基础学习：动态ACL配置详解 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/270/2021_2022__E5_9F_BA_E7_A1_80_E5_AD_A6_E4_c67_270369.htm IP访问控制列表算是Cisco IOS一个内在的security feature，以下是对常用的动态访问控制列表做了个总结。 Pt.1 Lock-and-Key Security Lock-and-Key Overview lock-and-key动态ACL使用IP动态扩展ACL过滤IP流量。当配置了lock-and-key动态ACL之后，临时被拒绝掉的IP流量可以获得暂时性的许可。 lock-and-key动态ACL临时修改路由器接口下已经存在的ACL，来允许IP流量到达目标设备。之后lock-and-key动态ACL把接口状态还原。 通过lock-and-key动态ACL获得访问目标设备权限的用户，首先要开启到路由器的telnet会话。接着lock-and-key动态ACL自动对用户进行认证。如果认证通过，那么用户就获得了临时性的访问权限。 Configuring Lock-and-Key 配置lock-and-key动态ACL的步骤如下： 1.设置动态ACL： BitsCN(config)#access-list {access-list-number} [dynamic dynamic-name [timeout minutes]] {deny|permit} telnet {source source-wildcard destination destination-wildcard} 2.扩展动态ACL的绝对计时器。可选： BitsCN(config)# access-list dynamic-extend 3.定义需要应用ACL的接口： BitsCN(config)#interface {interface} 4.应用ACL： BitsCN(config-if)#ip access-group {ACL} 5.定义VTY线路： BitsCN(config)#line vty {line-number [ending-line-number]} 6.对用户进行认证： BitsCN(config)#username {username} password {password} 7.采用TACACS认证或本地认证方式。可选：

BitsCN(config-line)#login {tacacs|local} 8.创建临时性的访问许可权限，如果没有定义参数host，默认为所有主机：BitsCN(config-line)#autocommand access-enable {host} [timeout minutes] Case 1 在5分钟内开启到172.16.1.2的telnet会话，如果认证成功，对用户给予120秒的访问许可权：!interface Ethernet0description this document is written by *****description powered by BitsCN ip address 172.16.1.1 255.255.255.0ip access-group 101 in!access-list 101 permit tcp any host 172.16.1.2 eq telnetaccess-list 101 dynamic BitsCN timeout 120 permit ip any any! line vty 0 4login tacacsautocommand access-enable timeout 5! Monitoring and Maintaining Lock-and-Key 查看ACL信息：BitsCN#show access-listsPt.2 TCP InterceptingTCP Intercepting Overview 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com