服务热线：400-615-1233
配套精品教学资料包
www.huatengedu.com.cn

WANGLUO GUZHANG CHULI YU YOUHUA

网络故障处理与优化

策划编辑：高　锐
责任编辑：许　青
封面设计：刘文东

ISBN 978-7-5635-6641-9

定价：53.00元

高等职业教育计算机系列创新教材

网络故障处理与优化

主编 吴超 王丹 于婷

北京邮电大学出版社

高等职业教育计算机系列创新教材

网络故障处理与优化

主编　吴　超　王　丹　于　婷

校企双元合作开发，以**26**个典型工作任务为载体，融入**网络关键技术**。坚持正确的**政治方向**和**价值导向**，将**职业标准**、**生产过程**和**思政元素**融入课程体系。推动教材配套**资源建设**，提供**教学课件**、**微课**、**动画**等数字化学习资源。

北京邮电大学出版社
www. buptpress. com

高等职业教育计算机系列创新教材

网络故障处理与优化

主　编　吴　超　王　丹　于　婷
副主编　黄军霞　郑红霞　王　平
王玉江

北京邮电大学出版社
www. buptpress. com

内 容 简 介

本书共9个项目，内容包括远程登录故障处理与优化、VLAN故障处理与优化、交换机其他故障处理与优化、STP及MSTP故障处理与优化、静态路由及RIP故障处理与优化、OSPF故障处理与优化、VRRP故障处理与优化、ACL及NAT故障处理与优化、DHCP故障处理与优化。

本书可作为高等职业院校计算机网络技术及相关专业的教材，也可供相关技术人员参考。

图书在版编目(CIP)数据

网络故障处理与优化 / 吴超，王丹，于婷主编. -- 北京：北京邮电大学出版社，2022.5
ISBN 978-7-5635-6641-9

Ⅰ.①网… Ⅱ.①吴… ②王… ③于… Ⅲ.①计算机网络—故障修复—高等职业教育—教材 Ⅳ.①TP393.07

中国版本图书馆CIP数据核字(2022)第073460号

策划编辑：高 锐 **责任编辑**：许 青 **封面设计**：刘文东

出版发行：北京邮电大学出版社
社　　址：北京市海淀区西土城路10号
邮政编码：100876
发 行 部：电话：010-62282185 传真：010-62283578
E-mail：publish@bupt.edu.cn
经　　销：各地新华书店
印　　刷：三河市金元印装有限公司
开　　本：787 mm×1 092 mm 1/16
印　　张：17.5插页1
字　　数：362千字
版　　次：2022年5月第1版
印　　次：2022年5月第1次印刷

ISBN 978-7-5635-6641-9 定 价：53.00元

·如有印装质量问题，请与北京邮电大学出版社发行部联系·

服务电话：400-615-1233

PREFACE 前言

随着信息时代网络技术的飞速发展，各行各业对复合型技术人才提出了更高的要求。要求他们不但要具有扎实的理论基础，还要有较强的实际动手能力；不但要有单一的应用技能，还要具有综合知识技能，以适应新时代网络技术的发展。

本书具有显著的职教特色，校企双元开发，采用企业真实工作案例，以任务驱动为引领，无缝对接企业实际岗位，同时将职业标准和生产过程的具体要求融入课程体系，兼顾职业能力培养的递进衔接，通过项目化案例构建知识体系。本书按照网络工程项目实施及运行的真实过程分解，重构知识点和技能点，让学生能以工程思维、系统思维了解企业项目运行实施的步骤、规范和方法，并在真实网络故障典型案例的学习中提升解决工程问题的综合能力。

本书具有以下特点。

1. 面向实战，理实一体

本书大量采用企业实际项目案例，以项目＋任务的方式体现，学生通过教师的引导，能够以系统化的方式在项目中发现故障、测试故障、收集故障现象、理解故障现象的关联关系，从而更好地以整体、连贯、系统化的视角去实践项目，从而培养自身的职业综合素养。

2. 紧随形势，覆盖全面

本书内容覆盖面广，书中 9 个项目 26 个子任务囊括了“网络故障处理与优化”课程的主要内容，包括交换协议、路由协议、安全、设备管理等，按照技术技能型人才培养规律，将网络关键技术融入各个典型案例中，以应用案例引领关键技术，便于学生对抽象技术进行理解，从而提高解决故障的能力。

3. 课程思政，春风化雨

本书基于行业产业调研结果，对华为网络设备的关键技术、应用领域等知识进行分析，将正确解决问题的思维方法及不畏困难、严谨细致、精益求精的职业品质融入教学过程，让学生正确规划学习目标和职业生涯，做社会主义核心价值观的践行者。

4. 资源丰富,形式多样

为更好地碎片化组织教学内容,本书提供了丰富的数字化学习资源,包括 PPT 教学课件、微课、动画、教学大纲、课程标准、学习指南、作业题或讨论题等。除了扫描书中二维码观看视频,学生还可以访问智慧职教 MOOC 学院观看视频或下载资源,更好地掌握学习内容,检验学习成果。

