**Moulik Tammana**

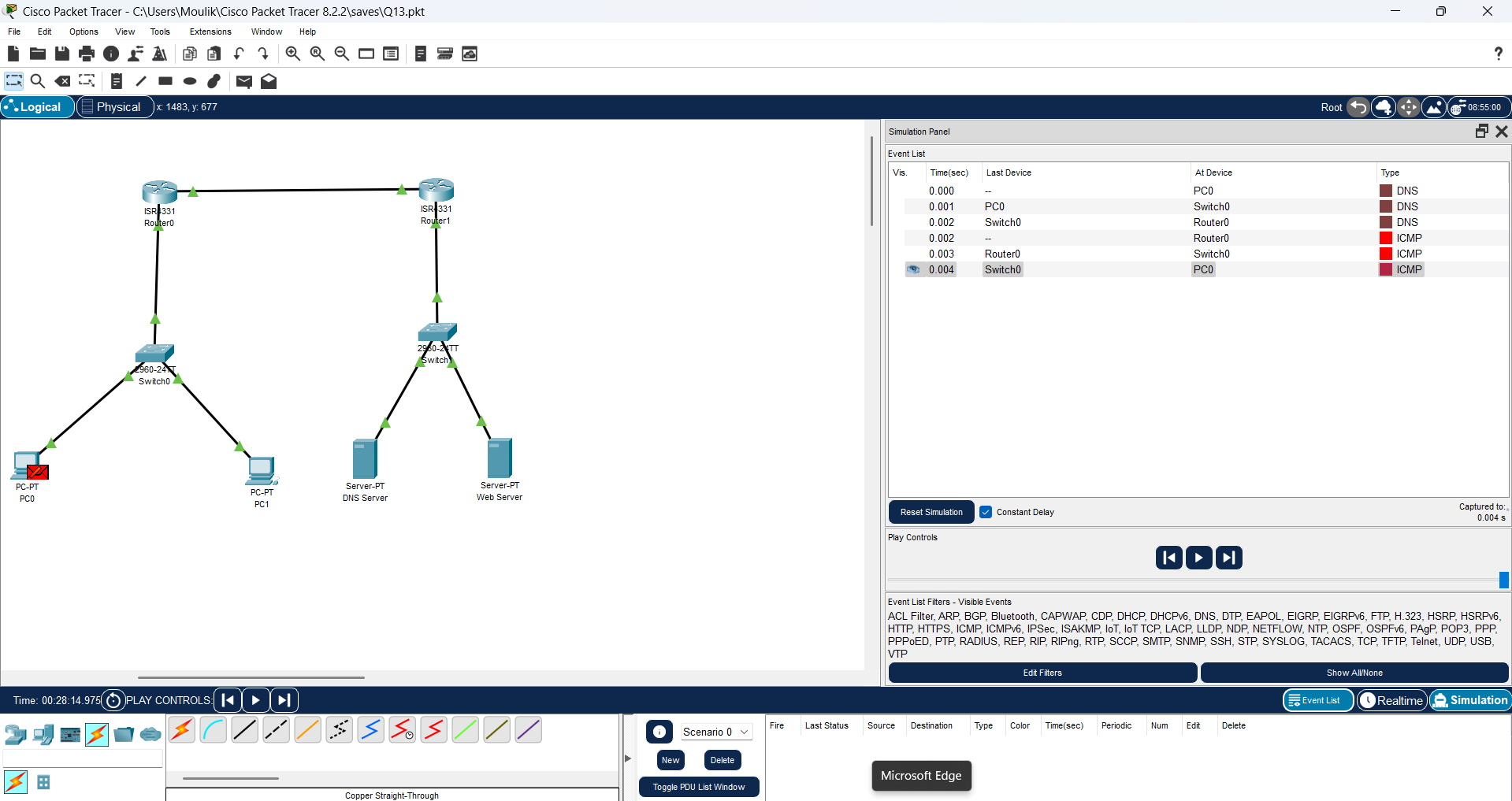
**Q13. Create an extended ACL to block specific applications, such as HTTP or FTP traffic. Test the ACL rules by attempting to access blocked services.**

****

****

**In Cisco Packet Tracer, an Extended Access Control List (ACL) can be implemented on a router to block specific applications such as HTTP (port 80) and FTP (port 21) traffic. The ACL is created using the access-list command and applied to the router’s interface to control inbound or outbound traffic. To configure this, an extended ACL (e.g., ACL 101) is defined to deny TCP traffic on ports 80 and 21 while allowing all other traffic. Once applied to the appropriate interface, testing can be performed by attempting to access a web server via HTTP or establish an FTP connection. If configured correctly, these services should be blocked, while other traffic, such as ICMP (ping), should remain unaffected. The ACL rules can be verified using the show access-lists and show running-config commands to ensure proper enforcement of network security policies.**

**So the above command is used to block the packet for getting forwarded.**

****