服务器的配置文件

```
#
 sysname SSH Server
#
aaa
 local-user client001 password cipher huawei
local-user client001 privilege level 3
 local-user client001 service-type ssh
#
 stelnet server enable
 ssh authentication-type default password
#
user-interface vty 0 4
 authentication-mode aaa
 protocol inbound ssh
#
return
```

9.7.3 配置交换机作为 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

当需要从一台交换机登录到其他交换机进行配置时，可以配置交换机作为 STelnet 客户端连接待配置的交换机。

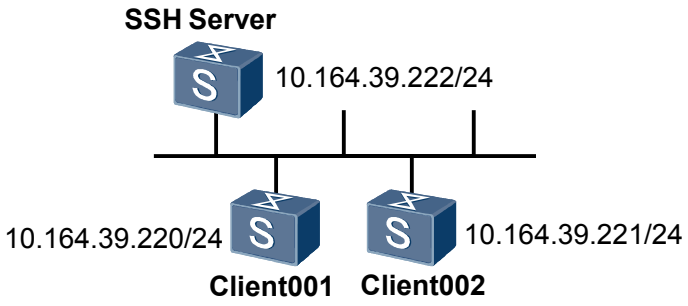
如图 9-5 所示，SSH 服务器端 STelnet 服务使能后，STelnet 客户端可以通过 Password、RSA、password-rsa 或 all 认证的方式登录到 SSH 服务器端。

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 9-5 配置 STelnet 客户端连接 SSH 服务器组网图



Switch	接口	对应的 VLANIF	IP 地址

华为专有和保密信息
版权所有 © 华为技术有限公司

SSH server	GigabitEthernet0/0/1	VLANIF 10	10.164.39.222/24
Client001	GigabitEthernet0/0/1	VLANIF 10	10.164.39.220/24
Client002	GigabitEthernet0/0/1	VLANIF 10	10.164.39.221/24

配置思路

采用如下的思路配置 STelnet 客户端连接 SSH 服务器：

1. 配置各接口所属 VLAN 以及对应 VLANIF 接口的 IP 地址。
2. 用户 Client001 和 Client002 的配置均在 SSH 服务器上完成。
3. 分别在 STelnet 客户端和 SSH 服务器端生成本地密钥对。
4. 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。
5. SSH 服务器端 STelnet 服务使能。
6. 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：

- FTP 服务器端和客户端的 IP 地址及所属 VLAN，具体请参见图 9-5。
- 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 配置接口所属 VLAN 和对应 VLANIF 接口的 IP 地址。

在作为服务器的 Switch 上创建 VLAN 10，并配置接口 VLANIF10 的 IP 地址为 10.164.39.222/24。

```
<Quidway> system-view
[Quidway]sysname Quidway
[Quidway] vlan 10
[Quidway] quit
[Quidway] interface GigabitEthernet 0/0/1
[Quidway-GigabitEthernet0/0/1] port hybrid pvid vlan 10
[Quidway-GigabitEthernet0/0/1] port hybrid untagged vlan 10
[Quidway-GigabitEthernet0/0/1] quit
[Quidway] interface vlanif 10
[Quidway-Vlanif10] ip address 10.164.39.222 24
```

作为客户端 Client001、Client002 的 Switch 的 IP 地址配置同上（略）。

步骤 2 在服务器端生成本地密钥对

```
<Quidway> system-view
[Quidway] rsa local-key-pair create
The key name will be: Quidway_Host
The range of public key size is (512 ~ 2048).
info: If the key modulus is greater than 512,
       It will take a few minutes.
```


版权所有 © 华为技术有限公司

```
Input the bits in the modulus[default = 512]:
Generating keys...
.......++++++++++++
..........++++++++++++
.................................++++++++
......++++++++
```

步骤 3 在服务器端创建 SSH 用户

说明

SSH 用户主要有 password、RSA、password-rsa、all 这 4 种认证方式:

- 如果 SSH 用户的认证方式为 password、password-rsa 时，必须配置同名的 local-user 用户;
- 如果 SSH 用户的认证方式为 RSA、password-rsa、all，服务器端应保存 SSH 客户端的 RSA 公钥。

配置 VTY 用户界面。

```
[Quidway] user-interface vty 0 4
[Quidway-ui-vty0-4] authentication-mode aaa
[Quidway-ui-vty0-4] protocol inbound ssh
[Quidway-ui-vty0-4] quit
```

- 创建 SSH 用户 Client001。

  # 新建用户名为 Client001 的 SSH 用户，且认证方式为 password。

  ```
  [Quidway] ssh user client001
  [Quidway] ssh user client001 authentication-type password
  ```

  # 为 SSH 用户 Client001 配置密码为 huawei。

  ```
  [Quidway] aaa
  [Quidway-aaa] local-user client001 password simple huawei
  [Quidway-aaa] local-user client001 service-type ssh
  ```

- 新建用户名为 Client002 的 SSH 用户，且认证方式为 RSA。

  ```
  [Quidway] ssh user client002
  [Quidway] ssh user client002 authentication-type rsa
  ```

步骤 4 配置服务器端 RSA 公钥

客户端生成客户端的本地密钥对

```
<Quidway> system-view
[Quidway] 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: 16:38:51  2007/5/25
Key name: client002_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
Host public key for PEM format code:
---- BEGIN SSH2 PUBLIC KEY ----
AAAAB3NzaC1yc2EAAAADAQABAAAAQQC/815LxhvXhvkHtd59Z3DD5f0XqyA8j8u7
yP3y98tnTlGehBkPa5eo6pH8S7nhiDZedL/VTGh3Z6icaOMdfj4b
---- END SSH2 PUBLIC KEY ----
Public key code for pasting into OpenSSH authorized_keys file :
```


华为专有和保密信息
版权所有 © 华为技术有限公司

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAAAQQC/815LxhvXhvkHtd59Z3DD5f0XqyA8j8u7yP3y98tn
TlGehBkPa5eo6pH8S7nhiDZedL/VTGh3Z6ica0Mdfj4b rsa-key

=================================================
Time of Key pair created: 16:38:51  2007/5/25
Key name: client002_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。

```
[Quidway] rsa peer-public-key RsaKey001
Enter "RSA public key" view, return system view with "peer-public-key end".
[Quidway-rsa-public-key] public-key-code begin
Enter "RSA key code" view, return last view with "public-key-code end".
[Quidway-rsa-key-code] 3047
[Quidway-rsa-key-code] 0240
[Quidway-rsa-key-code] BFF35E4B C61BD786 F907B5DE 7D6770C3 E5FD17AB
[Quidway-rsa-key-code] 203C8FCB BBC8FDF2 F7CB674E 519E8419 0F6B97A8
[Quidway-rsa-key-code] EA91FC4B B9E18836 5E74BFD5 4C687767 A89C6B43
[Quidway-rsa-key-code] 1D7E3E1B
[Quidway-rsa-key-code] 0203
[Quidway-rsa-key-code] 010001
[Quidway-rsa-key-code] public-key-code end
[Quidway-rsa-public-key] peer-public-key end
```

