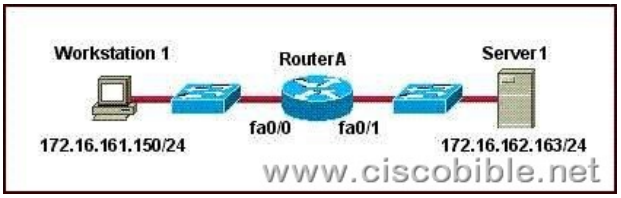
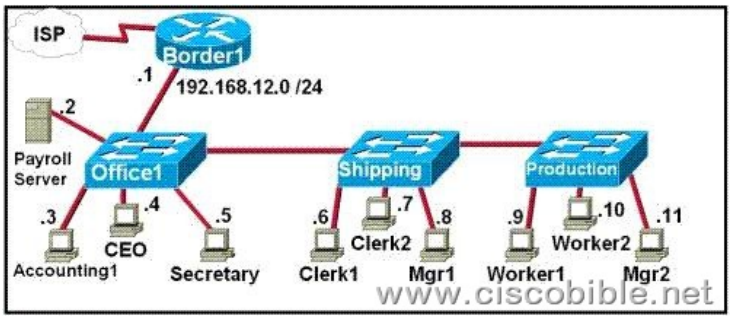
CCNA 640-802 Bible - Configure and Apply ACLs Based on Network Filtering

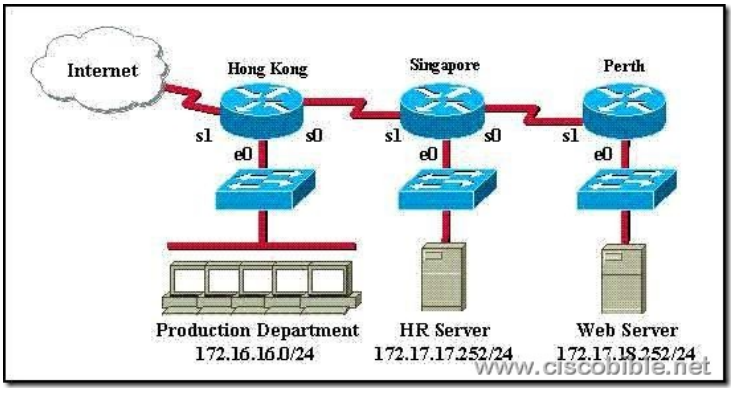
1. Refer to the graphic. It has been decided that Workstation 1 should be denied access to Server1. Which of the following commands are required to prevent only Workstation 1 from accessing Server1 while allowing all other traffic to flow normally? (Choose two.)



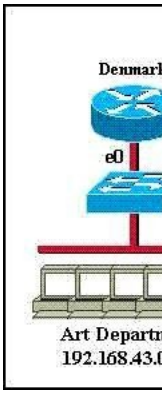
A:RouterA(config)# interface fa0/0 RouterA(config-if)# ip access-group 101 out B:RouterA(config)# interface fa0/0 RouterA(config-if)# ip access-group 101 in C:RouterA(config)# access-list 101 deny ip host 172.16.161.150 host 172.16.162.163 RouterA(config)# access-list 101 permit ip any any D:RouterA(config)# access-list 101 deny ip 172.16.161.150 0.0.0.255 172.16.162.163 0.0.0.0 RouterA(config)# access-list 101 permit ip any any **Correct Answers: B, C** Explanation: To block communication between Workstation A and Server 1, we have to configure Extended Access List. To define an extended IP access list, use the extended version of the access-list command in global configuration mode. To remove the access lists, use the no form of this command. access-list access-list-number [dynamic dynamic-name [timeout minutes]] {deny | permit} protocol source source-wildcard destination destination-wildcard Source Address will be of the Workstation A i.e. 172.16.161.150 and destination address will be of the Server 1 i.e. 172.16.162.163. The access list will be placed on the FA0/0 of Router A. 2. For security reasons, the network administrator needs to prevent pings into the corporate networks from hosts outside the internetwork. Which protocol should be blocked with access control lists? A: IP B: ICMP C: TCP D: UDP **Correct Answers: B** Explanation: A ping is a computer network tool used to test whether a particular host is reachable across an IP network. It works by sending ICMP "echo request" packets to the target host and listening for ICMP "echo response" replies. ping estimates the round-trip time, generally in milliseconds, and records any packet loss, and prints a statistical summary when finished. 3. Refer to the exhibit. The FMJ manufacturing company is concerned about unauthorized access to the Payroll Server. The Accounting1, CEO, Mgr1, and Mgr2 workstations should be the only computers with access to the Payroll Server. What two technologies should be implemented to help prevent unauthorized access to the server? (Choose two.)



