

1、配置 SSH

R1#conf t

R1(config)#int s1/0

R1(config-if)#ip add 10.1.12.1 255.255.255.0

R1(config-if)#no shut

R1(config-if)#exi

R1(config)#ip domain-name cisco.com -----为路由器配置一个域名，也可以认为该路由器属于这个域。

R1(config)#crypto key generate rsa -----生成一个为 rsa 算法的密钥

The name for the keys will be: R1.cisco.com

Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes.

How many bits in the modulus [512]: 1024 -----设置密钥为 1024 位

% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

*Mar 1 00:59:17.179: %SSH-5-ENABLED: SSH 1.99 has been enabled

PS: 在 Cisoc 中 rsa 支持 360-2048 位密钥，该算法的原理是：主机将自己的公用密钥分发给相关的客户机，客户机在访问主机时则使用该主机的公开密钥来加密数据，主机则使用自己的私有的密钥来解密数据，从而实现主机密钥认证，确定客户机的可靠身份。

R1(config)#line vty 0 15

R1(config-line)#login local -----设置使用本地数据库,即使用创建的用户名和密码。

R1(config-line)#transport input none -----关闭 VTY 其他的远程登录协议

R1(config-line)#transport input ssh -----配置只允许 SSH 登录，即其他远程登录方式不可使用，如 telnet。

R1(config-line)#exi

R1(config)#username admin password admin -----创建用户以及密码

R1(config)#enable secret cisco -----设置特权密码

R1(config)#ip ssh version 2 -----设置 SSH 版本号

R1(config)#end

R1#

2、登录测试

R2#telnet 10.1.12.1

```
Trying 10.1.12.1 ...
% Connection refused by remote host
R2#
R2#ssh -l admin 10.1.12.1
Password: 此处密码为 admin 用户的密码 admin
R1>en
Password: 此处密码为特权密码 cisco
R1#
```

ssh 一般配置步骤如下：

1.
先改主机名，hostname xxxx
- 2.
3.
加个域名：ip domain-name
- 4.
5.
创建 RSA 密钥对：crypto key generate rsa
- 6.
7.
输入密钥长度，默认：512，建议 1024
- 8.
9.
配置用户名密码：username xxx password xxx
- 10.
11.
进入虚拟终端：line vty 0 4
- 12.
13.
允许 ssh 连接：transport input ssh
- 14.
15.
建议把 ssh 版本改为 2：ip ssh version 2
- 16.