步骤 5 为 SSH 用户 Client002 绑定 SSH 客户端的 RSA 公钥

```
[Quidway] ssh user client002 assign rsa-key RsaKey001
```

步骤 6 SSH 服务器端 STelnet 服务使能

使能 STelnet 服务功能。

```
[Quidway] stelnet server enable
```

步骤 7 配置 SSH 用户 Client001、Client002 的服务方式为 STelnet

```
[Quidway] ssh user client001 service-type stelnet
[Quidway] ssh user client002 service-type stelnet
```

步骤 8 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。

```
[client001] ssh client first-time enable
[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 ...
The server is not authenticated. Continue to access it?(Y/N):y
Save the server's public key?(Y/N):y
```


版权所有 © 华为技术有限公司

```
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 20, and the current number
      of VTY users on line is 1.
<Quidway>
```

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 ...

info: The max number of VTY users is 20, and the current number
      of VTY users on line is 1.
<Quidway>
```

步骤 9 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 STelnet 服务已经使能，并且 STelnet 客户端已经成功连接到 SSH 服务器。

查看 SSH 状态信息。

```
[Quidway] 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: Disable
 STELNET server: Enable
```

查看 SSH 服务器的连接信息。

```
[Quidway] display ssh server session
Session 1:
       Conn: VTY 3
       Version: 2.0
       State: started
       Username: client001
       Retry: 1
       CTOS Cipher: aes128-cbc
       STOC Cipher: aes128-cbc
       CTOS Hmac: hmac-sha1-96
       STOC Hmac: hmac-sha1-96
       Kex: diffie-hellman-group1-sha1
       Service Type: stelnet
       Authentication Type: password
Session 1:
       Conn: VTY 4
       Version: 2.0
       State: started
       Username: client002
       Retry: 1
       CTOS Cipher: aes128-cbc
       STOC Cipher: aes128-cbc
       CTOS Hmac: hmac-sha1-96
       STOC Hmac: hmac-sha1-96
       Kex: diffie-hellman-group1-sha1
       Service Type: stelnet
       Authentication Type: rsa
```


版权所有 © 华为技术有限公司

查看 SSH 用户信息。

```
[Quidway] display ssh user-information
User 1:
       User Name: client001
       Authentication-type: password
       User-public-key-name: -
       Sftp-directory: -
       Service-type: stelnet
       Authorization-cmd: No
  User 2:
       User Name: client002
       Authentication-type: rsa
       User-public-key-name: RsaKey001
       Sftp-directory: -
       Service-type: stelnet
       Authorization-cmd: No
```

----结束

配置文件

- SSH 服务器 Quidway 上的配置文件

```
#
 sysname Quidway
#
 vlan batch 10
#
interface Vlanif10
 ip address 10.164.39.222 255.255.255.0
#
 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 simple huawei
 local-user client001 service-type ssh
#
stelnet server enable
 ssh user client001
 ssh user client002
 ssh user client001 authentication-type password
 ssh user client002 authentication-type rsa
 ssh user client002 assign rsa-key RsaKey001
 ssh user client001 service-type stelnet
 ssh user client002 service-type stelnet
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
user-interface vty 0 4
 authentication-mode aaa
 protocol inbound ssh
#
return
```

- SSH 客户端 Client001 的配置文件

```
#
 sysname client001
#
```


版权所有 © 华为技术有限公司

```
 vlan batch 10
#
interface Vlanif10
 ip address 10.164.39.220 255.255.255.0
#
ssh client first-time enable
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
return
```

- SSH 客户端 Client002 的配置文件

```
#
 sysname client002
#
 vlan batch 10
#
interface Vlanif10
 ip address 10.164.39.221 255.255.255.0
#
ssh client first-time enable
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
return
```

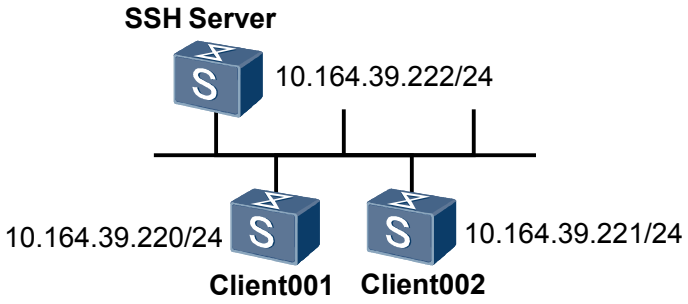
9.7.4 配置 SFTP 客户端连接 SSH 服务器的示例

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 9-6 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 9-6 配置 SFTP 客户端连接 SSH 服务器组网图



Switch	接口	对应的 VLANIF	IP 地址
SSH server	GigabitEthernet0/0/1	VLANIF 10	10.164.39.222/24
Client001	GigabitEthernet0/0/1	VLANIF 10	10.164.39.220/24
Client002	GigabitEthernet0/0/1	VLANIF 10	10.164.39.221/24

华为专有和保密信息
版权所有 © 华为技术有限公司

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. 配置各接口所属 VLAN 以及对应 VLANIF 接口的 IP 地址。
2. 用户 Client001 和 Client002 的配置均在 SSH 服务器上完成。
3. 分别在 SFTP 客户端和 SSH 服务器端生成本地密钥对。
4. 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。
5. SSH 服务器端 SFTP 服务使能。
6. 配置 SSH 用户的服务方式和授权目录。
7. 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：

- FTP 服务器端和客户端的 IP 地址及所属 VLAN，具体请参见图 9-6。
- 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 配置接口所属 VLAN 和对应 VLANIF 接口的 IP 地址。

在作为服务器的 Switch 上创建 VLAN 10，并配置 VLAN 10 的接口 IP 地址为 10.164.39.222/24。

```
<Quidway> system-view
[Quidway] vlan 10
[Quidway] quit
[Quidway] interface GigabitEthernet 0/0/1
[Quidway-GigabitEthernet0/0/1] port hybrid pvid vlan 10
[Quidway-GigabitEthernet0/0/1] port hybrid untagged vlan 10
[Quidway-GigabitEthernet0/0/1] quit
[Quidway] interface vlanif 10
[Quidway-Vlanif10] ip address 10.164.39.222 24
```

作为客户端 Client001、Client002 的 Switch 的 IP 地址配置同上（略）。

步骤 2 在服务器端生成本地密钥对

