If you wanted to deny all Telnet connections to only network 192.168.10.0, which command could you use?

A. access-list 100 deny tcp 192.168.10.0 255.255.255.0 eq telnet

B. access-list 100 deny tcp 192.168.10.0 0.255.255.255 eq telnet

C. access-list 100 deny tcp any 192.168.10.0 0.0.0.255 eq 23

D. access-list 100 deny 192.168.10.0 0.0.0.255 any eq 23

**Step 1:**

Telnet is a protocol for connecting to remote computers (referred to as hosts) across a TCP/IP network (such as the internet). You can connect to a telnet server using telnet client software on your computer (that is, the remote host).

**Step 2: Answer with Explanation**

**Answer : option c** **access-list 100 deny tcp any 192.168.10.0 0.0.0.255 eq 23**

The extended access list ranges are 100–199 and 2000–2699, hence 100 is a valid access list number. Telnet utilises TCP, hence TCP is a legitimate protocol. All that's left now is to find the source and destination addresses. Only the third option contains the right parameter sequence. Answer B might work, but the query expressly mentions "only" for the network 192.168.10.0, and answer B's wildcard is too broad.

**Hence option c is the answer**