

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 的特点和应用。

二、实验学时

2 学时

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。

六、实验考核

- 1、基本考核：提交实验报告册；
- 2、实验考核：无。

七、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。

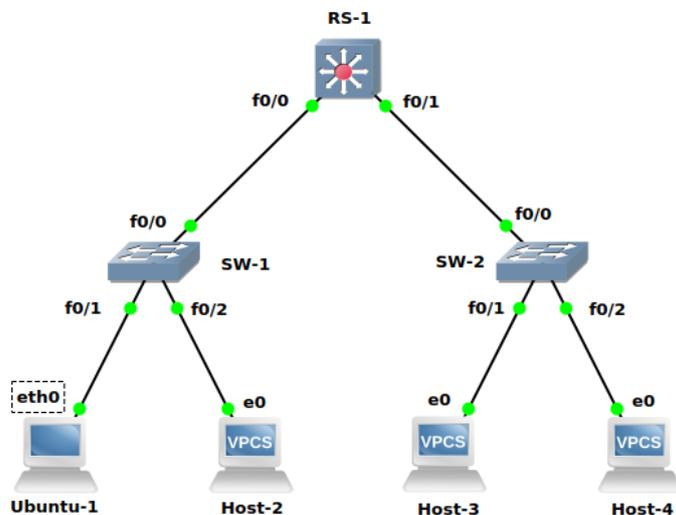


图 7-1 拓扑结构

步骤 02：实验网络设计

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 |
|---------------|-------|-----------------------|------------------------------|
| Host-1~Host-4 | 终端主机 | -- | Host-1 为 UbuntuDockerGuest-1 |
| SW-1~SW-2 | 二层交换机 | CISCO C3640 (二层模块) | -- |
| RS-1 | 路由交换机 | CISCO C3640 | -- |

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 | Host-1 | 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 |
|--------|-----------------|---------------|-----------|-----------|
| Host-1 | 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 | -- |
| RS-1 | VLAN12 | 172.16.65.254 /24 | -- |

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，具体配置方法请参考实验一。

步骤 04: 实验准备的补充说明

实验中所用到的 Ubuntu-1 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)#login local
SW-1(config)# exit
SW-1# write
```

步骤 02: 设置抓包点, 启动 Wireshark 进行抓包

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

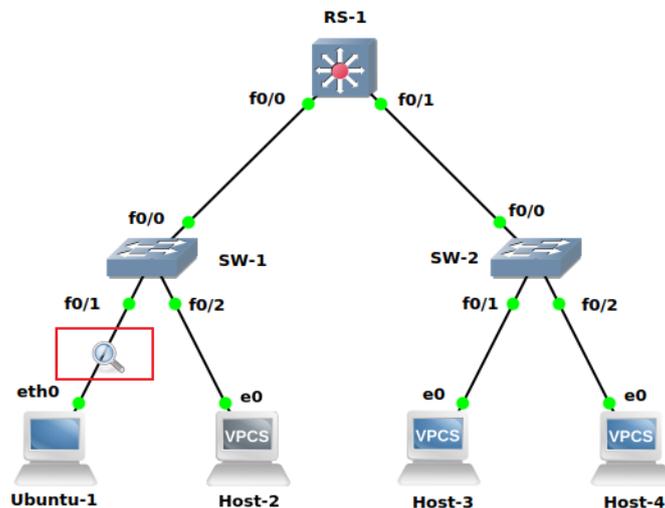


图 7-2 设置抓包点

步骤 03: 在管理终端上使用 TELNET 远程管理 SW-1

打开 Ubuntu-1 的终端, 在终端中通过 TELNET 工具远程登录 SW-1, 如图 7-3 所示。

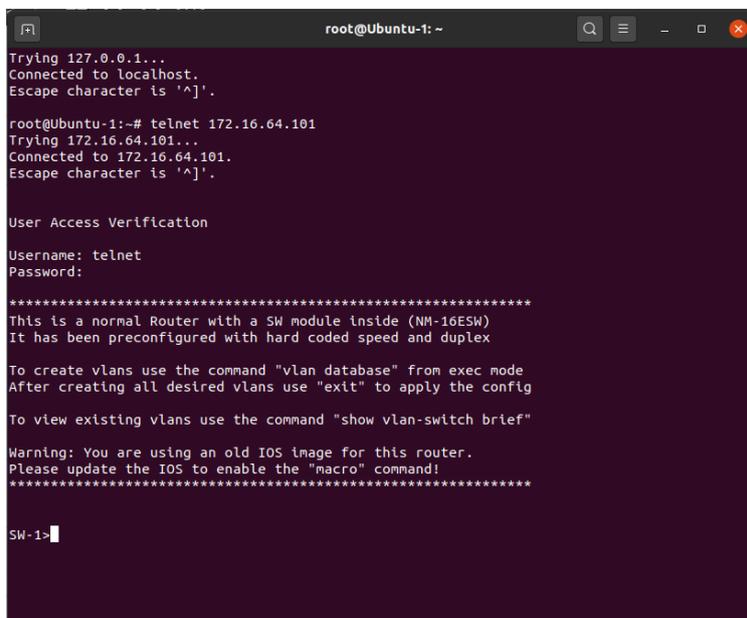


图 7-3 远程登录 SW-1

参考命令:

