SSH简单原理及在CiscoIOS设备上启用SSH思科认证 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/644/2021_2022_SSH_E7_AE_80_E5_8D_95_E5_c101_644045.htm 编辑特别推荐: 全国计算机等级考试（等考）指定教材 全国计算机等级考试学习视频 全国计算机等级考试网上辅导招生 全国计算机等级考试时间及科目预告 百考试题教育全国计算机等级考试在线测试平台 全国计算机等级考试资料下载 全国计算机等级考试论坛 SSH(Secure Shell)是什么呢？权威的说法是：‘ Secure shell is a de facto standard for remote logins and encrypted file transfers. ’。SSH由芬兰赫尔辛基大学的Tatu Ylonen在1995年发明，其主要目的就是通过认证和加密手段在互联网提供一条安全的连接(并不仅是Terminal)，默认运行于TCP 22号端口。目前有两种协议版本：SSH-1和SSH-2。 要理解SSH首先要明白它的几把Key: Host Key / Server Key / Session Key / User Key 具体见下表: Name Lifetime Created by Type Purpose Host key Persistent Administrator Public Identify a server/machine Server key One hour Server Public Encrypt the session key(SSH1 only) Session key One session Client (and server) Secret Protect communications User key Persistent User Public Identify a user to the server SSH简单的运行过程如下： 1、Client端向Server端发起SSH连接请求。 2、Server端向Client端发起版本协商。 3、协商结束后Server端发送Host Key公钥 Server Key公钥，随机数等信息。到这里所有通信是不加密的。 4、Client端返回确认信息，同时附带用公钥加密过的一个随机数，用于双方计算Session Key。 5、进入认证阶段。从此以后所有通信均加密。 6、认证成功后，

进入交互阶段。 我这里写的极其简单，有兴趣参考这本书：SSH the Secure Shell 2nd Edition 或者参看RFC：http://www.ietf.org/rfc/rfc4251.txt 也可看看这里：http://www.51cto.com/art/200511/12308.htm 在Cisco IOS设备上启用SSH Cisco 在SSH的支持上动作迟缓，12.0开始引入SSH-1，12.1开始引入SSH-2，至今都只实现了一个精简版的SSH，很多东西都不支持，比如 BlowFish算法。Cisco似乎并不是很热心于SSH带来的安全性。可能在Cisco的逻辑中，对网络设备的访问处于严格受限专网当中，想从中进行Sniffer非常不容易。我也亲见过许多大型运营商的DCN网里面完全采用了Telnet，似乎也没有什么大的问题。因为，如果入侵者是处心积虑的高手，SSH也存在着问题，比如man-in-the-middle攻击，处理起来就会加大管理成本。还是那句话，安全是没有绝对的。 对于没有专网，同时在限定访问地址范围内存在Sniffer可能性的网络设备，开启SSH还是有必要的，下面就是配置步骤： 1、设定IOS设备主机名 Router(config)#host SSH-Test 2、设定IOS设备所在域名 SSH-Test(config)#ip domain-name test.com 3、建立RSA公钥(这是我们前面提到的哪一个Key?) SSH-Test(config)#crypto key generate rsa 这时系统会提示你输入modulus的长度，默认为512，取值范围是360-2048，越长安全性越好，但Key的生成时间也会越长，这是个2500上的耗时参考表： Router 360 bits 512 bits 1024 bits 2048 bits (maximum) Cisco 2500 11 seconds 20 seconds 4 minutes 38 seconds more than 1 hour 注意，这条命令是一次性的，不会被保存到startup-config中。但是在执行这条命令后再保存配置，所生成的RSA Key会被保存到nvram

的Private-Config中。 RSA Key可以用这条命令查看：
SSH-Test#sh crypto key mypubkey rsa 4、设置ssh访问特性(可选)
SSH-Test(config)#ip ssh time-out 60 !ssh会话超时时间，以秒为单位 SSH-Test(config)#ip ssh authentication-retries 3 !ssh登录认证重试次数 5、开启本地用户认证 SSH-Test(config)#username test password test SSH-Test(config)#line vty 0 4
SSH-Test(config-line)#login local !也可以用aaa new-model命令 6、限定只能用SSH登录 SSH-Test(config)#line vty 0 4
SSH-Test(config-line)#transport input ssh 7、用access-class限定特定IP可以向本设备发起SSH连接 略 好了，可以用PuTTY测试一下了。 补充： 1、Cisco上的3DES Feature是要花钱买的，如果你用的是普通DES加密的时候，PuTTY会提示你，确认即可。 2、将Cisco IOS作为SSH客户端时，使用ssh命令即可，参数很简单。注意从一个3DES设备访问一个DES设备的时候，要用-c参数将加密算法改为DES。 3、开启SSH服务后，banner login将不被显示，banner motd将在登录后显示。 相关参考资料：
http://www.cisco.com/en/US/tech/tk583/tk617/technologies_tech_note09186a00800949e2.shtml
http://www.cisco.com/en/US/tech/tk583/tk617/tsd_technology_support_protocol_home.html 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com