本书由吴超、王丹、于婷担任主编,黄军霞、郑红霞、王平、王玉江担任副主编。具体编写分工如下:吴超负责统稿及项目 1、项目 5 的编写,王平负责项目 2 的编写,郑红霞负责项目 3 的编写,于婷负责校稿及项目 4、项目 8 的编写,黄军霞负责项目 6 的编写,王丹负责校稿及项目 7、项目 9 的编写,王玉江作为企业专家负责对企业真实案例进行梳理与审核。

由于编者水平有限,书中不足之处在所难免,恳请广大读者批评指正。在使用本书的过程中,如果发现错误或不妥之处,抑或有更好的建议,欢迎发送邮件至 k12dian@126.com,以便我们更好地完善书中内容。

编　者

视频:课程简介

CONTENTS 目录

项目 1

远程登录故障处理与优化

远程登录可以允许授权用户进入网络中的其他远端设备，如同本地用户一样对远端设备进行文件读取、编辑、删除等操作。远程登录逐渐被人们认识和广泛地应用于学习、工作和生活中，更多、更方便的远程登录方式也在慢慢丰富市场，满足各种阶层和目的的用户需求。本项目通过对 Telnet(teletype network)和 SSH(secure shell)远程登录协议的典型故障进行分析与排除，使学生掌握相关故障处理的方法。

Telnet 协议是 Internet 远程登录服务的标准协议和主要方式，操作简单方便，但由于其是基于明文传输的协议，包括用户名和登录密码都采用明文的方式在网络上传播，具有一定的安全隐患。

SSH 协议是专为远程登录会话和其他网络服务提供安全性的协议，可以有效防止远程管理过程中的信息泄露问题。

学习目标

- 熟悉远程登录的应用场景。
- 理解 Telnet、SSH 的原理。
- 能进行远程登录相关配置。
- 会分析、处理远程登录常见故障。

思政园地

不同的应用场景对安全要求有所不同，需要选择合适的远程登录方式。如果配置错误，会造成安全隐患，给用户带来时间和金钱上的损失。同时，远程登录需要开启用户的虚拟端口，如果忘记就无法实现，只能赶到设备所在地进行配置。所以严谨细致的工作态度对网络工程师来说十分重要，要贯穿工作始终。

任务 1-1　Telnet 故障处理与优化

视频

学习任务单

任务名称	任务 1-1　Telnet 故障处理与优化				
考核点	Telnet 远程登录	组内人数	3	任务单分值	10
任务描述	如图 1-1-1 所示，某公司为网络管理员分配权限，在路由器 R2、R3 上远程访问 Telnet 服务器 R1。网络设备使用 10.1.1.0 网段，子网掩码为 24 位；Telnet 服务器配置网络管理员权限用户级别为 3；认证模式为 AAA，用户名为 admin，密码为 admin@123。 但在工作过程中发现 R2 的认证模式为 password，用户级别为默认的 0 级，而 R3 远程登录失败				
任务分析	从 Telnet 协议的实现及技术原理分析，需要从认证模式配置、密码设置、Telnet 服务器中允许同时登录的最大用户数等方面进行故障排查				
成果展示与评价	各组成员合作排除 Telnet 远程登录故障，使设备按要求正常运行，小组互评后由教师综合评定成绩				

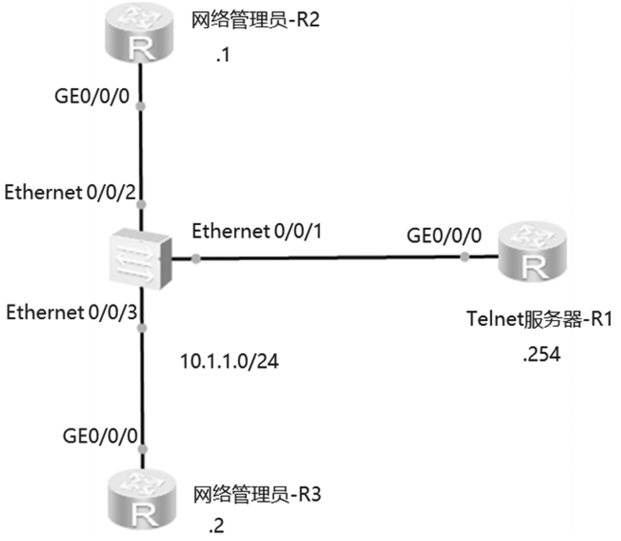

图 1-1-1　Telnet 远程登录拓扑图

故障分析

1. 查询 Telnet 当前配置状态

1)在 R2 上查询当前 Telnet 配置状态

在 R2 上执行“telnet 10.1.1.254”命令，查询当前 Telnet 配置状态。结果显示 R2 通过 password 认证模式成功远程登录 Telnet 服务器 R1，但执行“System-view”命令后，无法进

入系统视图，即用户级别为默认的 0 级。

```
<R2> telnet 10.1.1.254
  Press CTRL_] to quit telnet mode
  Trying 10.1.1.254 ...
  Connected to 10.1.1.254 ...
Login authentication
Password: * * * *
<R1> System-view
Error: Unrecognized command found at '^' position.
```

2)在 R3 上查询当前 Telnet 配置状态

在 R3 上执行“telnet 10.1.1.254”命令，查询当前 Telnet 配置状态。结果显示 R3 远程登录失败，与要求不相符。

```
<R3>telnet 10.1.1.254
  Press CTRL_] to quit telnet mode
  Trying 10.1.1.254 ...
  Error: Can't connect to the remote host
```

