ACL学习：自反访问列表引入和配置 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/267/2021_2022_ACL_E5_AD_A6_E4_B9_A0_EF_c101_267166.htm 三台路由器串联，要求阻止R3对R1的远程访问（telnet），但只能在R2上做。R1可以对R3进行telnet登陆。 1 底层配置 R1interface Serial2/1ip address 12.0.0.1 255.255.255.0router eigrp 90network 12.0.0.0 0.0.0.255no auto-summary R2interface Serial2/1ip address 12.0.0.2 255.255.255.0interface Serial2/2ip address 23.0.0.2 255.255.255.0router eigrp 90network 0.0.0.0no auto-summary R3interface Serial2/1ip address 23.0.0.3 255.255.255.0router eigrp 90network 23.0.0.0 0.0.0.255no auto-summary 2 在R2上做ACL 拒绝R3对R1的所有TCP连接，但不能影响R1对R3的telnet 在这里我们先用扩展访问列表做一下，看能不能实现 。r2(config)#access-list 100 deny tcp host 23.0.0.3 host 12.0.0.1r2(config)#access-list 100 permit ip any anyr2(config)#int s2/2r2(config-if)#ip access-group 100 in / 将ACL应用到接口 为了验证将R1和R3的VTY线路配置成直接登陆，无需密码 。r1(config)#line vty 0 4r1(config-line)#no loginr3(config)#line vty 0 4r3(config-line)#no login 现在进行验证。r3#telnet 12.0.0.1Trying 12.0.0.1 ...% Destination unreachable. gateway or host down 在R3上无法telnetR1，访问列表起了作用。我们再去R1做一下验证。r1#telnet 23.0.0.3Trying 23.0.0.3 ...% Connection timed out. remote host not responding 这时，R1也无法telnet R3 这可不是我们所希望的结果。那为什么会产生这种结果呢？这是因为R1向R3发起telnet请求时，是R1的一个随机

端口与R3的23号端口通信。R3收到这个请求后，再用自己的23号端口向R1的随即端口回应。在这个例子中，R1向R3的请求，R3可以收到。但当R3向R1回应时，却被R2上的ACL阻止了。因为R2的ACL的作用是阻止R3向R1的所有TCP连接。这个TCP回应也就被阻止掉了，所以就间接的造成了R1无法telnet到R3. 