实验七：TELNET 与 SSH 协议分析

一、实验目的

1、了解 TELNET 与 SSH 协议；
2、掌握 TELNET 与 SSH 报文结构；
3、了解 TELNET 与 SSH 进行远程设备管理。

二、实验学时

2 学时

扫码看步骤

三、实验类型

验证性

四、实验需求

1、硬件

每人配备计算机 1 台，不低于双核 CPU、8G 内存、500GB 硬盘。

2、软件

推荐 Ubuntu Desktop 操作系统，安装 GNS 3 仿真软件，安装 Wireshark 抓包工具。
支持 Windows 操作系统，安装 GNS 3 仿真软件，安装 Wireshark 抓包工具。

3、网络

计算机使用固定 IP 地址接入局域网，并支持对互联网的访问。

4、工具

无。

五、实验任务

1、通过 TELNET 远程管理交换机；
2、通过 SSH 远程管理路由器；
3、对 TELNET 和 SSH 协议进行分析。

六、实验内容及步骤

任务 1：实验准备

步骤 01：实验拓扑设计
网络拓扑结构，如图 7-1 所示。

步骤 02：实验网络设计

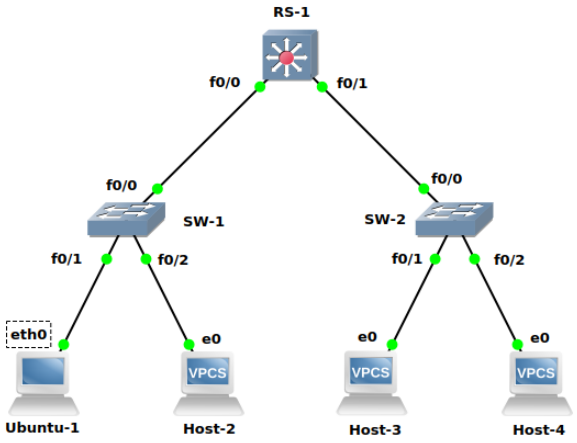

图 7-1 拓扑结构

①本实验涉及的设备说明，如表 7-1 所示。

表 7-1 设备表

设备	设备类型	规格型号	备注
Ubuntu	终端主机	Ubuntu Docker Guest	
Host-2~Host-4	终端主机	--	
SW-1~SW-2	二层交换机	RouteSwitch-3600 （二层模块）	--
RS-1	路由交换机	RouteSwitch-3600	--

②交换机接口与 VLAN 规划，如表 7-2 所示。

表 7-2 交换机接口与 VLAN 规划表

交换机	接口	VLANID	连接设备	接口类型
SW-1	f0/1	11	Ubuntu	Access
SW-1	f0/2	12	Host-2	Access
SW-1	f0/0	--	RS-1	Trunk
SW-2	f0/1	11	Host-3	Access
SW-2	f0/2	12	Host-4	Access
SW-2	f0/0	--	RS-1	Trunk
RS-1	f0/0	--	SW-1	Trunk
RS-1	f0/1	--	SW-2	Trunk

③地址规划，如表 7-3 所示。

表 7-3 主机地址规划表

主机	IP 地址/子网掩码	网关	接入位置	所属 VLANID
Ubuntu	172.16.64.1 /24	172.16.64.254	SW-1 f0/1	11
Host-2	172.16.65.1 /24	172.16.65.254	SW-1 f0/2	12
Host-3	172.16.64.2 /24	172.16.64.254	SW-2 f0/1	11

Host-4	172.16.65.2 /24	172.16.65.254	SW-2 f0/2	12

④交换机接口地址，如表 7-4 所示。

表 7-4 交换机接口地址规划表

交换机	接口	VLANID	地址	接口类型
SW-1	f0/1	11	172.16.64.101/24	Access
SW-1	f0/2	12	172.16.65.101/24	Access
SW-2	f0/1	11	172.16.64.102/24	Access
SW-2	f0/2	12	172.16.65.102/24	Access

