视频 - 保护访问方法（9 分钟）

您在网络上安装设备时，比如一台 Cisco 系列交换机，想要做的第一件事是保证设备访问的安全性，只有管理员有权配置它或者更改它的设置。为此，我们需要设置一些初始配置设置来确保访问安全。我将点击台式 PC 并点击终端模拟程序，此刻您可以看到我与交换机建立了一个控制台连接。

在本视频中，我将直接在交换机上使用命令行界面。您可以看到，我已在用户执行模式下您可以看到，我已经登录到交换机登录到交换机，没有经过任何身份验证。进入到用户执行模式，没有经过任何身份验证。这是一种安全性风险。一种更高的安全性风险是我也可以输入 enable 命令来进入特权执行模式，而无需任何类型的身份验证或密码。在特权执行模式下，我可以开始配置交换机，我们要做的第一件事是保护对特权执行模式的访问。

为此，我将进入全局配置模式并输入命令“enable secret”，然后输入密码。您会希望尽可能使用复杂的强密码。因为这是一个测试案例场景，所以我将使用密码“class”。“secret”参数可以保证密码“class”将在配置文件中加密。此命令的一种替代形式是“enable password class”。该命令的这种形式不会在配置文件中为密码加密。所以我将删除该命令。我们看看 enable secret password class 是否有效。我将按 Ctrl+C 进入特权执行模式，然后退出交换机。下面按回车键。我现在处于特权执行模式。输入“enable”，可以看到我被要求输入密码。我输入密码时，您无法看到我输入的任何字符。我将输入“class”并按回车键，可以看到我现在处于特权执行模式。

我们看看截至目前的运行配置。我们可以输入命令“show running-config”来查看我们的运行配置。按回车键后，可以在顶部看到我们的“enable secret”命令。5 表示它是 MD5 散列，这是我们的密码“class”的单向散列值。因此您可以看到“enable secret”命令是如何模糊处理配置文件中的密码的。是如何隐藏配置文件中的密码的。要查看配置文件的剩余内容，可以按键盘上的空格键。现在我们已加密“enable password”或接入了特权执行模式，或进入特权执行模式的密码，但如何保护通过控制台对交换机的访问呢？我们也可以保护该访问。为此，我将输入“enable”、密码“class”，我将使用“conf t”命令进入全局配置模式，而且需要进入 line console 0 的线路配置模式。我将输入“line console 0”，现在我处于线路配置模式。我现在可以输入控制台连接的密码。我将输入“password”，通常我会使用复杂的密码，但对于本演示，我将使用密码“cisco”并按回车键。我输入“login”命令，该命令在 line console 0 上启用全局管理登录。确保控制台端口的安全性后，我还想保护用于远程登录的虚拟终端访问。我将输入“line vty”来表示虚拟终端或虚拟电传，然后输入我想允许远程访问的线路数。Cisco 交换机支持通过 16 个虚拟终端同时进行远程登录。要配置所有 16 次登录，我只需输入表示第一个终端的 0、一个空格，然后输入我想要配置的最后一个终端。在本例中我将输入 15。我将能够配置虚拟终端 0 到 15。我将输入“password cisco”，然后输入 login 命令。

我们在运行配置中看看这些密码。为此，我将按 Ctrl+C 来进入特权执行模式，然后输入命令“show run”，这是“show running-config”的缩写。按 Tab 键后，您可以看到完整的命令。这是运行配置文件。我按下空格键，向底部移动，您可以看到 line con 0、line vty 0 到 4 和 line vty 5 到 15 的配置。IOS 将虚拟终端线路分为两组：0 到 4 和 5 到 15。请注意密码“cisco”显示为明文。这不同于“enable secret password”，后者通过单向散列函数加密。如果可以加密这些密码，使它们不再显示为明文，我们可以显著增加交换机的安全性。

为此，我将返回到全局配置模式并输入命令“service password-encryption”。此命令将对交换机上的所有密码执行轻量级的加密。现在如果我们返回到特权执行模式并查看运行配置文件.....可以看到此结果，按空格键移动到底部，可以看到现在密码“cisco”已使用类型 7 加密算法加密。这不是很强的加密形式但它添加了一个安全层。保护交换机访问的另一个重要的初始配置命令是设置一条标语消息。为此，我将进入全局配置模式并键入命令“banner motd”表示“当日消息”。现在我可以输入一条会在用户登录时向他们显示的消息。此消息将充当针对未授权用户的法律警告，告知他们正在非法侵入，我们将采取法律行动。我现在可以输入安全性消息。我输入的消息将需要放在两个分隔符之间。使用一个不是消息中的字符的分隔符是个不错的主意。例如，我将使用引号作为消息的分隔符。在问号之间，我将放入消息“严禁未授权访问“违反者将受到法律最大限度的追究！”这将让任何潜在的攻击者知道它们正在侵入一个安全设备或安全网络，而且这是一个受法律保护的环境。按回车键后标语就设置好了。现在我们观察其中一些安全性配置。我将按 Ctrl+C；输入“exit”离开交换机。按回车键。我看到了警告标语和要求输入密码来访问控制台的请求。访问控制台。我将输入密码“cisco”，现在我处于用户执行模式。然后输入“enable”。我现在被要求输入另一个密码来进入特权执行模式。我输入密码“class”，现在我拥有交换机的完全访问权。