```
root@Ubuntu-1:~# telnet 172.16.64.101
// 输入用户名和密码
Username: telnet
```

Password: 123

实验考核要求:

- 考核点 7-1: 在 Ubuntu-1 上使用 TELNET 远程登录 SW-1, 将截图结果填写到实验报告册。

步骤 04: 配置 SW-2 支持 TELNET 远程管理。

参照 SW-1 配置方法对 SW-2 进行 TELNET 服务搭建。

步骤 05: 在管理终端上使用 TELNET 远程管理 SW-2。

参照上述实验使用 Ubuntu-1 通过 TELNET 工具远程登录 SW-2。

实验考核要求:

- 考核点 7-2: 完成 SW-2 的配置, 并使用 Ubuntu-1 远程登录 SW-2, 将截图结果填写到实验报告册。

步骤 06: 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 RS-1 产生到的 TELNET 报文, 并按照要求填写以下表格, 如表 7-7 所示。

表 7-7 TELNET 报文分析表

| 源地址/源端口 | 目的地址/目的端口 | 报文内容 | 十六进制表示 | 大小 (byte) |
|---------|-----------|------|--------|-----------|
| | | | | |
| | | | | |
| | | | | |
| | | | | |

实验考核要求:

- 考核点 7-3: 完成表 7-7, 将结果填写到实验报告册。

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:

```
SW-1#configure terminal
// 设置超时时间
SW-1(config)#ip ssh time-out 30
// 设置认证失败次数
SW-1(config)#ip ssh authentication-retries 3
```

```

// 设置主机域名
SW-1(config)#ip domain-name cisco.com
// 生成 rsa 密钥
SW-1(config)#crypto key generate rsa
// 设置登录用户名和密码
SW-1(config)#username ssh secret 456
SW-1(config)#line vty 0 4
// 设置 ssh 登录
SW-1(config-line)#transport input ssh
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-1 与 SW-1 之间设置抓包点, 并启动 Wireshark 进行抓包, 如图 7-4 所示。

