实例：限制路由器虚拟终端的连接访问 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/461/2021_2022__E5_AE_9E_E4_BE_8B_EF_BC_9A_E9_c101_461677.htm 对于网络管理员来说，关于路由器的安全可以做的事情很多。如堵住安全漏洞、避免身份危机、限制逻辑访问等。我们也有可能为控制台和虚拟终端连接配置了一个用户名和密码提示，这些措施固然重要。不过，我们还要注意实施其它方面的安全功能。 基础知识 我们可以采取的一项重要的安全措施是实施访问控制列表(ACL)，它实现的是基本的安全。共有两种类型的访问控制列表：数字的和名称的。这两种类型中的每一种都可分为标准的和扩展的。 数字式的访问列表：在操作系统中，数字1到99和1300到1999是为标准的访问列表准备的，而数字100-199和数字2000-2699是为扩展访问列表保留的。在本文中，我们仅仅使用一个基本的访问控制列表来保护我们的虚拟终端连接端口即VTY端口。简言之，我们仅允许某些IP地址或某些网络地址能够远程登录(telnet)到我们的路由器。 名称式的访问列表：一个名称式访问控制列表允许我们通过一个包括文字和数字的名称来引用它。这也就意味着不再使用数字，我们的访问列表可以具备一个有意义的名字，如“ manage_telnet ”,这个名字使得其意义和目的非常清楚。 标准的访问列表：借助于标准的访问列表，我们可以指定数据包的源地址。因此，我们可以检查数据包来自哪里，并且根据数据包的源IP地址，我们可以或者允许，或者拒绝这种通信。 扩展的访问列表：通过扩展的访问列表，我们能够更加精细地控制细节。除了可以控制源IP地址，我们还可以控制

目的IP地址，我们还可以检查源端口号和目的端口号，甚至可以检查许多其它的高级参数，如TCP与UDP、ICMP的比较等。 实例 在本文的例子中，我们将使用数字式的标准访问列表。我们将使用访问列表号1，虽然可以从标准访问列表范围中选择任意一个数字。也就是说我们能够检查这个数据包的源IP地址。 在这里，笔者只想允许一个人能够登录到路由器(您该不会希望有很多人可以登录到您的路由器吧?)。只需先写出访问列表，然后将其应用于我们的VTY端口(用于远程登录)。我们将用“ * ”来控制特定的位模式，并只允许采用几乎任何组合的特定的网络/子网。 此外，在这里有一些免费的白皮书讨论这些问题。您可以根据自己的路由器和网络参考其中的配置。 下面具体看一个实例： 以下是引用片段： bbone_ok>enable bbone_ok #config t bbone_ok (config)#access-list 1 permit 130.107.12.114 在这几行中，我们仅仅进入了全局配置模式，创建了一个访问列表号1，并只允许源自130.107.12.114的数据包。那么，我们如何知道这是一个源地址而不是目标地址呢?很简单，因为这是一个标准的访问列表(1是标准访问列表范围中的第一个数字)，而且此标准访问列表所能做的唯一事情就是检查源IP地址。 到目前为止，这个访问列表还没有做任何事情，因为我们并没有将其运用到任何地方。为了便于理解，我们可以将这个访问列表当作一个安全警卫。我们已经雇用了这个安全警卫，不过我们还没有为他分配任务呢：该让他警卫哪一个门?可以通过使用show startup-config命令查看其“ 门 ”的配置，这个列表应当可以被运用到我们希望控制的任何接口上。因为我们想控制VTY端口，所以先给出访问VTY接口的命令：以下是引用

片段： bbone_ok(config)#line vty 0 4
bbone_ok(config-line)#access-class 1 in 一旦我们进入了行配置模式，就可以通过“ access-class ”命令应用前面所创建的访问列表1。“ access-class ”命令将此访问列表应用于行配置模式(即此处的VTY)。 如此一来，这就仅允许拥有IP地址130.107.12.114的用户能够登录到我们的设备，其它的工作站都被禁止。 这个简单的例子向我们展示了访问控制列表的功能，但愿对你有所帮助。 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