```
<Quidway> system-view
[Quidway] rsa local-key-pair create
The key name will be: Quidway_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]:
Generating keys...
..........++++++++++++
.................++++++++++++
...++++++++
..........++++++++
```

步骤 3 在服务器端创建 SSH 用户

版权所有 © 华为技术有限公司

说明

SSH 用户主要有 password、RSA、password-rsa、all 这 4 种认证方式:

- 如果 SSH 用户的认证方式为 password、password-rsa 时，必须配置同名的 local-user 用户;
- 如果 SSH 用户的认证方式为 RSA、password-rsa、all，服务器端应保存 SSH 客户端的 RSA 公钥。

配置 VTY 用户界面。

```
[Quidway] user-interface vty 0 4
[Quidway-ui-vty0-4] authentication-mode aaa
[Quidway-ui-vty0-4] protocol inbound ssh
[Quidway-ui-vty0-4] quit
```

- 创建 SSH 用户 Client001。

  # 新建用户名为 Client001 的 SSH 用户，且认证方式为 password。

  ```
  [Quidway] ssh user client001
  [Quidway] ssh user client001 authentication-type password
  ```

  # 为 SSH 用户 Client001 配置密码为 huawei。

  ```
  [Quidway] aaa
  [Quidway-aaa] local-user client001 password simple huawei
  [Quidway-aaa] local-user client001 service-type ssh
  ```

- 新建用户名为 Client002 的 SSH 用户，且认证方式为 RSA。

  ```
  [Quidway] ssh user client002
  [Quidway] ssh user client002 authentication-type rsa
  ```

步骤 4 配置服务器端 RSA 公钥

客户端生成客户端的本地密钥对

```
<Quidway> system-view
[Quidway] 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: 16:38:51  2007/5/25
Key name: client002_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
Host public key for PEM format code:
---- BEGIN SSH2 PUBLIC KEY ----
AAAAB3NzaC1yc2EAAAADAQABAAAAQQC/815LxhvXhvkHtd59Z3DD5f0XqyA8j8u7
yP3y98tnTlGehBkPa5eo6pH8S7nhiDZedL/VTGh3Z6ica0Mdfj4b
---- END SSH2 PUBLIC KEY ----
Public key code for pasting into OpenSSH authorized_keys file :
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAAAQQC/815LxhvXhvkHtd59Z3DD5f0XqyA8j8u7yP3y98tn
TlGehBkPa5eo6pH8S7nhiDZedL/VTGh3Z6ica0Mdfj4b rsa-key

=====================================================
Time of Key pair created: 16:38:51  2007/5/25
Key name: client002_Server
Key type: RSA encryption Key
=====================================================
```


华为专有和保密信息
版权所有 © 华为技术有限公司

```
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。

```
[Quidway] rsa peer-public-key RsaKey001
Enter "RSA public key" view, return system view with "peer-public-key end".
[Quidway-rsa-public-key] public-key-code begin
Enter "RSA key code" view, return last view with "public-key-code end".
[Quidway-rsa-key-code] 3047
[Quidway-rsa-key-code] 0240
[Quidway-rsa-key-code] BFF35E4B C61BD786 F907B5DE 7D6770C3 E5FD17AB
[Quidway-rsa-key-code] 203C8FCB BBC8FDF2 F7CB674E 519E8419 0F6B97A8
[Quidway-rsa-key-code] EA91FC4B B9E18836 5E74BFD5 4C687767 A89C6B43
[Quidway-rsa-key-code] 1D7E3E1B
[Quidway-rsa-key-code] 0203
[Quidway-rsa-key-code] 010001
[Quidway-rsa-key-code] public-key-code end
[Quidway-rsa-public-key] peer-public-key end
```

步骤 5 为 SSH 用户 Client002 绑定 SSH 客户端的 RSA 公钥

```
[Quidway] ssh user client002 assign rsa-key RsaKey001
```

步骤 6 SSH 服务器端 SFTP 服务使能

使能 SFTP 服务功能

```
[Quidway] sftp server enable
```

步骤 7 在 SSH 服务器端配置 SSH 用户的服务方式和授权目录

目前 SSH 服务器端已配置了两个 SSH 用户：Client001 和 Client002，Client001 的认证方式是 password，Client002 的认证方式是 RSA。

```
[Quidway] ssh user client001 service-type sftp
[Quidway] ssh user client001 sftp-directory flash:/
[Quidway] ssh user client002 service-type sftp
[Quidway] ssh user client002 sftp-directory flash:/
```

步骤 8 SFTP 客户端连接 SSH 服务器

第一次登录，则需要使能 SSH 客户端首次认证功能。

```
[client001] ssh client first-time enable
[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
Input Username:client001
Trying 10.164.39.222 ...
Press CTRL+K to abort
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
```


版权所有 © 华为技术有限公司

```
Input Username: client002
Trying 10.164.39.222 ...
Press CTRL+K to abort
sftp-client>
```

步骤 9 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。

```
[Quidway] display ssh server status
SSH version : 1.99
 SSH connection timeout : 60 seconds
 SSH server key generating interval : 0 hours
 SSH Authentication retries : 3 times
 SFTP server: Enable
STELNET server: Disable
```

查看 SSH 服务器的连接信息。

```
[Quidway] display ssh server session
Session 1:
       Conn: VTY 3
       Version: 2.0
       State: started
       Username: client001
       Retry: 1
       CTOS Cipher: aes128-cbc
       STOC Cipher: aes128-cbc
       CTOS Hmac: hmac-sha1-96
       STOC Hmac: hmac-sha1-96
       Kex: diffie-hellman-group1-sha1
       Service Type: sftp
       Authentication Type: password
Session 2:
       Conn: VTY 4
       Version: 2.0
       State: started
       Username: client002
       Retry: 1
       CTOS Cipher: aes128-cbc
       STOC Cipher: aes128-cbc
       CTOS Hmac: hmac-sha1-96
       STOC Hmac: hmac-sha1-96
       Kex: diffie-hellman-group1-sha1
       Service Type: sftp
       Authentication Type: rsa
```

查看 SSH 用户信息。

```
[Quidway] display ssh user-information
User 1:
       User Name: client001
       Authentication-type: password
       User-public-key-name: -
       Sftp-directory: flash:
       Service-type: sftp
       Authorization-cmd: No
  User 2:
       User Name: client002
       Authentication-type: rsa
       User-public-key-name: RsaKey001
       Sftp-directory: flash:
       Service-type: sftp
       Authorization-cmd: No
```