2. 故障汇总

将测试结果汇总成表 1-1-1，共有 2 项测试失败：R2 虽然可以远程登录 R1，但认证模式为 password，用户级别为默认的 0 级，而 R3 远程登录 R1 失败。

表 1-1-1　Telnet 测试结果汇总

序号	路由器 1	路由器 2	测试方法	预期测试结果	实际测试结果	是否发生故障
1	R2	R1	telnet 命令	远程登录成功，用户级别为 3，认证模式为 AAA，用户名为 admin，密码为 admin@123	远程登录成功，认证模式为 password，用户级别为默认的 0 级	是
2	R3	R1	telnet 命令	远程登录成功，用户级别为 3，认证模式为 AAA，用户名为 admin，密码为 admin@123	远程登录失败	是

3. 故障原因分析

本任务主要是用模拟环境来实现，因此物理问题及设备问题可以忽略。从 Telnet 协议的实现及技术原理分析，可能存在以下故障点。

(1)IP 地址配置错误。

(2)密码设置错误。

(3)认证模式配置错误。

(4)Telnet 服务器中配置的可同时使用用户数小于实际用户数。

知识链接

1. Telnet 应用场景

如果企业网络中有一台或多台网络设备需要进行远程配置和管理，管理员可以使用 Telnet 远程连接到每一台设备上，对这些设备进行集中管理和维护。Telnet 提供了一个交互式操作界面，允许终端远程登录到任何可以充当 Telnet 服务器的设备上。Telnet 用户可以像通过 Console 端口进行本地登录一样对设备进行操作。远端 Telnet 服务器和终端之间无须直连，只需保证两者之间可以互相通信即可。通过使用 Telnet，用户可以方便地实现对设备进行远程管理和维护，如图 1-1-2 所示。

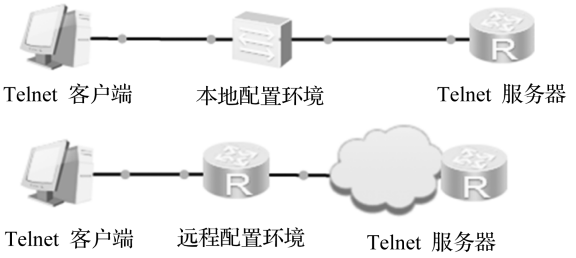

图 1-1-2　终端通过 Telnet 对本地和远程网络设备进行管理

2. Telnet 认证模式

在配置 Telnet 登录用户界面时，必须配置认证方式，否则用户无法成功登录设备。Telnet 认证模式有 AAA 和 password(密码)两种。如表 1-1-2 所示，当配置用户界面的认证模式为 AAA 时，用户登录设备时需要先输入登录用户名和密码才能登录；当配置用户界面的认证模式为 password 时，用户登录设备时需要先输入登录密码才能登录。

表 1-1-2　Telnet 认证模式

认证模式	描　　述
AAA	登录时通过用户名和密码实现认证
password	登录时只通过密码实现认证

3. Telnet 配置

1)Telnet 服务器配置

在 Telnet 服务器上进行配置，通常使用密码认证机制来认证连接到 VTY(virtual type terminal)接口的用户。VTY 是网络设备用来管理和监控通过 Telnet 方式登录的用户的界面。网络设备为每个 Telnet 用户分配一个 VTY 界面。下面代码中“vty 0 4”的含义是指 VTY0、VTY1、VTY2、VTY3、VTY4，共 5 个用户。如果需要增加 Telnet 用户的登录数量，可以使用“user-interface maximum-vty”命令来调整 VTY 界面的数量。执行“authentication-mode password”命令，可以配置 VTY 通过密码对用户进行认证。

```
[Huawei] interface Ethernet 1/0/0
[Huawei-Ethernet1/0/0] ip address 192.168.1.1 24
[Huawei] user-interface vty 0 4
[Huawei-ui-vty0-4] authentication-mode password
[Huawei-ui-vty0-4] set authentication password cipher huawei
```

2)客户端访问 Telnet 服务器

远端设备配置为 Telnet 服务器之后，可以在客户端上执行“telnet”命令来与服务器建立 Telnet 连接，如图 1-1-3 所示。客户端会收到需要认证相关的提示信息，用户输入的认证密码需要匹配 Telnet 服务器上保存的密码。认证通过之后，用户就可以通过 Telnet 远程连接到 Telnet 服务器上，在本地对远端设备进行配置和管理。

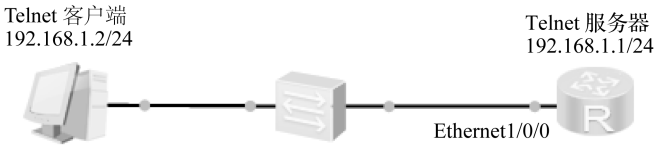

图 1-1-3　Telnet 服务器配置及客户端访问

```
<Guest>telnet 192.168.1.1
Trying 192.168.1.1 ...
Press CTRL+K to abort
Connected to 192.168.1.1 ...
Login authentication
Password: * * * * * *
Info: The max number of VTY users is 10, and the number
      of current VTY users on line is 1.
      The current login time is 2020-04-11 16:32:00.
<Huawei>
```