⑤路由接口地址，如表 7-5 所示。

表 7-5 路由接口地址规划表

设备名称	接口名称	接口地址	备注
RS-1	VLAN11	172.16.64.254 /24	VLAN11 的 SVI
RS-1	VLAN12	172.16.65.254 /24	VLAN12 的 SVI

⑥路由规划，如表 7-6 所示。

表 7-6 路由规划表

路由设备	目的网络	下一跳地址	路由类型
RS-1	172.16.64.0 /24	172.16.64.254	直连路由
RS-1	172.16.65.0 /24	172.16.65.254	直连路由

步骤 03：在 GNS3 中实现网络

根据以上内容，在 GNS3 中实现实验中所需网路。

步骤 04：实验准备的补充说明

实验中所用到的 Ubuntu 的添加方法请参照实验六。

任务 2：通过 TELNET 远程管理交换机

步骤 01：配置 SW-1 支持 TELNET 远程管理

在 SW-1 上配置 TELNET 服务。

参考命令：

```
SW-1#configure terminal
// 设置 TELNET 用户名和密码
SW-1(config)#username telnet secret 123
// 设置同时打开 0 到 4 共 5 个会话
SW-1(config)#line vty 0 4
// 开启登录
SW-1(config-line)#login local
SW-1(config-line)# exit
SW-1(config)# exit
SW-1# write
```

步骤 02：设置抓包点，启动 Wireshark 进行抓包

在 Ubuntu 与 SW-1 之间设置抓包点，并启动 Wireshark 进行抓包，如图 7-2 所示。

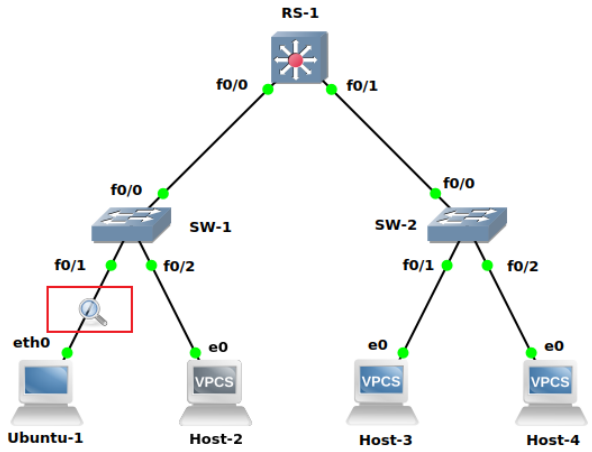

图 7-2 设置抓包点

步骤 03：在管理终端上使用 TELNET 远程管理 SW-1

打开 Ubuntu 的终端，在终端中通过 TELNET 工具远程登录 SW-1。

参考命令：

```
root@Ubuntu:~# telnet 172.16.64.101
// 输入用户名和密码
Username：telnet
Password：123
```

