**实验  SSH访问交换机/路由器**

**1.实验目的**

通过本实验可以掌握：

①SSH的配置。

②SSH的访问方式。

**2.实验拓扑**

SSH配置实验拓扑如图2-1所示。



**3.相关知识补充**

过去对路由器的远程管理访问一般使用TCP端口23上的Telnet。但Telnet是在安全不是问题的年代开发的。为此，所有Telnet流量以明文的形式转发。

SSH已经替代了Telnet，作为远程路由器连接管理的最佳工具，它提供强大的私密性和会话的集成。SSH使用TCP端口22。它提供类似出站Telnet连接的功能，但连接是加密的。通过认证和加密，SSH允许在不安全的网络中进行安全的通信。想在路由器上激活SSH，必须配置以下参数：  

**Hostname（主机名）  **

**Domain name（域名）**

**Asymmetrical keys（非对称密钥）  **

**Local authentication（本地验证）**

4.实验步骤

本实验对S1允许SSH访问，但禁止Telnet访问。

1. 对交换机和PC1作初始配置

 S1(config)#enable secret cisco123

 S1(config)#line vty 0 15

S1(config-line)#password cisco

S1(config-line)#login

S1(config-line)#exit

S1(config)#int vlan 1

S1(config-if)#ip address 1.1.1.1 255.255.255.0

S1(config-if)#no shut

（2）配置主机名和域名

S1(config-if)#exit

S1(config)#hostname zzz

zzz (config)#ip domain-name myccnp.com

zzz (config)#

//要生成密钥，必须配置域名

（3）配置非对称密钥

zzz (config)#crypto key generate rsa

//当提示密钥长度时，输入1024。注：缺省为512。

（4）配置用于认证的登录用户名及口令

zzz (config)#username admin password cisco

（5）配置SSH版本

zzz (config)#ip ssh version 2

Please create RSA keys (of at least 768 bits size) to enable SSH v2.

（6）配置SSH会话最大空闲超时值和SSH连接认证重试次数

zzz (config)#ip ssh time-out 60      //最大空闲超时：60秒

zzz (config)#ip ssh authentication-retries 2  //认证重试次数：2次  S1(config)#

（7）在VTY线路上禁用Telnet，并激活SSH。

zzz (config)#line vty 0 15

zzz (config-line)#no transport input all //禁用所有流量

zzz (config-line)#transport input ssh  //允许SSH流量

 zzz (config-line)#login local      //要求本地认证

（8）在S1上验证SSH的配置及运行

1)  验证SSH版本及其他设置

zzz #show ip ssh

SSH Enabled – version 2.0

Authentication timeout: 60 secs; Authentication retries: 2

2)  验证SSH是否在运行

zzz #show ssh

%No SSHv2 server connections running.

%No SSHv1 server connections running.

（9）在在PC0的命令行窗口中对R1和R2分别进行telnet 和ssh的测试， telnet 应失败，而ssh应成功。

PC>telnet 1.1.1.1

Trying 1.1.1.1 ...Open

[Connection to 1.1.1.1 closed by foreign host]

//以上表示telnet不成功。

 PC>ssh -l admin 1.1.1.1

Open

Password:

zzz >en

Password:

zzz #

//以上表示SSH成功。