故障排除与实施

在故障分析环节，通过测试发现两项故障：R2 的 Telnet 认证模式为 password，用户级别为默认的 0 级；R3 不能正常访问 Telnet 服务器。结合 Telnet 的技术原理，依次进行相关故障排除与问题处理。

1. 核查各网络设备的 IP 地址

根据任务规划，列出路由器 R1、R2、R3 接口的 IP 地址，如表 1-1-3 所示。

表 1-1-3　各路由器 IP 地址对应表

路 由 器	接　　口	IP 地址
R1	GE0/0/0	10.1.1.254/24
R2	GE0/0/0	10.1.1.1/24
R3	GE0/0/0	10.1.1.2/24

1)查看各路由器接口 IP 地址

使用“display ip interface brief”命令查看各路由器接口配置的 IP 地址，与表 1-1-3 中规划 IP 地址对比后，发现 R1 和 R2 配置正确，R3 的 GE0/0/0 接口 IP 地址应配置为 10.1.1.2/24，但错误配置成了 10.1.2.1/24。

```
<R1>display ip interface brief
 * down: administratively down
^down: standby
(l): loopback
(s): spoofing
The number of interface that is UP in Physical is 2
The number of interface that is DOWN in Physical is 2
The number of interface that is UP in Protocol is 2
The number of interface that is DOWN in Protocol is 2
Interface                         IP Address/Mask      Physical   Protocol
GigabitEthernet0/0/0              10.1.1.254/24        up         up
```

```
<R2>display ip interface brief
 * down: administratively down
^down: standby
(l): loopback
(s): spoofing
The number of interface that is UP in Physical is 2
The number of interface that is DOWN in Physical is 2
The number of interface that is UP in Protocol is 2
The number of interface that is DOWN in Protocol is 2
Interface                         IP Address/Mask      Physical   Protocol
GigabitEthernet0/0/0               10.1.1.1/24            up         up
```

```
<R3>display ip interface brief
 * down: administratively down
^down: standby
(l): loopback
(s): spoofing
The number of interface that is UP in Physical is 2
The number of interface that is DOWN in Physical is 2
The number of interface that is UP in Protocol is 2
The number of interface that is DOWN in Protocol is 2
Interface                         IP Address/Mask      Physical   Protocol
GigabitEthernet0/0/0               10.1.2.1/24            up         up
```

2)修正错误 IP 地址

在路由器 R3 上使用“ip address”命令将 GE0/0/0 接口 IP 地址由 10.1.2.1/24 修改为

10.1.1.2/24。

```
[R3] interface GigabitEthernet0/0/0
[R3-GigabitEthernet0/0/0] ip address 10.1.1.2 24
```

2. 查询 Telnet 服务器 R1 的当前参数配置

1)查询 R1 允许同时远程登录的最大用户数

在 R1 上使用“display user-interface maximum-vty”命令查询到允许同时远程登录最大用户数为 5(大于 2),符合要求。

```
<R1>display user-interface maximum-vty
Maximum of VTY user:5
```

2)查询 R1 远程登录配置参数

使用“display current-configuration”命令查询 R1 远程登录配置参数。可以看到 AAA 认证模式下“local-user admin service-type”错误配置为 http,应改为 telnet;同时“user-interface vty 0 4”下“authentication-mode”错误配置为 password 认证,应改为 AAA 认证。

```
<R1> display current-configuration
#
aaa
authentication-scheme default
authorization-scheme default
accounting-scheme default
domain default
domain default_admin
local-user admin password cipher %$%$K8m.Nt84DZ}e#<0'8bmE3Uw}%$%$
local-user admin service-type http
#
user-interface vty 0 4
authentication-mode password
set authentication password cipher %$%$D--j+}WqKA"E>,BNq3HK,*gu)zST$nqTn/! $w/>=Y32)
*gx,%$%$
```

使用“user privilege level”命令将 R1 远程登录用户级别设置为 3 级,并使用“authentication-mode”命令将 R1 远程登录用户认证模式设置为 AAA。

```
[R1] user-interface vty 0 4
[R1-ui-vty0-4] user privilege level 3
[R1-ui-vty0-4] authentication-mode aaa
```

使用“service-type”命令配置用户接入类型为 telnet,配置用户名为 admin,密码为 admin@123。

```
[R1] aaa
[R1-aaa] local-user admin service-type telnet
[R1-aaa] local-user admin password cipher admin@123
```

3. 在新配置环境下进行测试

1)使用 telnet 命令测试远程登录

在 R2 和 R3 上分别使用“telnet 10.1.1.254”命令测试,结果显示 R2 和 R3 正常远程登录 R1,认证模式为 AAA,用户名为 admin,密码为 admin@123。

```
<R2>telnet 10.1.1.254
  Press CTRL_] to quit telnet mode
  Trying 10.1.1.254 ...
  Connected to 10.1.1.254 ...
Login authentication
Username: admin
Password: * * * * * * * * *
<R1>
Enter system view, return user view with Ctrl+Z.
[R1]
```

```
<R3>telnet 10.1.1.254
  Press CTRL_] to quit telnet mode
  Trying 10.1.1.254 ...
  Connected to 10.1.1.254 ...
Login authentication
Username: admin
Password: * * * * * * * * *
<R1>
Enter system view, return user view with Ctrl+Z.
[R1]
```