----结束

华为专有和保密信息
版权所有 © 华为技术有限公司

配置文件

- SSH 服务器 Quidway 上的配置文件

```
#
 sysname Quidway
#
 vlan batch 10
#
interface Vlanif10
 ip address 10.164.39.222 255.255.255.0
#
 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 simple huawei
 local-user client001 service-type ssh
#
sftp server enable
ssh user client001
 ssh user client002
 ssh user client001 authentication-type password
 ssh user client002 authentication-type rsa
 ssh user client002 assign rsa-key RsaKey001
ssh user client001 service-type sftp
 ssh user client002 service-type sftp
ssh user client001 sftp-directory flash:/
ssh user client002 sftp-directory flash:/
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
user-interface vty 0 4
 authentication-mode aaa
 protocol inbound ssh
#
return
```

- SSH 客户端 Clien001 的配置文件

```
#
 sysname client001
#
 vlan batch 10
#
interface Vlanif10
 ip address 10.164.39.220 255.255.255.0
#
ssh client first-time enable
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
return
```

- SSH 客户端 Clien002 的配置文件

```
#
 sysname client002
#
 vlan batch 10
```


版权所有 © 华为技术有限公司

```
#
interface Vlanif10
 ip address 10.164.39.221 255.255.255.0
#
ssh client first-time enable
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
return
```

9.7.5 配置 SSH 服务器支持其他端口号访问的示例

配置 SSH 服务器支持其他端口号访问的示例。在本示例中，通过设定 SSH 服务器端的监听端口号为其他端口号，实现只有合法的用户才能建立 SSH 连接。

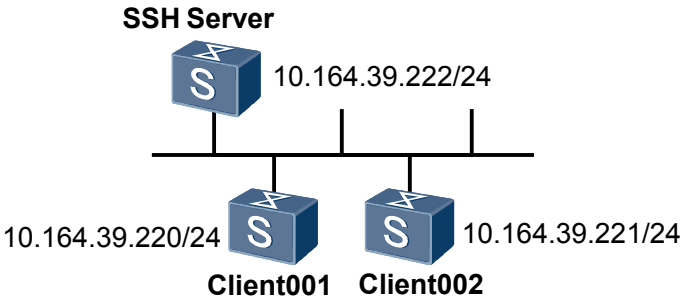
组网需求

SSH 协议的标准监听端口号为 22，如果攻击者不断访问标准端口，导致带宽和服务器性能的下降，导致其他正常用户无法访问。

通过设定 SSH 服务器端的监听端口号为其他端口号，攻击者不知道 SSH 监听端口号的更改，仍然发送标准端口号 22 的 socket 连接，SSH 服务器检测发现请求连接端口号不是监听的端口号，就不建立 socket 连接。

这样只有合法的用户采用 SSH 服务器设定的非标准监听端口才能建立 socket 连接，进行 SSH 协议的版本号协商、算法协商及会话密钥生成、认证、会话请求、会话阶段等过程。

图 9-7 配置 SSH 服务器支持其他端口号访问组网图



Switch	接口	对应的 VLANIF	IP 地址
SSH server	GigabitEthernet0/0/1	VLANIF 10	10.164.39.222/24
Client001	GigabitEthernet0/0/1	VLANIF 10	10.164.39.220/24
Client002	GigabitEthernet0/0/1	VLANIF 10	10.164.39.221/24

配置思路

采用如下的思路配置 SSH 服务器支持其他端口号访问的示例：

1. 配置各接口所属 VLAN 以及对应 VLANIF 接口的 IP 地址。

华为专有和保密信息
版权所有 © 华为技术有限公司

2. 用户 Client001 和 Client002 的配置均在 SSH 服务器上完成。
3. 分别在 SFTP 客户端和 SSH 服务器端生成本地密钥对。
4. 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。
5. SSH 服务器端 STelnet 和 SFTP 服务使能。
6. 配置 SSH 用户的服务方式和授权目录。
7. 设置 SSH 服务器端监听端口号。
8. 用户 Client001 和 Client002 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：

- FTP 服务器端和客户端的 IP 地址及所属 VLAN，具体请参见图 9-7。
- SSH 用户名及认证方式。
- SSH 用户密码或 RSA 公钥。
- 服务器名。
- SSH 服务器端监听端口号。

操作步骤

步骤 1 配置接口所属 VLAN 和对应 VLANIF 接口的 IP 地址。

在作为服务器的 Switch 上创建 VLAN 10，并配置 VLAN 10 的接口 IP 地址为 10.164.39.222/24。

```
<Quidway> system-view
[Quidway] vlan 10
[Quidway-vlan10] quit
[Quidway] interface GigabitEthernet 0/0/1
[Quidway-GigabitEthernet0/0/1] port hybrid pvid vlan 10
[Quidway-GigabitEthernet0/0/1] port hybrid untagged vlan 10
[Quidway-GigabitEthernet0/0/1] quit
[Quidway] interface vlanif 10
[Quidway-Vlanif10] ip address 10.164.39.222 24
[Quidway-Vlanif10] quit
```

作为客户端 Client001、Client002 的 Switch 的 IP 地址配置同上（略）。

步骤 2 在服务器端生成本地密钥对

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

步骤 3 配置服务器端 RSA 公钥

在客户端生成客户端的本地密钥对

版权所有 © 华为技术有限公司

```
<Quidway> system-view
[Quidway] 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: 16:38:51  2007/5/25
Key name: client002_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
Host public key for PEM format code:
---- BEGIN SSH2 PUBLIC KEY ----
AAAAB3NzaC1yc2EAAAADAQABAAAAQQC/815LxhvXhvkHtd59Z3DD5f0XqyA8j8u7
yP3y98tnTlGehBkPa5eo6pH8S7nhiDZedL/VTGh3Z6ica0Mdfj4b
---- END SSH2 PUBLIC KEY ----
Public key code for pasting into OpenSSH authorized_keys file :
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAAAQQC/815LxhvXhvkHtd59Z3DD5f0XqyA8j8u7yP3y98tn
TlGehBkPa5eo6pH8S7nhiDZedL/VTGh3Z6ica0Mdfj4b rsa-key

=====================================================
Time of Key pair created: 16:38:51  2007/5/25
Key name: client002_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]
```

