Cisco路由器用 H替代Telnet连接 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/267/2021_2022_Cisco_E8_B7_AF_E7_94_c101_267165.htm 如果你一直利用Telnet控制网络设备，你可以考虑采用其他更安全的方式。本文告诉你如何用SSH替换Telnet. 使用Telnet这个用来访问远程计算机的TCP/IP协议以控制你的网络设备相当于在离开某个建筑时大喊你的用户名和口令。很快地，会有人进行监听，并且他们会利用你安全意识的缺乏。 SSH是替代Telnet和其他远程控制台管理应用程序的行业标准。SSH命令是加密的并以几种方式进行保密。 在使用SSH的时候，一个数字证书将认证客户端（你的工作站）和服务器（你的网络设备）之间的连接，并加密受保护的口令。SSH1使用RSA加密密钥，SSH2使用数字签名算法（DSA）密钥保护连接和认证。 加密算法包括Blowfish，数据加密标准（DES），以及三重DES（3DES）。SSH保护并且有助于防止欺骗，“ 中间人 ”攻击，以及数据包监听。 实施SSH的第一步是验证你的设备支持SSH.请登录你的路由器或交换机，并确定你是否加载了一个支持SSH的IPSec IOS镜像。 在我们的例子中，我们将使用Cisco IOS命令。运行下面的命令：Router> Show flash 该命令显示已加载的IOS镜像名称。你可以用结果对比你的供应商的支持特性列表。 在你验证了你的设备支持SSH之后，请确保设备拥有一个主机名和配置正确的主机域，就像下面的一样：Router> config terminalRouter (config)# hostname hostnameRouter (config)# ip domain-name domainname 在这个时候，你就可以启用路由器上的SSH服务器。要启用SSH服务器，你首先必须

利用下面的命令产生一对RSA密钥：Router (config)# crypto key generate rsa 在路由器上产生一对RSA密钥就会自动启用SSH.如果你删除这对RSA密钥，就会自动禁用该SSH服务器。 实施SSH的最后一步是启用认证，授权和审计（AAA）。在你配置AAA的时候，请指定用户名和口令，会话超时时间，一个连接允许的尝试次数。像下面这样使用命令：Router (config)# aaa new-modelRouter (config)# username passwordRouter (config)# ip ssh time-outRouter (config)# ip ssh authentication-retries 要验证你已经配置了SSH并且它正运行在你的路由器上，执行下面的命令：Router# show ip ssh 在验证了配置之后，你就可以强制那些你在AAA配置过程中添加的用户使用SSH，而不是Telnet.你也可以在虚拟终端（vty）连接中应用SSH而实现同样的目的。这里给出一个例子：Router (config)# line vty 0 4Router (config-line)# transport input SSH 在你关闭现存的Telnet会话之前，你需要一个SSH终端客户端程序以测试你的配置。我极力推荐PuTTY；它是免费的，而且它是一个优秀的终端软件。 最后的想法 当你在你的路由器和交换机上启用了SSH之后，保证你修改了所有现存的访问控制列表以允许对这些设备的连接。你现在可以向你的上级报告你已经堵上了一个巨大的安全漏洞：现在所有的网络管理会话都被加密并且被保护着。 