ACL的基本原理、功能与局限性 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/465/2021_2022_ACL_E7_9A_84_E5_9F_BA_E6_c67_465264.htm 网络中常说的ACL是Cisco IOS所提供的一种访问控制技术，初期仅在路由器上支持，近些年来已经扩展到三层交换机，部分最新的二层交换机如2950之类也开始提供ACL的支持。只不过支持的特性不是那么完善而已。在其它厂商的路由器或多层交换机上也提供类似的技术，不过名称和配置方式都可能有细微的差别。本文所有的配置实例均基于 Cisco IOS的ACL进行编写。 基本原理：ACL使用包过滤技术，在路由器上读取第三层及第四层包头中的信息如源地址、目的地址、源端口、目的端口等，根据预先定义好的规则对包进行过滤，从而达到访问控制的目的。 功能：网络中的节点资源节点和用户节点两大类，其中资源节点提供服务或数据，用户节点访问资源节点所提供的服务与数据。ACL的主要功能就是一方面保护资源节点，阻止非法用户对资源节点的访问，另一方面限制特定的用户节点所能具备的访问权限。 配置ACL的基本原则：在实施ACL的过程中，应当遵循如下两个基本原则： 最小特权原则：只给受控对象完成任务所必须的最小的权限 最靠近受控对象原则：所有的网络层访问权限控制 局限性：由于ACL是使用包过滤技术来实现的，过滤的依据又仅仅只是第三层和第四层包头中的部分信息，这种技术具有一些固有的局限性，如无法识别到具体的人，无法识别到应用内部的权限级别等。因此，要达到end to end的权限控制目的，需要和系统级及应用级的访问权限控制结合使用。 100Test 下载频道开通，