步骤 04：配置 SW-2 支持 TELNET 远程管理。

参照 SW-1 配置方法，实现对 SW-2 的 TELNET 远程管理。并使用 Ubuntu 通过 TELNET 工具进行测试。

步骤 05：分析对 SW-1 进行远程管理的通信报文。

在 Wireshark 中过滤出通过 TELNET 工具远程登录 SW-1 产生到的 TELNET 报文，通过报文分析的方法找到 SW-1 的账号和口令。

将能够分析出账号和口令的报文信息，填写到表 7-7。

表 7-7 TELNET 报文分析表

源地址 IP 地址	目的 IP 地址	源端口	目的端口	数据内容
…				

任务 3：通过 SSH 远程管理路由器

步骤 01：配置 RS-1 支持 SSH 远程管理

在网络拓扑中对 RS-1 配置 SSH 服务。

参考命令：

```
RS-1#configure terminal
RS-1#configure terminal
// 设置主机域名，开始 SSH 的必须
RS -1(config)#ip domain-name teachdemo.com
// 开启 3A 认证
RS -1(config)#aaa new-model
// 生成 rsa 密钥
RS -1(config)#crypto key generate rsa
// 请注意：设置密钥长度时，填写 1024，因为 ssh2 要求至少为 768。
// 看到 ssh 2.0 开启成功后，说明配置正确。
// 如果需要删除 RSA 密钥，请使用 crypto key zeroize rsa
// 设置登录用户名和密码
RS-1(config)#username demouser privilege 0 secret Demo#123456
// privilege 0 表示 ssh 时不会自动进入特权模式
// 密码一定要满足 SSH 2 的复杂密码要求
// 设置 enable 特权密码
RS-1(config)#enable secret Demo#987654321
// 配置 vty 虚拟终端
RS-1(config)#line vty 0 4
// 4 是最大并行连接数
// 设置仅允许 SSH 登录
RS-1(config-line)#transport input ssh
// 设置超时时间
RS-1(config-line)#exec-timeout 10 0
RS-1(config-line)#exit
// 完成 SSH 的其他配置
// 设置认证失败次数
RS-1(config)#ip ssh authentication-retries 3
// 设置超时时间，单位是秒
RS -1(config)#ip ssh time-out 30
// 设置 SSH 的协议版本
RS-1(config)#ip ssh version 2
RS-1(config)#exit
// 保存配置信息
RS-1#write
```

步骤 02：设置抓包点，启动 Wireshark 进行抓包

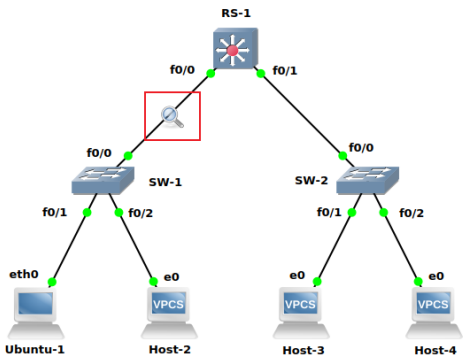

图 7-3 设置抓包点

在 Ubuntu 与 SW-1 之间设置抓包点，并启动 Wireshark 进行抓包，如图 7-3 所示。

步骤 03：在管理终端上使用 SSH 远程管理 RS-1

打开 Ubuntu 的终端，在终端中通过 SSH 工具远程登录 RS-1。

参考命令：

```
// 输入用户名和主机 IP
root@Ubuntu:~# ssh -l demouser 172.16.64.254
// 输入密码（参见步骤 01 的配置，密码为 Demo#123456
Password:
```

注意：

如果在登陆时出现下属错误：

```
root@Ubuntu-1:~# ssh -l teachuser 172.16.64.254
Unable to negotiate with 172.16.64.254 port 22: no matching key exchange method found. Their offer: diffie-hellman-group1-sha1
```

请在 Host 中进行下述操作，在 ssh_config 配置文件中增加一行。

```
vi /etc/ssh/ssh_config
增加的内容如下，放置在配置文件的最后一行即可：
KexAlgorithms +diffie-hellman-group1-sha1
```

步骤 04：分析对 RS-1 进行远程管理的通信报文

在 Wireshark 中过滤出通过 SSH 工具远程登录 RS-1 产生到的 SSH 报文，并通过报文分析的方法找到 RS-1 的账号和口令。

如果找不到账号和口令，请说明为什么？并根据报文总结 SSH 进行远程管理的通信分为哪几个阶段。

七、实验考核

实验考核分为【实验随堂查】和【实验线上考】两个部分。

实验随堂查：每个实验设置 3-5 考核点。完成实验任务后，任课教师随机选择一个考核点，学生现场进行演示和汇报讲解。

实验线上考：每个实验设置 5-10 个客观题。通过线上考核平台（课堂派）进行作答。

1、实验随堂查

本实验随堂查设置 3 个考核点，具体如下。

考核点 1：实现通过 TELNET 进行远程管理。

考核点 2：实现通过 SSH 进行远程管理。

考核点 3：完成 TELNET 和 SSH 的通信分析。

2、实验线上考

本实验线上考共 10 题，其中单选 3 题、多选 2 题、判断 3 题、填空 2 题。