在服务器端将客户端上产生的 RSA 公钥传送到服务器端。

```
[Quidway] rsa peer-public-key RsaKey001
Enter "RSA public key" view, return system view with "peer-public-key end".
[Quidway-rsa-public-key] public-key-code begin
Enter "RSA key code" view, return last view with "public-key-code end".
[Quidway-rsa-key-code] 3047
[Quidway-rsa-key-code] 0240
[Quidway-rsa-key-code] BFF35E4B C61BD786 F907B5DE 7D6770C3 E5FD17AB
[Quidway-rsa-key-code] 203C8FCB BBC8FDF2 F7CB674E 519E8419 0F6B97A8
[Quidway-rsa-key-code] EA91FC4B B9E18836 5E74BFD5 4C687767 A89C6B43
[Quidway-rsa-key-code] 1D7E3E1B
[Quidway-rsa-key-code] 0203
[Quidway-rsa-key-code] 010001
[Quidway-rsa-key-code] public-key-code end
[Quidway-rsa-public-key] peer-public-key end
```

步骤 4 在服务器端创建 SSH 用户

华为专有和保密信息
版权所有 © 华为技术有限公司

说明

SSH 用户主要有 password、RSA、password-rsa、all 这 4 种认证方式。

- 如果 SSH 用户的认证方式为 password、password-rsa 时，必须配置同名的 local-user 用户；
- 如果 SSH 用户的认证方式为 RSA、password-rsa、all，服务器端应保存 SSH 客户端的 RSA 公钥。

配置 VTY 用户界面。

```
[Quidway] user-interface vty 0 4
[Quidway-ui-vty0-4] authentication-mode aaa
[Quidway-ui-vty0-4] protocol inbound ssh
[Quidway-ui-vty0-4] quit
```

创建 SSH 用户 Client001，新建用户名为 Client001 的 SSH 用户，且认证方式为 password。

```
[Quidway] ssh user client001
[Quidway] ssh user client001 authentication-type password
```

为 SSH 用户 Client001 配置密码为 huawei。

```
[Quidway] aaa
[Quidway-aaa] local-user client001 password simple huawei
[Quidway-aaa] local-user client001 service-type ssh
[Quidway-aaa] quit
```

配置 Client001 的服务方式为 STelnet。

```
[Quidway] ssh user client001 service-type stelnet
```

新建用户名为 Client002 的 SSH 用户，且认证方式为 RSA，并绑定 SSH 客户端 RSA 公钥。

```
[Quidway] ssh user client002
[Quidway] ssh user client002 authentication-type rsa
[Quidway] ssh user client002 assign rsa-key RsaKey001
```

配置 Client002 的服务方式为 SFTP，授权目录为 flash:/。

```
[Quidway] ssh user client002 service-type sftp
[Quidway] ssh user client002 sftp-directory flash:/
```

步骤 5 SSH 服务器端使能 STelent 和 SFTP 服务

```
[Quidway] stelnet server enable
[Quidway] sftp server enable
```

步骤 6 配置 SSH 服务端新的监听端口号

```
[Quidway] ssh server port 1025
```

步骤 7 SSH 客户端连接 SSH 服务器

第一次登录，则需要使能 SSH 客户端首次认证功能。

```
[client001] ssh client first-time enable
[client002] ssh client first-time enable
```

STelnet 客户端用新端口号连接 SSH 服务器。

```
[client001] stelnet 10.164.39.222 1025
Please input the username:client001
Trying 10.164.39.222 ...
Press CTRL+K to abort
Connected to 10.164.39.222 ...
he server is not authenticated. Do you continue to access it?(Y/N):y
Do you want to save the server's public key?(Y/N):y
```


版权所有 © 华为技术有限公司

```
he 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 20, and the current number
      of VTY users on line is 1.
<Quidway>
```

SFTP 客户端用新端口号连接 SSH 服务器。

```
[client002]sftp 10.164.39.222 1025
Input Username:client002
Trying 10.164.39.222 ...
Press CTRL+K to abort
The server's public key does not match the one we cached.
The server is not authenticated. Do you continue to access it?(Y/N):y
Do you want to update the server's public key we cached?(Y/N):y
sftp-client>
```

步骤 8 检查配置结果

攻击者使用原端口号 22 访问 SSH 服务器，不能成功。

```
[client002] sftp 10.164.39.222
Input Username:client002
Trying 10.164.39.222 ...
Press CTRL+K to abort
Can't establish tcp connection to server
```

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 SSH 服务器端当前监听端口号，并且 STelnet 客户端或 SFTP 客户端已经成功连接到 SSH 服务器。

查看 SSH 状态信息。

```
[Quidway] 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
 SSH server port: 1025
```

查看 SSH 服务器的连接信息。

```
[Quidway] display ssh server session
Session 1:
       Conn: VTY 3
       Version: 2.0
       State: started
       Username: client001
       Retry: 1
       CTOS Cipher: aes128-cbc
       STOC Cipher: aes128-cbc
       CTOS Hmac: hmac-sha1-96
       STOC Hmac: hmac-sha1-96
       Kex: diffie-hellman-group1-sha1
       Service Type: stelnet
       Authentication Type: password
Session 2:
       Conn: VTY 4
       Version: 2.0
       State: started
       Username: client002
       Retry: 1
       CTOS Cipher: aes128-cbc
```


版权所有 © 华为技术有限公司

```
  STOC Cipher: aes128-cbc
  CTOS Hmac: hmac-sha1-96
  STOC Hmac: hmac-sha1-96
  Kex: diffie-hellman-group1-sha1
  Service Type: sftp
  Authentication Type: rsa
```

----结束

配置文件

- SSH 服务器 Quidway 上的配置文件

```
#
 sysname Quidway
#
 vlan batch 10
#
interface Vlanif10
 ip address 10.164.39.222 255.255.255.0
#
 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 simple huawei
 local-user client001 service-type ssh
#
 sftp server enable
 stelnet server enable
 ssh server port 1025
 ssh user client001
 ssh user client002
 ssh user client001 authentication-type password
 ssh user client002 authentication-type RSA
 ssh user client002 assign rsa-key RsaKey001
 ssh user client001 service-type stelnet
 ssh user client002 service-type sftp
 ssh user client002 sftp-directory flash:/
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
user-interface vty 0 4
 authentication-mode aaa
 protocol inbound ssh
#
return
```

- SSH 客户端 Clien001 的配置文件

```
#
 sysname client001
#
 vlan batch 10
#
interface Vlanif10
 ip address 10.164.39.220 255.255.255.0
#
 ssh client first-time enable
#
```


版权所有 © 华为技术有限公司

```
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
return
```