2)测试结果汇总

在 R2 和 R3 上使用“telnet”命令测试远程登录后,将测试结果进行记录,如表 1-1-4 所示。实际测试结果与预期效果一致,完成故障处理与优化。

表 1-1-4　修改后 Telnet 测试结果汇总

序号	路由器 1	路由器 2	测试方法	预期测试结果	实际测试结果	是否发生故障
1	R2	R1	telnet 命令	远程登录成功,用户级别为 3,认证模式为 AAA,用户名为 admin,密码为 admin@123	与预期效果一致	否
2	R3	R1	telnet 命令	远程登录成功,用户级别为 3,认证模式为 AAA,用户名为 admin,密码为 admin@123	与预期效果一致	否

4. 任务总结

本任务主要针对 Telnet 协议配置的故障排除，以理论化故障排除思路为指导，以任务式驱动为方法，形象再现了 Telnet 协议的原理学习和操作实现过程，为实际环境中的 Telnet 协议故障排除提供了良好的方法和操作步骤。在实际应用环境中应按照以下故障排除规范来一一检查：首先检查 IP 地址配置是否错误；其次检查 Telnet 服务器参数配置是否错误，包括允许同时远程登录的最大用户数、远程登录用户级别、远程登录用户认证模式等，直到查出所有故障为止。

任务实施单

任务名称		任务 1-1　Telnet 故障处理与优化			
班级		完成人		日期	
实施步骤		命令行		设备状态	
故障分析	分别在 R2 和 R3 上查询当前 Telnet 配置状态	R2： R3：		R2 故障现象： R3 故障现象：	
故障处理	1. 核查各网络设备的 IP 地址	R1： R2： R3：		R1 是否存在故障： R1 故障原因及处理方法： R2 是否存在故障： R2 故障原因及处理方法： R3 是否存在故障： R3 故障原因及处理方法：	
	2. 核查 R1 的当前参数配置	R1：		R1 是否存在故障： R1 故障原因及处理方法：	
新配置环境下进行测试	分别在 R2 和 R3 上使用“telnet”命令测试远程登录	R2： R3：		实测结果与预期效果是否一致：	
任务总结					

任务 1-2　SSH 故障处理与优化

视频

学习任务单

任务名称	任务 1-2　SSH 故障处理与优化				
考核点	SSH 远程登录	组内人数	3	任务单分值	10
任务描述	如图 1-2-1 所示，某公司要为网络管理员分配权限，为了保证网络安全，在服务器 R2 上配置 SSH 协议，客户端 R1、R3 采用 SSH 协议登录 R2，不允许使用 Telnet 登录。SSH 远程访问的用户名为 user-ssh，密码为 huawei123。同时 Client1 和 R2 能够登录公司的 FTP 服务器，登录用户名为 huawei，密码为 huawei@123。 但在实际工作中发现，Client1 无法登录 FTP 服务器，R1、R3 登录 R2 的方式是 Telnet 而不是更安全的 SSH				
任务分析	从 SSH 协议的实现及技术原理分析，需要从认证模式配置、SSH 协议中的用户名和密码设置、VTY 认证配置等方面进行故障排查				
成果展示与评价	各组成员合作排除 SSH 远程登录故障，使设备按要求正常运行，小组互评后由教师综合评定成绩				

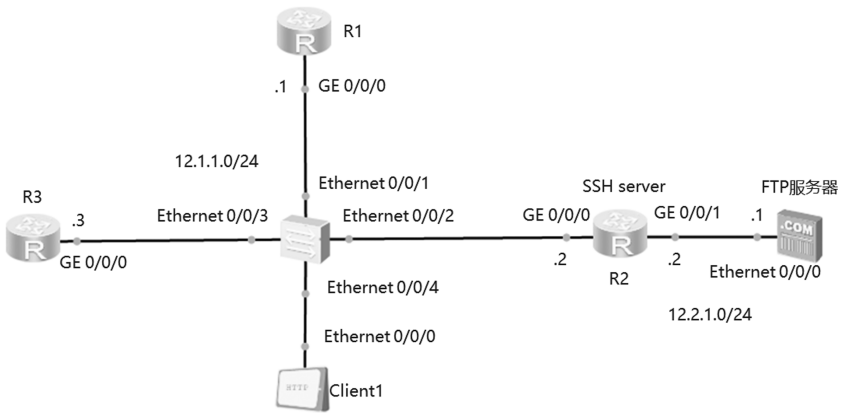

图 1-2-1　SSH 远程登录拓扑图

故障分析

1. 测试远程访问 FTP 服务器状态

1）测试 Client1 远程访问 FTP 服务器状态

按照网络规划，在 Client1 中配置服务器地址为 12. 2. 1. 1，端口号为 21，用户名为 huawei，密码为 huawei@123。测试其与 FTP 服务器的连通性，结果显示连接服务器失败，如图 1-2-2 所示。