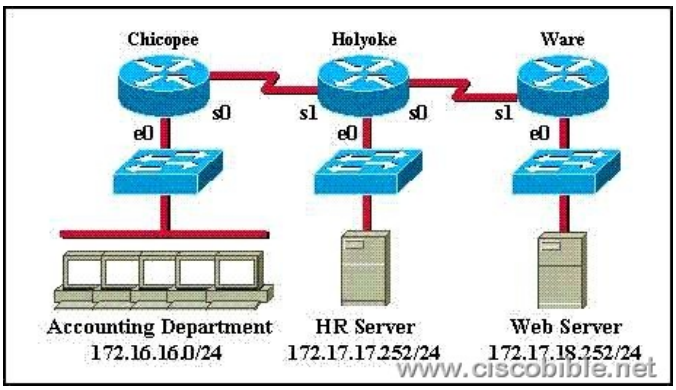
A:access lists B:encrypted router passwords C:STP D:VLANs E:VTP F:wireless LANs **Correct Answers: A, D** 4. Refer to the graphic. Assuming the following goals: 1) allow Telnet from the Internet to the HR server 2) allow HTTP access from the Internet to the web server 3) all other traffic from the Internet should be blocked Which of the following access list statements are necessary to accomplish these goals? (Select two.)



A:access-list 101 permit tcp any 172.17.18.252 0.0.0.0 eq 80 B:access-list 1 permit tcp any 172.17.17.252 0.0.0.0 eq 23 C:access-list 101 deny tcp any 172.17.18.252 0.0.0.0 eq 80 D:access-list 101 permit tcp 172.17.17.252 0.0.0.0 any eq 23 E:access-list 101 deny tcp any 172.17.17.252 0.0.0.0 eq 23 F:access-list 101 permit tcp any 172.17.17.252 0.0.0.0 eq 23 **Correct Answers: A, F** Explanation: Because of the implicit deny rule at the end of every access list, only two choices need to be made, as the final requirement is automatic. A. This is correct as we need to allow the access list to allow port 80 connections (port 80 = HTTP) from anywhere, to the web server's IP address. F. This will fulfill the first requirement, as it allows port 23 (Telnet) traffic from anywhere. **Incorrect Answers:** B. The answer asks you to create an access list, a single one. The answer choices require you to choose two answers. For two statements to be on the same list, you need them to have the same number. So answer choice B can be ruled out by process of elimination. In addition to this, access list 1 is an illegal number, since we need an extended access list to use source and destination information, and extended access lists are in the 100-199 range. D. This is incorrect as it allows telnet traffic from the HR server to the Internet, but we need it to be the other way around. C, E: Because of the implicit deny any rule; we need to only be concerned with the access rules that permit traffic. 5. Refer to the graphic. Which of the following access list statements are necessary to allow FTP access to the HR server from the Internet while blocking all other traffic? (Select two.)



A:access-list 101 permit tcp any 192.168.44.252 0.0.0.0 eq 21 B:access-list 101 permit tcp any 192.168.44.252 0.0.0.0 eq 20 C:access-list 101 permit tcp 192.168.44.252 0.0.0.0 any eq 20 D:access-list 101 permit tcp 192.168.44.252 0.0.0.0 any eq 21 E:access-list 101 deny tcp any 192.168.44.252 0.0.0.0 gt 21 F:access-list 101 deny tcp 192.168.44.252 0.0.0.0 any gt 21 **Correct Answers: A, B** Explanation: FTP uses two ports: TCP port 20 and TCP port 21. you want to allow all hosts (ANY) to access the HR server (192.168.44.252 0.0.0.0) through ftp (eq 20 & eq 21) and the implicit deny any rule will block everything else. 6. An access list has been designed to prevent HTTP traffic from the Accounting Department from reaching the HR server attached to the Holyoke router. Which of the following access lists will accomplish this task when grouped with the e0 interface on the Chicopee router?



A: permit ip any any deny tcp 172.16.16.0 0.0.0.255 172.17.17.252 0.0.0.0 eq 80 B: permit ip any any deny tcp 172.17.17.252 0.0.0.0 172.16.16.0 0.0.0.255 eq 80 C: deny tcp 172.17.17.252 0.0.0.0 172.16.16.0 0.0.0.255 eq 80 permit ip any any D: deny tcp 172.16.16.0 0.0.0.255 172.17.17.252 0.0.0.0 eq 80 permit ip any any **Correct Answers: D**