两个vlan之间单向控制，reflexiveacl配置介绍 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/260/2021_2022__E4_B8_A4_E4_B8_AAvlan_c101_260712.htm 在做工程中，有时候用户要求2个vlan之间的访问是单向访问，以下内容为介绍支持单向访问的配置案例 Reflexive ACLs 反身ACL是在Cisco IOS Release 11.3引入的.它只能和扩展的命名IP ACL一起定义而不能和基于数字的或标准ACL,以及其他协议的ACL一起.语法如下: ip access-list extended permit any any reflect name [timeout] ip access-list extended evaluate interface ip access-group {number|name} {in|out} 做网络的单向访问其实实现的是防火墙的基本功能:我是内网,你是外网,我能访问你,但你不能访问我. 所以现在假设RouterA的E0口所连网段为内网段,RouterA S0所连的网段为外网段,还假设我想做的是内网的PC机能ping通外网RouterB的S1口,但RouterB却ping不进我的内网. 用ACL来实现类似的单向访问控制需要用到一种特殊的ACL,叫Reflexive ACL.Reflexive ACL的配置分为两个部分,一部分是outbound的配置,一部分是inbound的配置. 在继续下面的说明之前,先说点题外话.在最开始想到单向访问问题时,我(也包括其它一些我的同事)自然的就这么想:那我在E0口上允许PC的流量进来,然后再在S0口上禁止RouterB的流量进来不就行了?看上去好像没什么问题,但一试就知道其实是不行的.为什么不行呢,因为很多人都忽略了这么一个问题:即绝大多数的网络流量都是有去有回的,上面的方法只解决了去的问题,但这个流量在到达RouterB后,RouterB还需要返回这个流量给PC,这个返回的流量到了RouterA的S0口,但上面的方法却在S0口上禁止

了RouterB的流量进来,回来的流量被挡住了,通讯失败. 好,下面再切回来.Reflexive ACL中outbound的部分决定了我出去的哪些内网网络流量是需要被单向访问的,inbound部分决定了这些流量在返回后能被正确的识别并送给内网发起连接的PC机. Reflexive ACL中outbound的部分: ip access-list extended outbound_filter permit icmp any any reflect icmp_traffic permit ip any any !---注意在Reflexive ACL中只能用named方式的ACL,不能用numbered方式的ACL. !---基本配置和普通ACL并没有什么太多不同,不同之处是reflect icmp_traffic,它的意思是这条ACE作为单向流量来处理,并且给了一个名称叫icmp_traffic,icmp_traffic在inbound部分被引用. !---permit ip any any并不是必要的,加在这里是为了另一个测试,下面会说明. Reflexive ACL中inbound的部分: ip access-list extended inbound_filter evaluate icmp_traffic deny ip any any log !---inbound的配置有和普通ACL有点不同了,第一句evaluate icmp_traffic对上述outbound配置中的icmp_traffic进行了引用,也就是说,它要检查从外网进来的流量,如果这个流量确实是从内网发起的对外访问的返回流量,那么允许这个流量进来.