访问控制列表使用原则 PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/206/2021_2022__E8_AE_BF_E9_97_AE_E6_8E_A7_E5_c101_206079.htm 由于ACL涉及的配置命令很灵活，功能也很强大，所以我们不能只通过一个小小的例子就完全掌握全部ACL的配置。在介绍例子前为大家将ACL设置原则罗列出来，方便各位读者更好的消化ACL知识。 1、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。也就是说被控制的总规则是各个规则的交集，只满足部分条件的是不容许通过规则的。 2、最靠近受控对象原则 所有的网络层访问权限控制。也就是说在检查规则时是采用自上而下在ACL中一条条检测的，只要发现符合条件了就立刻转发，而不继续检测下面的ACL语句。 3、默认丢弃原则 在CISCO路由交换设备中默认最后一句为ACL中加入了DENY ANY ANY，也就是丢弃所有不符合条件的数据包。这一点要特别注意，虽然我们可以修改这个默认，但未改前一定要引起重视。 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，要达到端到端的权限控制目的，需要和系统级及应用级的访问权限控制结合使用。