图 1-2-2　Client1 登录 FTP 服务器失败

2)测试 R2 远程访问 FTP 服务器状态

在 R2 上执行“ftp 12.2.1.1”命令,测试是否可以远程访问 FTP 服务器,结果显示当输入正确的用户名和密码后,R2 可以正常远程登录。

```
<R2>ftp 12.2.1.1
Trying 12.2.1.1 ...
Press CTRL+K to abort
Connected to 12.2.1.1.
220 FtpServerTry FtpD for free
User(12.2.1.1:(none)): huawei
331 Password required for huawei .
Enter password: * * * * * * * *
230 User huawei logged in , proceed
[R2-ftp]
```

2. 测试远程访问服务器 R2 状态

1)测试 R1 远程访问服务器 R2 状态

在 R1 上执行“stelnet”命令远程登录 R2,结果显示登录失败;但使用“telnet”命令时,输入用户名和密码后成功远程访问 R2。

```
[R1] stelnet 12.1.1.2
Please input the username:
Trying 12.1.1.2 ...
Press CTRL+K to abort
Error: Failed to connect to the remote host.
```

```
<R1>telnet 12.1.1.2
  Press CTRL_] to quit telnet mode
  Trying 12.1.1.2 ...
  Connected to 12.1.1.2 ...
Login authentication
Username: user-ssh
Password: * * * * * * * * *
<R2>
```

2)测试 R3 远程访问服务器 R2 状态

同理,在 R3 上执行“stelnet”命令远程登录 R2,结果显示登录失败;但使用“telnet”命令时,输入用户名和密码后成功远程访问 R2。

```
[R3] stelnet 12.1.1.2
Please input the username:
Trying 12.1.1.2 ...
Press CTRL+K to abort
Error: Failed to connect to the remote host.
```

```
<R3>telnet 12.1.1.2
  Press CTRL_] to quit telnet mode
  Trying 12.1.1.2 ...
  Connected to 12.1.1.2 ...
Login authentication
Username: user-ssh
Password: * * * * * * * * *
<R2>
```

3. 故障汇总

将测试结果汇总成表 1-2-1,共有 3 项测试失败:Client1 无法访问 FTP 服务器,R1、R3 登录 R2 的方式是 Telnet 而不是更安全的 SSH。

表 1-2-1　SSH 测试结果汇总

序号	设备 1	设备 2	测试方法	预期测试结果	实际测试结果	是否发生故障
1	Client1	FTP 服务器	FTP	成功	失败	是
2	R2	FTP 服务器	FTP	成功	成功	否
3	R1	R2	SSH	成功	Telnet 成功,SSH 失败	是
4	R3	R2	SSH	成功	Telnet 成功,SSH 失败	是

4. 故障原因分析

本任务主要是用模拟环境来实现,因此物理问题及设备问题可以忽略,主要从 SSH 协议的相关概念及 SSH 协议的配置和操作方面进行故障排查。从 SSH 协议的实现及技术原

理分析，可能存在以下故障点。

(1)IP 地址配置错误。

(2)用户名和密码设置错误。

(3)SSH 协议配置错误。

(4)VTY 认证配置错误。

知识链接

1. 安全外壳简述

由于 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，单纯地提供 Telnet 服务容易招致主机 IP 地址欺骗、路由欺骗等。

安全外壳(secure shell，SSH)协议是在传统的 Telnet 协议基础上发展起来的一种安全的远程登录协议。相比于 Telnet，SSH 无论是在认证方式还是在数据传输的安全性上，都有很大的提高。

SSH 在华为网络设备上被称为 SSH Telnet(简称 Stelnet)，为网络终端访问提供安全的 Telnet 服务。

2. SSH 配置

1)SSH 服务器配置

图 1-2-3 所示为在 SSH 服务器上进行配置。

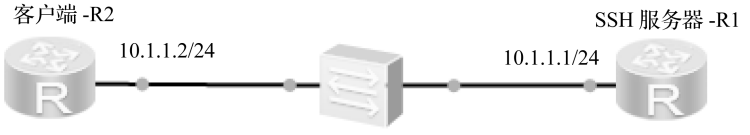

图 1-2-3　SSH 服务器配置及客户端访问

(1)创建本地用户 user-ssh，将其对应密码设置为 huawei@123，设置用户级别为最高级 15 级，并设置该用户服务于 SSH 应用。

```
[R1] aaa
[R1-aaa] local-user user-ssh password cipher huawei@123
Info: Add a new user.
[R1-aaa] local-user user-ssh privilege level 15
[R1-aaa] local-user user-ssh service-type ssh
[R1-aaa] quit
```

(2)开启 SSH 服务，设置 SSH 用户的认证方式为默认的密码认证，并创建本地密钥。

```
[R1] ssh user user-ssh authentication-type password
Authentication type setted, and will be in effect next time
[R1] stelnet server enable
Info: Succeeded in starting the STELNET server.
[R1] rsa local-key-pair create
```

(3)设置 VTY 认证类型为 AAA 认证。

```
[R1] user-interface vty 0 4
[R1-ui-vty0-4] authentication-mode aaa
[R1-ui-vty0-4] protocol inbound ssh
```

2)客户端访问 SSH 服务器

远端设备配置为 SSH 服务器之后,可以在客户端上执行“stelnet”命令来与服务器建立 SSH 连接。客户端会收到需要认证相关的提示信息,用户输入的用户名和密码需要匹配 SSH 服务器上保存的用户名及对应密码。认证通过之后,用户就可以通过 Stelnet 远程连接到 SSH 服务器上,在本地对远端设备进行配置和管理。

```
[R2] ssh client first-time enable
[R2] stelnet 10.1.1.1
Please input the username: user-ssh
Trying 10.1.1.1 ...
Press CTRL+K to abort
Connected to 10.1.1.1 ...
Login authentication
Password: * * * * * * *
<R1>
```