- SSH 客户端 Clien002 的配置文件

```
#
 sysname client002
#
 vlan batch 10
#
interface Vlanif10
 ip address 10.164.39.221 255.255.255.0
#
 ssh client first-time enable
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
return
```

9.7.6 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。

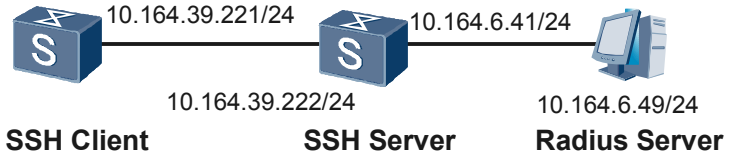
组网需求

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 9-8 所示。

图 9-8 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。

华为专有和保密信息
版权所有 © 华为技术有限公司

4. 分别在 STelnet 客户端和 SSH 服务器端生成本地密钥对。SSH 服务器端监听端口号。
5. 分别在客户端和 SSH 服务器端生成本地密钥对。
6. 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。
7. SSH 服务器端 STelnet 和 SFTP 服务使能。
8. 配置 SSH 用户的服务方式和授权目录。
9. 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：

- 配置两个 SSH 用户采用的认证方式是 Password。
- 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

```
<Quidway> system-view
[Quidway] rsa local-key-pair create
The key name will be: Quidway_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

```
<Quidway> system-view
[Quidway] 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: Quidway_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
```


版权所有 © 华为技术有限公司

```
    010001
Host public key for PEM format code:
---- BEGIN SSH2 PUBLIC KEY ----
AAAAB3NzaC1yc2EAAAADAQABAAAAQQC/815LxhvXhvkHtd59Z3DD5f0XqyA8j8u7
yP3y98tnTlGehBkPa5eo6pH8S7nhiDZedL/VTGh3Z6icaOMdfj4b
---- END SSH2 PUBLIC KEY ----
Public key code for pasting into OpenSSH authorized_keys file :
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAAAQQC/815LxhvXhvkHtd59Z3DD5f0XqyA8j8u7yP3y98tn
TlGehBkPa5eo6pH8S7nhiDZedL/VTGh3Z6icaOMdfj4b rsa-key
=====================================================
Time of Key pair created: 16:38:51  2007/5/25
Key name: Quidway_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。

```
[Quidway] rsa peer-public-key RsaKey001
Enter "RSA public key" view, return system view with "peer-public-key end".
[Quidway-rsa-public-key] public-key-code begin
Enter "RSA key code" view, return last view with "public-key-code end".
[Quidway-rsa-key-code] 3047
[Quidway-rsa-key-code] 0240
[Quidway-rsa-key-code] BFF35E4B C61BD786 F907B5DE 7D6770C3 E5FD17AB
[Quidway-rsa-key-code] 203C8FCB BBC8FDF2 F7CB674E 519E8419 0F6B97A8
[Quidway-rsa-key-code] EA91FC4B B9E18836 5E74BFD5 4C687767 A89C6B43
[Quidway-rsa-key-code] 1D7E3E1B
[Quidway-rsa-key-code] 0203
[Quidway-rsa-key-code] 010001
[Quidway-rsa-key-code] public-key-code end
[Quidway-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。

```
[Quidway] user-interface vty 0 4
[Quidway-ui-vty0-4] authentication-mode aaa
[Quidway-ui-vty0-4] protocol inbound ssh
[Quidway-ui-vty0-4] quit
```

在 SSH 服务器端创建 SSH 用户 ssh1@ssh.com 和 ssh2@ssh.com。

```
[Quidway] ssh user ssh1@ssh.com
[Quidway] ssh user ssh1@ssh.com authentication-type password
[Quidway] ssh user ssh1@ssh.com service-type stelnet
[Quidway] ssh user ssh2@ssh.com
[Quidway] ssh user ssh2@ssh.com authentication-type password
[Quidway] ssh user ssh2@ssh.com service-type sftp
```

步骤 4 配置 RADIUS 模板

配置认证方案 newscheme，认证方法为 RADIUS。

版权所有 © 华为技术有限公司

```
[Quidway] aaa
[Quidway-aaa] authentication-scheme newscheme
[Quidway-aaa-authen-newscheme] authentication-mode radius
[Quidway-aaa-authen-newscheme] quit
```

配置 SSH 服务端的 RADIUS 模板为 ssh。

```
[Quidway] 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。

```
[Quidway-radius-ssh] radius-server authentication 10.164.6.49 1812
```

配置 RADIUS 服务器密钥为 huawei。

```
[Quidway-radius-ssh] radius-server shared-key huawei
[Quidway-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。

```
[Quidway] aaa
[Quidway-aaa] domain ssh.com
[Quidway-aaa-domain-ssh.com] authentication-scheme newscheme
[Quidway-aaa-domain-ssh.com] radius-server ssh
[Quidway-aaa-domain-ssh.com] quit
[Quidway-aaa] quit
```

步骤 6 SSH 客户端连接 SSH 服务器。

使能 SSH 服务器端的 STelnet 和 SFTP 服务功能。

```
[Quidway] stelnet server enable
[Quidway] 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
Do you want to save the server's public key?(Y/N):y
The server's public key will be saved with the name: 10.164.39.222. 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.
<Quidway>
```

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 ...
```


版权所有 © 华为技术有限公司

```
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。

```
[Quidway-aaa] display radius-server configuration
-------------------------------------------------------------------
  Server-template-name             :  ssh
  Protocol-version                 :  standard
  Traffic-unit                     :  B
  Shared-secret-key                :  huawei
  Timeout-interval(in second)      :  5
  Primary-authentication-server    :  10.164.6.49:1812:LoopBack-1
  Primary-accounting-server        :  0.0.0.0:0:LoopBack0
  Secondary-authentication-server  :  0.0.0.0:0:LoopBack0
  Secondary-accounting-server      :  0.0.0.0:0:LoopBack0
  Retransmission                   :  3
  Domain-included                  :  YES
  -------------------------------------------------------------------
```

查看 SSH 服务器的连接信息。

```
[Quidway] display ssh server session
Session 1:
       Conn                 : VTY 0
       Version              : 2.0
       State                : started
       Username             : ssh1@ssh.com
       Retry                : 1
       CTOS Cipher          : aes128-cbc
       STOC Cipher          : aes128-cbc
       CTOS Hmac            : hmac-sha1-96
       STOC Hmac            : hmac-sha1-96
       Kex                  : diffie-hellman-group1-sha1
       Service Type         : stelnet
       Authentication Type  : password
  Session 2:
       Conn                 : VTY 1
       Version              : 2.0
       State                : started
       Username             : ssh2@ssh.com
       Retry                : 1
       CTOS Cipher          : aes128-cbc
       STOC Cipher          : aes128-cbc
       CTOS Hmac            : hmac-sha1-96
       STOC Hmac            : hmac-sha1-96
       Kex                  : diffie-hellman-group1-sha1
       Service Type         : sftp
       Authentication Type  : password
```

----结束

配置文件

SSH 服务器的配置文件

