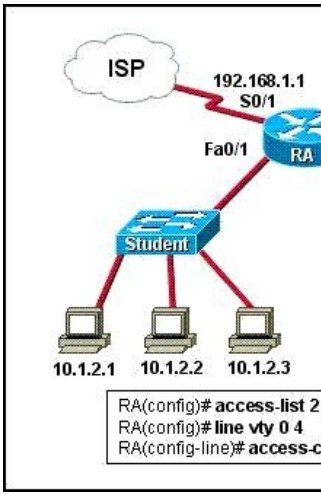
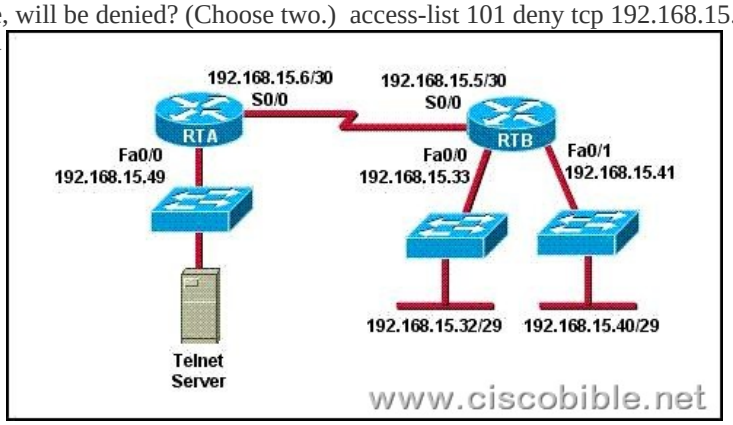
CCNA 640-802 Bible - Configure and Apply an ACLs to Limit Telnet and SSH

1. Unauthorized users have used Telnet to gain access to a company router. The network administrator wants to configure and apply an access list to allow Telnet access to the router, but only from the network administrator's computer. Which group of commands would be the best choice to allow only the IP address 172.16.3.3 to have Telnet access to the router? A: access-list 3 permit host 172.16.3.3 line vty 0 4 ip access-group 3 in B: access-list 3 permit host 172.16.3.3 line vty 0 4 access-class 3 in C: access-list 101 permit tcp any host 172.16.3.3 eq telnet interface s0/0 ip access-group 101 in D: access-list 101 permit tcp any host 172.16.3.3 eq telnet access-list 101 permit ip any any interface s0/0 ip access-group 101 in **Correct Answers: B** Explanation: To restrict incoming and outgoing connections between a particular vty (into a Cisco device) and the addresses in an access list, use the access-class command in line configuration mode. Example: The following example defines an access list that permits only hosts on network 192.89.55.0 to connect to the virtual terminal ports on the router: access-list 12 permit 192.89.55.0 0.0.0.255 line 1 5 access-class 12 in 2. Refer to the exhibit. Why would the network administrator configure RA in this manner?

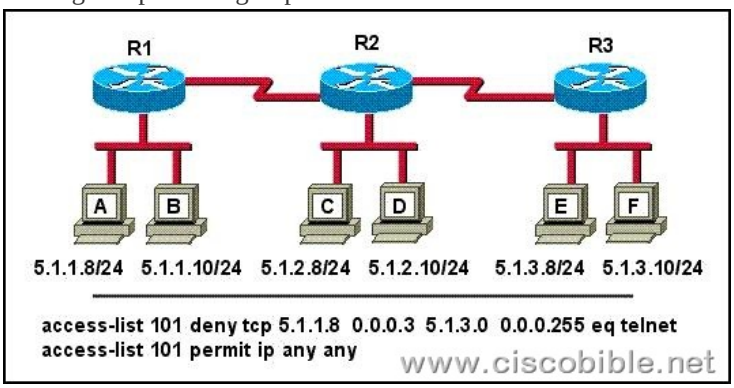


A: to give students access to the Internet B: to prevent students from accessing the command prompt of RA C: to prevent administrators from accessing the console of RA D: to give administrators access to the Internet E: to prevent students from accessing the Internet F: to prevent students from accessing the Admin network **Correct Answers: B** Explanation: An ACL is configured on RA to allow users on the 10.1.1.0/24 network to access VTY line of RA and to prevent the access of other users. 3. Refer to the exhibit. The access list has been configured on the S0/0 interface of router RTB in the outbound direction. Which two packets, if routed to the interface, will be denied? (Choose two.) access-list 101 deny tcp 192.168.15.32 0.0.0.15 any eq telnet access-list 101 permit ip any any



A:source ip address: 192.168.15.5; destination port: 21 B:source ip address:, 192.168.15.37 destination port: 21 C:source ip address:, 192.168.15.41 destination port: 21 D:source ip address:, 192.168.15.36 destination port: 23 E:source ip address: 192.168.15.46; destination port: 23 F:source ip address:, 192.168.15.49 destination port: 23 **Correct Answers: D, E** Explanation: This question is to examine the understanding of the ACL. We can learn from the above-mentioned ACL configuration information that access-list 101 denies the telnet session from the IP address of 192.168.15.32/28 segment, and the telnet port number is 23. Therefore, according to the above-mentioned conditions, the data packet will be discarded if the IP address of 192.168.15.32-192.168.15.47 segment launch telnet request. 4. The access control list shown in the graphic has been applied to the

Ethernet interface of router R1 using the ip access-group 101 in command. Which of the following Telnet sessions will be blocked by this ACL? (Choose two.)



A: from host A to host 5.1.1.10 B: from host A to host 5.1.3.10 C: from host B to host 5.1.2.10 D: from host B to host 5.1.3.8 E: from host C to host 5.1.3.10 F: from host F to host 5.1.1.10 **Correct Answers: B, D** Explanation: All the telnet sessions from the single host (host B) to any device in the 5.1.3.0/24 network will be denied, while all other traffic will be permitted as specified by the second line in access list 101.