故障排除与实施


视频

在故障分析环节,共有 3 项测试失败:Client1 无法访问 FTP 服务器,R1、R3 登录 R2 的方式是 Telnet,而不是更安全的 SSH。结合 SSH 的技术原理,依次进行相关故障排除与问题处理。

1. 核查各网络设备的 IP 地址

根据任务规划,列出路由器 R1、R2、R3,FTP 服务器及 Client1 接口的 IP 地址,如表 1-2-2 所示。

表 1-2-2　IP 地址规划表

网络设备	接　口	IP 地址
R1	GE0/0/0	12.1.1.1/24
R2	GE0/0/0	12.1.1.2/24
	GE0/0/1	12.2.1.2/24
R3	GE0/0/0	12.1.1.3/24
FTP 服务器	Ethernet0/0/0	12.2.1.1/24
Client1	Ethernet0/0/0	12.1.1.20/24

(1)使用“display ip interface brief”命令查看各路由器接口配置的 IP 地址,与表 1-2-2 中的规划 IP 对比后,发现 R1、R2 和 R3 配置均正确。

```
<R1>display ip interface brief
Interface                         IP Address/Mask      Physical   Protocol
GigabitEthernet0/0/0              12.1.1.1/24          up         up

<R2>display ip interface brief
Interface                         IP Address/Mask      Physical   Protocol
GigabitEthernet0/0/0              12.1.1.2/24          up         up
GigabitEthernet0/0/1              12.2.1.2/24          up         up

<R3>display ip interface brief
Interface                         IP Address/Mask      Physical   Protocol
GigabitEthernet0/0/0              12.1.1.3/24          up         up
```

(2)核查 Client1 配置,如图 1-2-4 所示,Client1 的 IPv4 和 FtpClient 参数配置正确。

图 1-2-4　Client1 的参数配置

(3)核查 FTP 服务器配置,如图 1-2-5 所示,FTP 服务器的 FtpServer 参数配置正确,但网关错误配置成了 12.2.1.254,应修改为图 1-2-6 中的网关地址“12.2.1.2”。

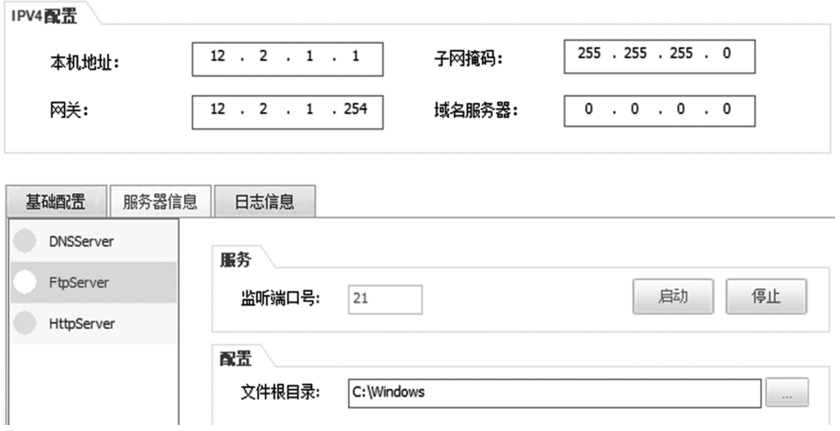

图 1-2-5　FTP 服务器的参数配置

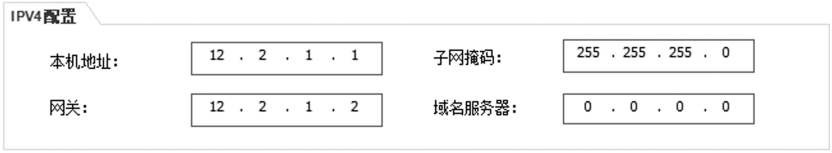

图 1-2-6　修改 FTP 服务器网关地址

2. 查询 SSH 服务器 R2 当前参数配置

使用“display current-configuration”命令查询 R2 远程登录配置参数。可以看到 R2 没有开启 SSH 协议，AAA 认证模式下用户 user-ssh 的服务类型错误配置成了 telnet，同时 VTY 配置下允许使用的协议错误配置成了 all。

```
<R2>display current-configuration
#
aaa
authentication-scheme default
authorization-scheme default
accounting-scheme default
domain default
domain default_admin
local-user admin password cipher %$%$K8m.Nt84DZ}e#<0'8bmE3Uw}%$%$
local-user admin service-type http
local-user user-ssh password cipher %$%$kVsQ8i_OX#sRkxPV;_D(*dEq%$%$
local-user user-ssh privilege level 3
local-user user-ssh service-type telnet
#
user-interface vty 0 4
authentication-mode aaa
protocol inbound all
```

使用“stelnet server enable”命令开启 SSH 服务，并创建本地密钥。

```
[R2] ssh user user-ssh authentication-type password
[R2] stelnet server enable
[R2] rsa local-key-pair create
```