```
#
 sysname Quidway
#
radius-server template ssh
 radius-server authentication 10.164.6.49 1812
#
```


版权所有 © 华为技术有限公司

```
 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
 #
 domain ssh.com
  authentication-scheme newscheme
  radius-server ssh
 #
#
sftp server enable
stelnet server enable
ssh user ssh1@ssh.com
 ssh user ssh2@ssh.com
ssh user ssh1@ssh.com authentication-type password
 ssh user ssh2@ssh.com authentication-type password
ssh user ssh2@ssh.com assign rsa-key RsaKey001
ssh user ssh1@ssh.com service-type stelnet
 ssh user ssh2@ssh.com service-type sftp
#
user-interface vty 0 4
 authentication-mode aaa
 protocol inbound ssh
#
return
```


版权所有 © 华为技术有限公司

10 Web 网管配置

关于本章

通过网管配置 S5700 前，需要配置 S5700 作为 Web 网管服务器。

10.1 Web 网管概述
用户通过 Web 网管，可以在图形界面下非常直观地管理和维护 S5700 系列以太网交换机。

10.2 启用 Web 网管
介绍如何加载 Web 网页文件，创建 Web 网管帐号。

版权所有 © 华为技术有限公司

10.1 Web 网管概述

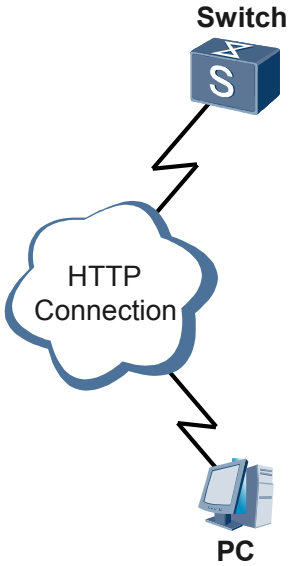
用户通过 Web 网管，可以在图形界面下非常直观地管理和维护 S5700 系列以太网交换机。

为了方便用户对 S5700 系列以太网交换机的维护和使用，华为公司特推出该系列以太网交换机 Web 网管功能。

S5700 内置一个 Web 服务器，与 S5700 相连的终端（以下均以 PC 为例）可以通过 Web 浏览器访问 S5700。

Web 网管的运行环境如**图 10-1** 所示。

图 10-1 Web 网管运行环境



10.2 启用 Web 网管

介绍如何加载 Web 网页文件，创建 Web 网管帐号。

10.2.1 通过 Console 口登录 S5700

10.2.2 设置 S5700 的管理 IP 地址
介绍如何配置 S5700 的管理 IP 地址。

10.2.3 上传 Web 网页文件
介绍 Web 网页文件的获取路径及如何以 FTP 方式上传 Web 网页文件至 S5700 设备。

10.2.4 加载 Web 网页文件
介绍如何加载 Web 网页文件。

10.2.5 创建 Web 网管帐号
在客户端通过 Web 方式登录 S5700 设备前，需要先在 S5700 设备上创建 Web 网管帐号。

版权所有 © 华为技术有限公司

10.2.6 登录 Web 网管
介绍如何通过 Web 方式登录 S5700 设备。

10.2.1 通过 Console 口登录 S5700

背景信息

在通过 Console 口搭建本地配置环境时，用户可以在 PC 上通过 Windows 系统中的“超级终端”与 S5700 建立连接。

操作步骤

步骤 1 请在 PC 上启动超级终端

选择“开始 > 程序 > 附件 > 通讯 > 超级终端”菜单项，Windows 系统启动超级终端。

步骤 2 新建连接

如图 10-2 所示。在“名称”文本框中输入新建连接的名称；选择图标。然后单击“确定”按钮。

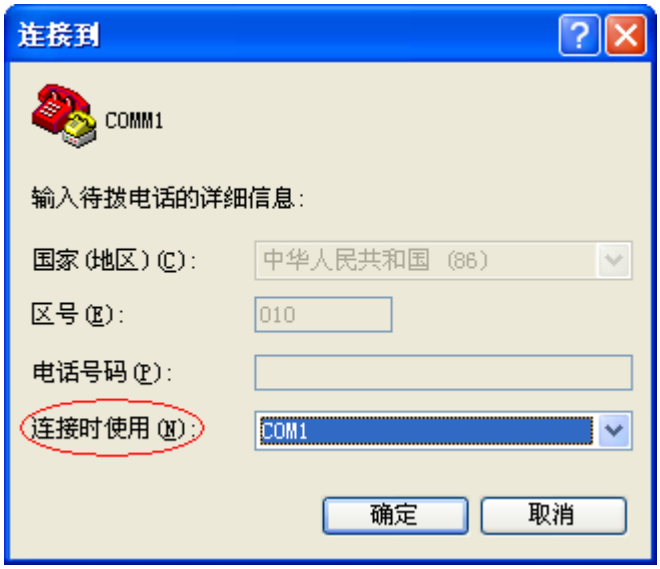
图 10-2 新建连接

步骤 3 设置连接端口

进入如图 10-3 所示的 [连接到] 窗口后，请根据 PC（或配置终端）实际使用的端口在“连接时使用”下拉列表框中进行选择。然后单击“确定”按钮。

华为专有和保密信息
版权所有 © 华为技术有限公司

图 10-3 连接端口设置



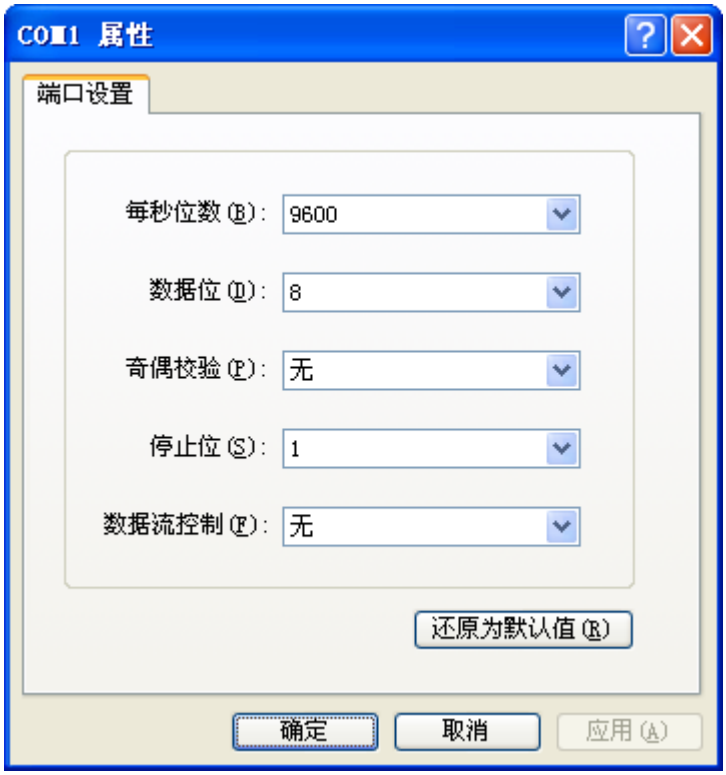
步骤 4 设置通信参数

进入如图 10-4 所示的 [端口属性] 窗口后，请按表 10-1 中的描述进行通信参数的设置。

说明

在其它的 Windows 操作系统中，“每秒位数”可能被描述为“波特率”；“数据流控制”可能被描述为“流量控制”。

图 10-4 端口通信参数设置



华为专有和保密信息
版权所有 © 华为技术有限公司

表 10-1 通信参数

参数	取值
每秒位数（波特率）	9600
数据位	8
奇偶校验	无
停止位	1
数据流控制（流量控制）	无

步骤 5 启动超级终端后，选择“文件 > 属性”菜单项，进入如图 10-5 所示的 [连接属性] 窗口。选择“设置”页签，在“终端仿真”下拉列表框中选择“自动检测”或“VT100”。单击“确定”按钮结束设置。

图 10-5 终端类型选择

按照以上 5 个步骤结束设置后，按下“Enter”键，屏幕出现<Quidway>提示符，表示登录到 S5700。此时就可输入命令，配置或管理 S5700。

----结束

版权所有 © 华为技术有限公司

10.2.2 设置 S5700 的管理 IP 地址

介绍如何配置 S5700 的管理 IP 地址。

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 meth 0/0/1**，进入管理网口视图。

步骤 3 执行命令 **ip address** *ip-address* { *mask* | *mask-length* } [**sub**]，配置接口的 IP 地址。

----结束

10.2.3 上传 Web 网页文件

介绍 Web 网页文件的获取路径及如何以 FTP 方式上传 Web 网页文件至 S5700 设备。

前提条件

Web 网页文件获取路径：请先登录华为公司技术支持网站（http://support.huawei.com），登录后，在“软件中心 > 版本软件 > 数通 > 以太网交换机 > S27&37&57 系列”路径下，根据版本名称，下载对应的版本软件。版本软件中包含 Web 网页文件，名称为“产品+软件版本号.web.zip”。

在上传 Web 网页文件前，请将文件拷贝到登录设备的客户端上。

背景信息

这里介绍如何以 FTP 方式上传 Web 网页文件。

说明

Web 网页文件也可以通过 TFTP 方式获取，此时，S5700 作为 TFTP 客户端，将存放 Web 网页文件的终端作为 TFTP 服务器。具体步骤请参考 **8.5.2 使用 TFTP 下载文件**。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ftp server enable**，使能 FTP 服务。

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** { **simple** | **cipher** } *password*，配置 FTP 用户名和密码。

步骤 5 执行命令 **local-user** *user-name* **ftp-directory** *directory*，配置 FTP 用户的访问路径。

步骤 6 执行命令 **local-user** *user-name* **service-type ftp**，配置 FTP 登录用户的服务类型。

步骤 7 在 PC 的 cmd 视图下执行命令 **ftp** *ip-address*，输入用户名和密码，登录 S5700。

