CCSP SNRS Lab2 - Lock-and-Key (Dynamic Access Lists)

?Lab Topology?

?Lab Object? Technical characteristics: *1.* Provide the authentication based on the single user. *2.* Simplify the management in a large network. *3.* Reduce the handling burden of the router, as the list is temporary and is not written statically. *4.* Reduce the possibility of address spoofing attack. **?Lab Process?** *1.* The configuration steps of Dynamic Access Lists: GW(config)#access-list 101 permit tcp any host 192.168.1.1 eq 23 GW(config)#access-list 101 dynamic DACL timeout 9999 permit ip any any Here, timeout time is implicit, if time exceeds this time, re-authentication must be performed. GW(config)#interface e0/0 GW(config-if)#ip access-group 101 in GW(config)#username cisco password cisco GW(config)#line vty 0 4 GW(config-line)#login local GW(config-line)#autocommand access-enable host timeout 6 After the success of authentication, the whole network will be allowed if not adding the host based on the host authentication. *2.* Test: When the inside router wants to access the outside router, first, telnet the gateway router, after the success of authentication, disconnect telnet and then the list will be generated dynamically on the gateway router. Thus the inside router can access the outside router. But the gateway router configured as above can't be login by telnet, Autocommand can be written under the username, thus the gateway router can be login GW(config)# username cisco autocommand access-enable host timeout 6 Clear the generated dynamic access list: GW(config)# clear access-template 101 DACL host 192.168.1.100 any