CCNA课程精彩回放之访问控制列表思科认证 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/638/2021_2022_CCNA_E8_AF_BE_E7_A8_8B_c101_638600.htm 访问控制列表（Access Control List，ACL) 是路由器接口的指令列表，用来控制端口进出的数据包。ACL适用于所有的被路由协议，如IP、IPX、AppleTalk等。 ACL的定义也是基于每一种协议的。如果路由器接口配置成为支持三种协议（IP、AppleTalk以及IPX）的情况，那么，用户必须定义三种ACL来分别控制这三种协议的数据包。 ACL的作用 ACL可以限制网络流量、提高网络性能。例如，ACL可以根据数据包的协议，指定数据包的优先级。 ACL提供对通信流量的控制手段。例如，ACL可以限定或简化路由更新信息的长度，从而限制通过路由器某一网段的通信流量。 ACL是提供网络安全访问的基本手段。如图1所示，ACL允许主机A访问人力资源网络，而拒绝主机B访问。ACL可以在路由器端口处决定哪种类型的通信流量被转发或被阻塞。例如，用户可以允许E-mail通信流量被路由，拒绝所有的Telnet通信流量。 ACL的执行过程 一个端口执行哪条ACL，这需要按照列表中的条件语句执行顺序来判断。如果一个数据包的报头跟表中某个条件判断语句相匹配，那么后面的语句就将被忽略，不再进行检查。 ACL具体的执行流程见图2。 在图2中，数据包只有在跟第一个判断条件不匹配时，它才被交给ACL中的下一个条件判断语句进行比较。如果匹配（假设为允许发送），则不管是第一条还是最后一条语句，数据都会立即发送到目的接口。如果所有的ACL判断语句都检测完毕，仍没有匹配的语句出口，则该数据包将视

为被拒绝而被丢弃。 这里要注意，ACL不能对本路由器产生的数据包进行控制。 ACL的分类 目前有两种主要的ACL:标准ACL和扩展ACL。 这两种ACL的区别是，标准ACL只检查数据包的源地址. 扩展ACL既检查数据包的源地址，也检查数据包的目的地址，同时还可以检查数据包的特定协议类型、端口号等。 网络管理员可以使用标准ACL阻止来自某一网络的所有通信流量，或者允许来自某一特定网络的所有通信流量，或者拒绝某一协议簇（比如IP）的所有通信流量。 扩展ACL比标准ACL提供了更广泛的控制范围。例如，网络管理员如果希望做到“ 允许外来的Web通信流量通过，拒绝外来的FTP和Telnet等通信流量 ”，那么，他可以使用扩展ACL来达到目的，标准ACL不能控制这么精确。 在路由器配置中，标准ACL和扩展ACL的区别是由ACL的表号来体现的，上表指出了每种协议所允许的合法表号的取值范围。 正确放置ACL ACL通过过滤数据包并且丢弃不希望抵达目的地的数据包来控制通信流量。然而，网络能否有效地减少不必要的通信流量，这还要取决于网络管理员把ACL放置在哪个地方。 假设在图3所示的一个运行TCP/IP协议的网络环境中，网络只想拒绝从RouterA的T0接口连接的网络到RouterD的E1接口连接的网络的访问，即禁止从网络1到网络2的访问。 根据减少不必要通信流量的通行准则，网管员应该尽可能地把ACL放置在靠近被拒绝的通信流量的来源处，即RouterA上。如果网管员使用标准ACL来进行网络流量限制，因为标准ACL只能检查源IP地址，所以实际执行情况为：凡是检查到源IP地址和网络1匹配的数据包将会被丢掉，即网络1到网络2、网络3和网络4的访问都将被禁止。由此可见，这个ACL

控制方法不能达到网管员的目的。同理，将ACL放在RouterB和RouterC上也存在同样的问题。只有将ACL放在连接目标网络的RouterD上（E0接口），网络才能准确实现网管员的目标。由此可以得出一个结论: 标准ACL要尽量靠近目的端。 网管员如果使用扩展ACL来进行上述控制，则完全可以把ACL放在RouterA上，因为扩展ACL能控制源地址（网络1），也能控制目的地址（网络2），这样从网络1到网络2访问的数据包在RouterA上就被丢弃，不会传到RouterB、RouterC和RouterD上，从而减少不必要的网络流量。因此，我们可以得出另一个结论：扩展ACL要尽量靠近源端。 ACL的配置 ACL的配置分为两个步骤： 第一步:在全局配置模式下，使用下列命令创建ACL： Router (config)# access-list access-list-number {permit | deny } {test-conditions} 其中，access-list-number为ACL的表号。人们使用较频繁的表号是标准的IP ACL（199）和扩展的IP ACL（100－199）。 在路由器中，如果使用ACL的表号进行配置，则列表不能插入或删除行。如果列表要插入或删除一行，必须先去掉所有ACL，然后重新配置。当ACL中条数很多时，这种改变非常烦琐。一个比较有效的解决办法是：在远程主机上启用一个TFTP服务器，先把路由器配置文件下载到本地，利用文本编辑器修改ACL表，然后将修改好的配置文件通过TFTP传回路由器。 这里需要特别注意的是，在ACL的配置中，如果删掉一条表项，其结果是删掉全部ACL，所以在配置时一定要小心。 在Cisco IOS11.2以后的版本中，网络可以使用名字命名的ACL表。这种方式可以删除某一行ACL，但是仍不能插入一行或重新排序。所以，笔者仍然建议使用TFTP服务器进行配置修改。 第二步：在接口配置模

式下，使用access-group命令ACL应用到某一接口上： Router (config-if)# {protocol} access-group access-list-number {in | out } 其中，in和out参数可以控制接口中不同方向的数据包，如果不配置该参数，缺省为out。 ACL在一个接口可以进行双向控制，即配置两条命令，一条为in，一条为out，两条命令执行的ACL表号可以相同，也可以不同。但是，在一个接口的一个方向上，只能有一个ACL控制。 值得注意的是，在进行ACL配置时，网管员一定要先在全局状态配置ACL表，再在具体接口上进行配置，否则会造成网络的安全隐患。