```
C:\>ftp 10.1.1.132
 Connected to 10.1.1.132.
220 FTP service ready.
User (10.1.1.132:(none)): client
331 Password required for client.
Password:
```


版权所有 © 华为技术有限公司

```
230 User logged in.
ftp>
```

步骤 8 在 FTP 视图下执行 **put** *local-filename* 命令，将 PC 上的 Web 网页文件（例如：web.zip）上传至 S5700。

```
ftp> put web.zip
200 Port command okay.
150 Opening ASCII mode data connection for web.zip.
226 Transfer complete.
ftp: 发送 251047 字节，用时 3.36Seconds 74.74Kbytes/sec.
ftp>
```

----结束

10.2.4 加载 Web 网页文件

介绍如何加载 Web 网页文件。

背景信息

加载 Web 网页文件前，文件必须已经上传至 S5700。

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 **http server load** *file-name*，加载 Web 网页文件。

----结束

10.2.5 创建 Web 网管帐号

在客户端通过 Web 方式登录 S5700 设备前，需要先在 S5700 设备上创建 Web 网管帐号。

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 **http server enable**，使能 HTTP 服务。

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** { **simple** | **cipher** } *password*，配置 HTTP 用户名和密码。

说明

在实际配置时最好使用 cipher 形式的密码，用户名和密码不要设置的过于简单，以保证安全性。

步骤 5 执行命令 **local-user** *user-name* **service-type http**，配置用户 admin 的访问类型为 HTTP。

步骤 6 执行命令 **quit**，返回系统视图。

步骤 7 （可选）执行命令 **http timeout** *timeout*，配置 HTTP 会话的超时时间，缺省情况下，会话超时时间为 30 分钟。

----结束

版权所有 © 华为技术有限公司

10.2.6 登录 Web 网管

介绍如何通过 Web 方式登录 S5700 设备。

操作步骤

步骤 1 在 PC 上打开 Web 浏览器，在地址栏中输入 S5700 的管理 IP 地址（PC 和 S5700 之间要有可达的路由），按回车键后将显示登录对话框。如图 10-6 所示，输入之前设置的 Web 网管帐号和密码，输入验证码，并选择 Web 网管系统的语言。

图 10-6 登录界面

说明

在单击“登录”之前，可以勾选“记住我的密码”，这样用户在下次登录系统时，输入用户名后密码会自动和用户名相匹配。

步骤 2 单击“登录”或直接按回车键即可进入 Web 网管系统主页面。

登录到 Web 网管后，可以对交换机进行配置。具体操作请参见《*Quidway S5700 系列以太网交换机 Web 网管客户端操作指南*》。

----结束

版权所有 © 华为技术有限公司