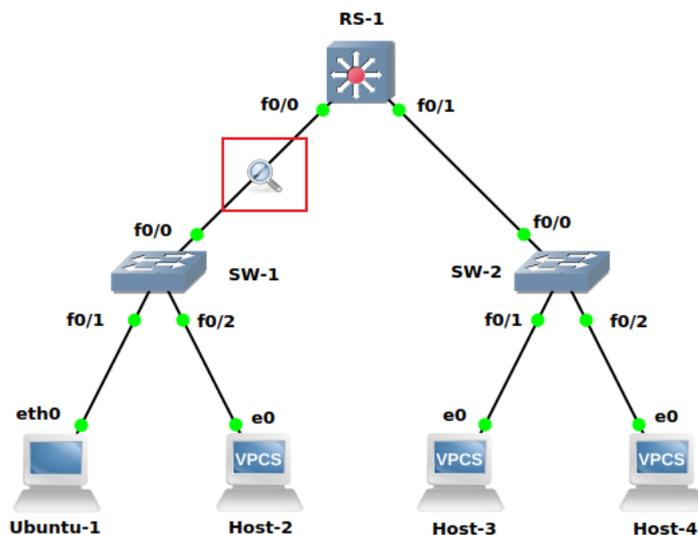


图 7-4 设置抓包点

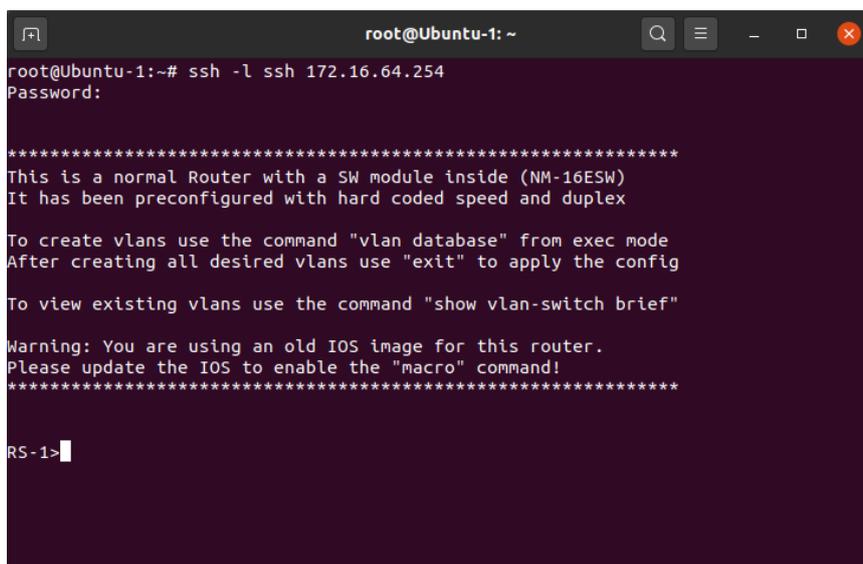


图 7-5 SSH 远程登录

步骤 03: 在管理终端上使用 SSH 远程管理 RS-1

打开 Ubuntu-1 的终端，在终端中通过 SSH 工具远程登录 RS-1，如图 7-5 所示。

参考命令：

```
// 输入用户名和主机 IP
root@Ubuntu-1:~# ssh -l ssh 172.16.64.101
// 输入密码
Password: 456
```

注意：如在登录过程中出现以下提示
Unable to negotiate with xx.xx.xx.xx port 22: no matching key exchange method.found.Their.offer:diffie-hellman-group1-sha1

解决方法：修改 Ubuntu-1 的 SSH 客户端配置 (/etc/ssh/ssh_config) 文件，通过使用 vi 命令在文件最后加上一行：**【KexAlgorithms +diffie-hellman-group1-sha1】** (此处+号前有个空格)

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，并按照要求填写以下表格，如表 7-7 所示。

表 7-7 SSH 报文分析表

| 序号 | 源地址/ 源端口 | 目的地址/ 目的端口 | 报文内容 | 大小 (byte) | 通信阶段 |
|----|-------------|---------------|------|--------------|------|
| 1 | | | | | |
| | | | | | |
| 2 | | | | | |
| | | | | | |
| 3 | | | | | |
| | | | | | |
| 4 | | | | | |
| | | | | | |

请解释报文中字段含义，如表 7-8 所示。

表 7-8 SSH 报文字段含义表

| 序号 | 名称 | 含义 |
|----|---|----|
| 1 | kex_algorithms | |
| 2 | server_host_key_algorithms | |
| 3 | encryption_algorithms_client_to_server | |
| 4 | encryption_algorithms_server_to_client | |
| 5 | mac_algorithms_client_to_server | |
| 6 | mac_algorithms_server_to_client | |
| 7 | compression_algorithms_client_to_server | |
| 8 | compression_algorithms_server_to_client | |
| 9 | languages_client_to_server | |
| 10 | languages_server_to_client | |

实验考核要求:

- 考核点 7-4: 完成表 7-7 和 7-8, 将结果填写到实验报告册。
-

八、实验思考

1、认识 TELNET 与 SSH

- (1) 通过上述实验, 比较 TELNET 与 SSH 有何不同?
- (2) TELNET 协议为什么要协商操作选项?

2、深入理解

(1) 根据对 SSH 登录报文的分析, 在 Ubuntu-1 中使用 SSH 远程登录 RS-1 时为什么会出出现以下错误, 请简要说明原因。

Unable to negotiate with xx.xx.xx.xx port 22: no matching key exchange method found. Their offer: diffie-hellman-group1-sha1。

- (2) SSH 的认证方式有几种, 请简要说明?