使用“service-type”命令配置用户接入类型为 SSH。

```
[R2] aaa
[R2-aaa] local-user user-ssh service-type ssh
```

使用“protocol inbound”命令将允许使用的协议改为 SSH。

```
[R2] user-interface vty 0 4
[R2-ui-vty0-4] protocol inbound ssh
```

在 R1 和 R3 上进行 SSH 初始配置。

```
<R1> system-view
[R1] ssh client first-time enable
```

```
<R3> system-view
[R3] ssh client first-time enable
```

3. 在新配置环境下进行测试

1)测试 Client1 登录 FTP 服务器

在 Client1 窗口的“客户端信息”选项卡的 FtpClient 界面中输入正确的服务器地址、端口号等参数,单击“登录”按钮,可以看到成功登录 FTP 服务器,显示出服务器文件列表,如图 1-2-7 所示。

图 1-2-7　Client1 成功登录 FTP 服务器

2)测试 R2 登录 FTP 服务器

在 R2 上使用“ftp 12.2.1.1”命令进行测试,输入用户名 huawei 及对应密码 huawei@123,结果显示 R2 正常远程登录 FTP 服务器。

```
<R2>ftp 12.2.1.1
Trying 12.2.1.1 ...
Press CTRL+K to abort
Connected to 12.2.1.1.
220 FtpServerTry FtpD for free
User(12.2.1.1:(none)):
331 Password required for huawei .
Enter password:
```

```
230 User huawei logged in , proceed
[R2-ftp]
```

3)测试 R1、R3 登录 SSH 服务器 R2

在 R1 和 R3 上进行 Telnet 测试，结果显示 R1 和 R3 无法访问 R2。

```
<R1>telnet 12.1.1.2
  Press CTRL_] to quit telnet mode
  Trying 12.1.1.2 ...
  Error: Can't connect to the remote host
```

```
<R3>telnet 12.1.1.2
  Press CTRL_] to quit telnet mode
  Trying 12.1.1.2 ...
  Error: Can't connect to the remote host
```

而在 R1 和 R3 上进行 SSH 测试，结果显示 R1 和 R3 可以正常访问 R2，符合任务要求。

```
[R1] stelnet 12.1.1.2
Please input the username: user-ssh
Trying 12.1.1.2 ...
Press CTRL+K to abort
Connected to 12.1.1.2 ...
Enter password: * * * * * * * *
<R2>
```

```
[R3] stelnet 12.1.1.2
Please input the username: user-ssh
Trying 12.1.1.2 ...
Press CTRL+K to abort
Connected to 12.1.1.2 ...
Enter password: * * * * * * * *
<R2>
```

4)测试结果汇总

在 Client1 和 R2 上测试远程访问 FTP 服务器后，在 R1 和 R3 上测试使用“stelnet”命令远程登录 R2，将测试结果进行记录，如表 1-2-3 所示。实际测试结果与预期效果一致，完成故障处理与优化。

表 1-2-3　修改后 SSH 测试结果汇总

序号	设备 1	设备 2	测试方法	预期测试结果	实际测试结果	是否发生故障
1	Client1	FTP 服务器	FTP	成功	成功	否
2	R2	FTP 服务器	FTP	成功	成功	否
3	R1	R2	SSH	成功	Telnet 失败，SSH 成功	否
4	R3	R2	SSH	成功	Telnet 失败，SSH 成功	否

4. 任务总结

本任务主要针对 SSH 协议配置的故障排除，以理论化故障排除思路为指导，以任务式驱动为方法，形象再现了 SSH 协议的原理学习和操作实现过程，为未来实际环境的 SSH 协议故障排除提供了良好的方法和操作步骤。在实际应用环境中应按照以下故障排除规范来一一检查：第一，检查各设备的 IP 地址规划是否错误；第二，检查 Client1 和 FTP 服务器配置是否错误；第三，检查 SSH 服务器参数配置是否错误等，直到查出所有故障为止。

任务实施单

任务名称		任务 1-2　SSH 故障处理与优化			
班级		完成人		日期	
实施步骤		命令行		设备状态	
故障分析	1. 测试远程访问 FTP 服务器状态	R2： 		Client1 是否存在故障： Client1 故障现象： R2 是否存在故障： R2 故障现象： 	
	2. 在 R1 和 R3 上测试远程访问服务器 R2 状态	R1： R3： 		R1 故障现象： R3 故障现象： 	
故障处理	1. 核查各网络设备的 IP 地址	R1： R2： R3： 		R1 是否存在故障： R1 故障原因及处理方法： R2 是否存在故障： R2 故障原因及处理方法： R3 是否存在故障： R3 故障原因及处理方法： Client1 是否存在故障： Client1 故障原因及处理方法： FTP 服务器是否存在故障： FTP 服务器故障原因及处理方法： 	

续表

实施步骤		命令行	设备状态
故障处理	2. 核查 SSH 服务器 R2 当前参数配置	R2： 	R2 是否存在故障： R2 故障原因及处理方法：
	3. 在 R1 和 R3 上进行 SSH 初始配置	R1： R3： 	
新配置环境下进行测试	测试登录 FTP 服务器及 SSH 服务器	R1： R2： R3： 	实测结果与预期效果是否一致：
任务总结			