

**Packet** **Tracer** **-** 配置 **SSH**

地址分配表

|  |  |  |  |
| --- | --- | --- | --- |
| 设备 | 接口 | **IP** 地址 | 子网掩码 |
| S1 | VLAN 1 | 10.10.10.2 | 255.255.255.0 |
| PC1 | NIC | 10.10.10.10 | 255.255.255.0 |

目标

第 **1** 部分：保护密码

第 **2** 部分：加密通信

第 **3** 部分：验证 **SSH** 实施

背景信息

SSH 应替代 Telnet 来管理连接。 Telnet 使用不安全的明文通信。SSH 则会为设备之间的所有传输数据提供强 加密，确保远程连接的安全。在这个练习中，您会使用密码加密和 SSH 来保护远程交换机。

说明

第 **1** 部分： 保护密码

a. 在 **PC1** 上使用命令提示符通过 Telnet 访问 **S1**。用户执行和特权执行密码为 **cisco**。

b. 保存当前配置， 以便可通过切换 **S1** 的电源修复您可能做出的任何错误操作。

c. 显示当前配置并注意密码是否采用明文。输入用于加密明文密码的命令： S1(config)# **service** **password-encryption**

d. 验证密码是否已加密。

第 **2** 部分： 加密通信

步骤 **1** ： 设置 **IP** 域名并生成安全的密钥。

通常，使用 Telnet 并不安全，因为数据是以明文形式传输。因此，只要 SSH 可用，就应使用 SSH。

a. 将域名配置为 **netacad.pka**。

b. 需要使用安全的密钥加密数据。使用 1024 作为密钥长度生成 RSA 密钥。

步骤 **2** ： 创建 **SSH** 用户并重新配置 **VTY** 线路为仅限 **SSH** 访问。

a. 使用 **cisco** 作为加密密码创建 **administrator** 用户。

b. 将 VTY 线路配置为检查本地用户名数据库查找登录凭证，以及仅允许使用 SSH 进行远程访问。删除现有 vty 线路密码。

2013 年 - 2020 思科和/或其附属公司。版权所有。思科公开信息 第 **1** 页 **2** www.netacad.com

步骤 **3** ： 验证 **SSH** 实施

a. 退出 Telnet 会话并尝试使用 Telnet 重新登录。该尝试应该会失败。

b. 尝试使用 SSH 登录。键入 **ssh**，然后按 **Enter**，不使用任何参数显示命令使用情况说明。 提示：**-l** 选项 为字母“L”，不是数字 1。

c. 成功登录后，进入特权模式并保存配置。如果您无法成功访问 **S1**，则切换电源， 然后再次从第 1 部分开 始。

*文档结尾*

2013 年 - 2020 思科和/或其附属公司。版权所有。思科公开信息 第 **2** 页 **2** www.netacad.com